Deutscher Bundestag **Drucksache 21/120**

21. Wahlperiode 10.04.2025

Unterrichtung

durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

33. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit (Tätigkeitsbericht für das Jahr 2024)

Zugeleitet mit Schreiben der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 10. April 2025 gemäß § 15 des Bundesdatenschutzgesetzes.

Inhaltsverzeichnis

1 Einleitung ... 8

2 Empfehlungen ... 11
2.1 Zusammenfassung der Empfehlungen des 33. Tätigkeitsberichts ... 11
2.2 Empfehlungen des 32. Tätigkeitsberichts ... 12

3 Schwerpunktthemen ... 19
3.1 Gesundheit ... 19
3.1.1 Forschungsdatenzentrum Gesundheit ... 19
3.1.2 Taskforce Forschungsdaten ... 20
3.1.3 European Health Data Space ... 20
3.1.4 Die neue ePA auf Widerspruchsbasis ... 21
3.2 Künstliche Intelligenz ... 23
3.2.1 KI-Verordnung ... 23
3.2.2 KI als Fokusthema der Gremienarbeit ... 24
3.2.3 BfDI Prüfkatalog für KI-Anwendungen ... 25
3.3 Sicherheit ... 26
3.3.1 Klage gegen den BND ... 26
3.3.2 BfDI droht Verlust der Aufsicht über die Nachrichtendienste ... 27
3.3.3 Gründlichkeit und Verhältnismäßigkeit beim „Sicherheitspaket“ ... 28
3.3.4 Debatte um Quick Freeze und Vorratsdatenspeicherung versachlichen ... 28

4 Gremien ... 30
4.1 Bericht aus der DSK ... 30
4.2 Europäischer Datenschutzausschuss ... 30
4.2.1 Allgemeiner Bericht aus dem EDSA ... 30
4.2.2 Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO ... 33
4.2.3 Bericht aus dem CSC ... 34
4.2.4 Entwicklungen im Bereich internationaler Datenübermittlungen ... 35
4.2.5 Coordinated Enforcement Framework Action 2024 ... 38
4.3 46. Jahreskonferenz der Global Privacy Assembly ... 38
4.4 Berlin Group ... 39
4.5 Weitere Gremien ... 41
4.5.1 ETIAS-Beratungsgremium für Grundrechte ... 41
4.5.2 G7 DPA Roundtable ... 42
4.5.3 High Level Group zur EU-Vorratsdatenspeicherung ... 43

5 Gesetzgebung ... 45
5.1 Gesundheit und Forschung ... 45
5.1.1 Bundesinstitut für Prävention und Aufklärung in der Medizin ... 45
5.1.2 Gesundheitsversorgungsstärkungsgesetz ... 45
5.1.3 Gesetz zur Reform der Notfallversorgung ... 46

5.2 Sicherheit . . . 46
5.2.1 Der Vorschlag zur Novelle des Sicherheitsüberprüfungsgesetzes . . . 46
5.2.2 Modernisierung des Bundespolizeigesetzes steht weiter aus . . . 48
5.2.3 BKA II-Entscheidung des Bundesverfassungsgerichts . . . 49
5.3 Inneres und Justiz . . . 50
5.3.1 Erstes Gesetz zur Änderung des Bundesdatenschutzgesetzes . . . 50
5.3.2 NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz . . . 51
5.3.3 OZG-Änderungsgesetz . . . 52
5.3.4 Registerzensusgesetz . . . 53
5.4 Wirtschaft und Finanzen . . . 54
5.4.1 Telemedien heißen nun Digitale Dienste . . . 54
5.4.2 Der Digital Service Act und das Digitale Dienste Gesetz . . . 55
5.4.3 Automatisiertes und vernetztes Fahren ohne umfassende Videoerfassung öffentlicher Räume . . . 56
5.4.4 Neue Gesetzgebung zur Bekämpfung von Finanzkriminalität . . . 57
5.5 Arbeit und Soziales . . . 58
5.5.1 Beschäftigtendatengesetz . . . 58
5.5.2 Kindergrundsicherung . . . 58

6 Informationsfreiheit . . . 60
6.1 Statistische Auswertungen zur Informationsfreiheit . . . 60
6.2 Gremien . . . 61
6.2.1 Konferenz der Informationsfreiheitsbeauftragten . . . 61
6.2.2 Internationale Konferenz der Informationsfreiheitsbeauftragten . . . 62
6.3 Erfahrungsaustausch . . . 64
6.3.1 Zweiter Europäischer Case Handling Workshop zur Informationsfreiheit . . . 64
6.3.2 Erfahrungsaustausch der Bundesbehörden zur Informationsfreiheit . . . 64
6.4 Vermittlungsverfahren . . . 65
6.4.1 Vertraulichkeit eines Fachgesprächs zwischen BVerfG und EGMR – zu den Grenzen des Vermittlungsverfahrens . . . 65
6.4.2 Grenzen der behördlichen Informationsbeschaffungspflicht . . . 65
6.4.3 Die Einstufung eines Dokuments erfasst nicht die gesamte Akte . . . 67
6.5 Beratungs- und Kontrollbesuche . . . 67
6.5.1 Beratungs- und Kontrollbesuch beim Bundespolizeipräsidium . . . 67
6.5.2 Beratungs- und Kontrollbesuch im BMVg . . . 68

7 Einzelthemen . . . 69
7.1 Gesundheit . . . 69
7.1.1 Authentifizierungsmöglichkeiten der gesetzlich Versicherten . . . 69
7.1.2 Entwicklung der medizinischen Registerlandschaft . . . 70
7.1.3 Ausgewählte Entscheidungen im Bereich Gesundheit . . . 71
7.1.4 Modellvorhaben Genomsequenzierung . . . 72
7.2 Inneres und Justiz . . . 73
7.2.1 Registermodernisierung . . . 73
7.2.2 EuGH-Urteile zum Beschwerderecht . . . 77
7.2.3 Datenschutz im Deutschen Bundestag . . . 78
7.2.4 Sicherheitslücken gefährden den Schutz personenbezogener Daten . . . 79
7.2.5 Die europäische Brieftasche für die digitale Identität und ihre nationale Umsetzung in Deutschland . . . 79
7.2.6 Anonymisierung . . . 81
7.2.7 Rechtsklarheit bei IFG-Anfragen über Frag-den-Staat . . . 81
7.2.8 Der neue Dienst „Mein Justizpostfach“ . . . 82
7.2.9 Frühzeitige Einbindung bei geplanter Neuregelung zur Verhütung von Strom- und Gasunterbrechungen . . . 83
7.2.10 Datenschutz bei der Bundestagswahl . . . 84

7.3 Wirtschaft und Finanzen . . . 84
7.3.1 European Blockchain Sandbox . . . 84
7.3.2 Messengerdienste . . . 85
7.3.3 Positionspapier zur Pseudonymisierung von Stromzählerdaten . . . 87
7.3.4 Untersuchungen von Android-Apps am Beispiel von Kinder-Smartwatches . . . 88
7.3.5 Anforderungen an sichere Videokonferenzdienste . . . 89
7.3.6 Zusammenarbeit mit anderen Aufsichtsbehörden . . . 90
7.3.7 Altersprüfung in digitalen Diensten . . . 91
7.3.8 „Chatkontrolle“ versus Grundrechte . . . 92
7.3.9 Zustellung in automatisierte Paketautomaten nach dem neuen Postgesetz . . . 94
7.3.10 50. Jour fixe Telekommunikation . . . 95
7.3.11 Kein KI-Training bei Meta . . . 95
7.3.12 Abomodelle bei großen Online-Plattformen . . . 96
7.4 Sicherheit . . . 97
7.4.1 Umsetzung des Smart-Borders-Programms der EU durch die Grenzkontrollbehörden . . . 97
7.4.2 OSINT-Beobachtungen im Internet . . . 98
7.4.3 Novellierung des Fluggastdatengesetzes . . . 99
7.4.4 Polizei 20/20 . . . 100
7.4.5 Sicherheitsüberprüfungen in der Wirtschaft . . . 102
7.4.6 BfDI erhält vollständigen FIU-Bericht . . . 103
7.4.7 Löscherfolge bei der FIU . . . 104
7.5 Arbeit und Soziales . . . 105
7.5.1 Berechtigungsnachweis für Sozialtickets . . . 105
7.5.2 Datenschutzpanne beim Rentenservice der Deutschen Post AG . . . 105

8 Kontrollen und Beratungen . . . 106
8.1 Beratungs- und Kontrollbesuche im Sicherheitsbereich . . . 106
8.1.1 Kontrolle von Speicherungen im Vorgangsbearbeitungssystem der Bundespolizei . . . 106
8.1.2 SÜG-Kontrollen belegen erhöhten Beratungsbedarf . . . 106
8.1.3 Kontrolle der Anti-Terror-Datei und der Rechtsextremismus-Datei . . . 108
8.1.4 Kontrolle des Gemeinsamen Extremismus- und Terrorismusabwehrzentrums . . . 109
8.1.5 Beratung und Kontrolle des BfV . . . 110
8.1.6 Beratung und Kontrolle des BAMAD . . . 113
8.1.7 Das Militärische Nachrichtenwesen in der Diskussion . . . 114
8.1.8 Informations- und Beratungsbesuch beim BND . . . 115
8.1.9 Keine Beeinträchtigung der sicherheitsbehördlichen Arbeit durch die Kontroll- und Beratungstätigkeit der BfDI . . . 115
8.1.10 Datenschutz im Schengen-Raum: Aufsicht über das SIS . . . 116
8.1.11 Beratung und Kontrolle beim GBA . . . 117
8.1.12 Kontrolle des BKA im Bereich der politisch motivierten Kriminalität im links zugeordneten politischen Spektrum . . . 117
8.1.13 Kontrolle verdeckter Maßnahmen beim BKA . . . 118
8.2 Allgemeine Beratungs- und Kontrollbesuche . . . 118
8.2.1 Erfahrungsaustausch mit den bDSB der gesetzlichen Krankenkassen . . . 118
8.2.2 Beratungs- und Kontrollbesuche bei gesetzlichen Kranken- sowie Pflegekassen . . . 119
8.2.3 Aus der Beratungs- und Kontrollpraxis bei Telekommunikationsanbietern . . . 119
8.2.4 Das Cloud-Reallabor . . . 120
8.2.5 Datenschutzrechtliche Kontrolle im Finanzamt Überlingen . . . 120
8.2.6 Kontrolle des IT-Systems „ANSWER“ beim BZSt . . . 121
8.2.7 Kontrolle in der deutschen Botschaft in London . . . 122
8.2.8 Datenschutz bei Vereinsverbotsverfahren . . . 122
8.2.9 Beratungs- und Kontrollbesuch im StBA . . . 123

9 BfDI intern ... 124
9.1 Personalentwicklung 2024 ... 124
9.2 Presse- und Öffentlichkeitsarbeit ... 124
9.3 Veranstaltungen der BfDI ... 126
9.4 Zahlen und Fakten zum Berichtsjahr ... 127
9.5 Aufbau Future Foresight bei der BfDI ... 129
9.6 Ein Behörden-Cluster für bessere Digitalisierung ... 131
9.7 Aus dem KI-Workshop des Digital Cluster Bonn ... 131

10 Zentrale Anlaufstelle ... 133

Anlagen ... 136
Anlage 1 Kontrollierte Stellen ... 136
Anlage 2 Erlassene Maßnahmen/Beanstandungen gegenüber öffentlichen Stellen ... 138
Anlage 3 Erlassene Maßnahmen/Beanstandungen gegenüber nicht-öffentlichen Stellen ... 145
Anlage 4 Übersicht Gremien national/europäisch/international ... 148
Abkürzungsverzeichnis ... 152

Impressum ... 156

1 Einleitung

Auch im Jahr 2024 setzte sich meine Behörde in den Bereichen Datenschutz und Informationsfreiheit nachhaltig für die Grundrechte der Bürgerinnen und Bürger ein. Viele Projekte konnten neu aufgenommen und zahlreiche erfolgreich zu Ende geführt werden. Meine Tätigkeit und die meines Vorgängers im Berichtszeitraum erläutere ich Ihnen in diesem Tätigkeitsbericht.

Vorab möchte ich Ihnen einleitend beschreiben, was ich anders machen möchte, was meine Vision ist, was Datenschutz anders machen muss, um eine Zukunft zu haben. Datenschutz ist kein Hindernis, sondern Chance und Standortvorteil, weil er Vertrauensgarant ist. Datenschutz ist Selbstbestimmung, Eigenverantwortung und Freiheit für alle Bürgerinnen und Bürger. Das Datenschutzrecht bietet einen Aktions- und Gestaltungsraum für Fortschritt, Teilhabe, gesamtgesellschaftliche Wertschöpfung sowie innere und äußere Sicherheit. Moderner Datenschutz steht einer digitalen Entwicklung mit Vorteilen für alle Bürgerinnen und Bürger nicht im Wege, sondern unterstützt sie.

Seien Sie versichert: Ich stehe der digitalen Transformation nicht entgegen, sondern möchte diese gemeinsam mit meiner Behörde konstruktiv begleiten und gleichzeitig den Schutz des informationellen Selbstbestimmungsrechts hoch halten. Ich sehe Datenschutz und Informationsfreiheit als Eckpfeiler zur Sicherung europäischer Werte. Ich möchte einer grundrechtssensiblen digitalen Transformation den Weg bereiten.

Hierfür habe ich mir ein strategisches und drei inhaltliche Ziele gesetzt:

Strategisch möchte ich noch früher und intensiver in den Dialog mit Gesellschaft und Gesetzgeber, Forschung und Wirtschaft gehen. Ich will so früh wie möglich wissen, wo die datenschutzrechtlichen Herausforderungen von Digitalisierungsprojekten liegen, um von Anfang an Lösungen anbieten zu können. Ich möchte zuhören, erklären, mitnehmen und Prozesse mitgestalten, statt auf die Rolle der „Nein-Sagerin“ beschränkt zu werden. Das war meine Behörde nie, auch wenn manche uns diese Rolle zugeschrieben haben. Es ist unsere gemeinsame Verantwortung, regulatorische Lösungen für Forschung und Entwicklung, Innovation und Wertschöpfung anzubieten, die mit den Grundrechten im Einklang stehen.

Meine Amtszeit ist eine Einladung zum Dialog an Gesellschaft, Gesetzgeber, Forschung und Wirtschaft. Ich möchte gemeinsam mit Ihnen konstruktive Lösungen für vertrauenswürdige digitale Innovationen entwickeln. Ich appelliere an alle Akteure, uns frühzeitig in die Gesetzgebung und die Ausgestaltung von Digitalisierungsprozessen aktiv einzubinden. Dort, wo die Zusammenarbeit schon gut funktioniert, sollten wir den gemeinsamen Weg weitergehen. Dort, wo es hakt, biete ich einen Neuanfang an.

Inhaltlich möchte ich in meiner Amtszeit drei Themenfeldern besondere Aufmerksamkeit widmen: Gesundheit, Künstliche Intelligenz und Sicherheit.

Im Gesundheitsbereich werden die sensibelsten personenbezogenen Daten verarbeitet. Deshalb ist es aus meiner Sicht essentiell, Datenschutz hier von vornherein mitzudenken. Dies betrifft etwa den Zugang zu Forschungsdaten, der ergiebig und zugleich datenschutzkonform sowie vertrauensvoll sein muss. Gerade im Gesundheitsbereich werden Datenschutz und Datennutzbarkeit noch immer zu sehr gegeneinander gedacht. Dabei hängt der Erfolg von Forschungsdatenzugang, digitalen Gesundheitsanwendungen und der elektronischen Patientenakte nach meiner festen Überzeugung gerade von hohen Datenschutz- und IT-Sicherheitsstandards ab. Sie müssen die Grundrechte der Betroffenen schützen, dürfen aber gleichzeitig ein hohes Maß an Funktionalität der Systeme nicht verhindern. Sie sind ein zentraler Baustein, um Krankheiten besser und schneller zu verstehen sowie zu behandeln. Ich wünsche mir im Gesundheitsbereich daher wieder mehr Austausch und mehr gegenseitiges Verständnis für Nutzerfreundlichkeit einerseits und grundrechtliche Erfordernisse andererseits.

Künstliche Intelligenz (KI) hat schon heute sowohl im Gesundheitswesen als auch in vielen anderen gesellschaftlichen Bereichen massiven Einfluss. KI bietet aus meiner Sicht große Chancen, etwa durch die Analyse großer Datenmengen zur Verbesserung von Diagnosen und Therapien. Allerdings birgt KI auch Datenschutzrisiken. Ich setze mich daher für eine vertrauenswürdige, rechtmäßige und grundrechtsorientierte KI-Landschaft ein. Die KI-Aufsicht gehört nach meiner festen Überzeugung in die Hände der Datenschutzbehörden: Wir haben schon jetzt die notwendigen Expertinnen und Experten dafür. Wir sind außerdem vollständig unabhängig und müssen keine teuren neuen Strukturen aufbauen. Gerade in Zeiten haushaltspolitischer Knappheit dürfte jede andere Entscheidung des Gesetzgebers besonders rechtfertigungsbedürftig sein.

Im Sicherheitsbereich wünsche ich mir ebenfalls mehr Dialog, Austausch und Beratung. Der Preis für unsere Sicherheit darf nie unsere Freiheit sein. Datenschutz ist hier von besonderer Bedeutung, da oft hochsensible Daten verarbeitet werden und das Risikopotenzial eines falschen Verdachts mit jedem erhobenen Datum und jeder automatisierten Analyse steigt. Gleichzeitig ist es völlig klar, dass die Sicherheit der Bevölkerung und des Staates unbedingt gewährleistet sein muss. Wir brauchen ein Gleichgewicht zwischen der Gewährleistung der inneren und äußeren Sicherheit sowie dem Schutz der Freiheitsrechte der Bürgerinnen und Bürger. Die bestehende unabhängige Kontrollarchitektur durch meine Behörde leistet hierzu einen wesentlichen Beitrag. Ich halte es daher für falsch, die behördliche Nachrichtendienstaufsicht auch in Bezug auf die Datenschutzkontrolle auf eine andere Behörde zu konzentrieren. Stattdessen sollte aus meiner Sicht die rechtliche Grundlage dafür geschaffen werden, dass sich meine Behörde mit den übrigen Aufsichtsbehörden besser inhaltlich austauschen kann. Das schafft weder Doppelkontrolle noch zusätzlichen Aufwand, sondern sichert schlichtweg die rechtsstaatlich erforderliche Aufsicht über die Nachrichtendienste.

Selbstverständlich sind auch die weiteren Bereiche der Tätigkeit meiner Behörde von hoher Bedeutung. Auch dort werde ich weiterhin so engagiert und ehrgeizig prüfen, informieren und beraten, wie bisher. Ich erwarte aber besondere Herausforderungen in den drei genannten Schwerpunktbereichen und insoweit einen engen Begleitungsbedarf. Insgesamt werbe ich noch stärker als bisher für einen Datenschutz, der rote Linien klar aufzeigt, aber unterhalb dieser roten Linien konstruktive Lösungen, einen Korridor des Möglichen, anbietet. Ein wichtiges Anliegen ist mir hierbei die positive Kommunikation mit allen Akteuren, die möglichst frühzeitig erfolgen und die strategischen Entscheidungen von Verantwortlichen beeinflussen soll. Wo Beratung nicht fruchtet werde ich aber selbstverständlich weiterhin meine Aufsichtsfunktion mit Nachdruck einfordern.

Besonders am Herzen bei der Erreichung meiner Ziele liegt mir die technische Expertise, die mein Haus im vergangenen Jahr weiter ausbauen konnte und auch ausbauen wird. Wir konnten zahlreiche technische Referentinnen und Referenten gewinnen. Zugleich konnten wir ein eigenes Referat für technologischen Datenschutz sowie Datensicherheit einrichten und ausbauen. Auch bauen wir unser IT-Labor sukzessive aus. Wir haben nun die Möglichkeit, Datenflüsse von Produkten und Anwendungen wie zum Beispiel digitalen Endgeräten und Apps dezidiert zu untersuchen. Diese Untersuchungsmöglichkeiten sind aus meiner Sicht ein essentieller Baustein, um die relevanten Datenflüsse vollständig und rechtlich fundiert bewerten zu können. Wir möchten sie noch im Jahr 2025 durch die Einrichtung eines KI-Reallabors ergänzen, damit KI-Systeme auch unter unserer aktiven Begleitung erprobt und anschließend datenschutzkonform in die reale Welt entlassen werden können.

Anknüpfend an unsere technische Pionierarbeit konnten wir auch den mir sehr wichtigen Bereich Strategic Foresights aufbauen. Im Rahmen mehrstufiger wissenschaftlicher Prozesse treffen wir uns regelmäßig mit internen wie externen Expertinnen und Experten, um uns mit relevanten Themen der Zukunft zu beschäftigen und frühzeitig datenschutzrechtliche Positionen zu erarbeiten. Hieran werden wir im kommenden Jahr anknüpfen und zu den Themen KI sowie Gesundheit Strategic Foresights durchführen. Ich bin der festen Überzeugung, dass wir mit den hieraus gewonnenen Erkenntnissen hilfreiche Leitlinien und Handlungsempfehlungen erarbeiten können, die bei zukunftsweisenden Themen frühzeitig für mehr Rechtssicherheit sorgen werden. Unsere Erkenntnisse werden wir zudem in interdisziplinären Fokusgruppen diskutieren und mittels empirischer Erhebungen verifizieren.

Lassen Sie uns abschließend einen Blick in die Zukunft wagen: Auch das kommende Jahr wird uns aus meiner Sicht rechtlich wie technisch vor datenschutzrechtliche und informationsfreiheitsrechtliche Herausforderungen stellen. Der Gesetzgeber wird insbesondere gefragt sein, die EU-Digitalrechtsakte national umzusetzen und zu harmonisieren sowie eine Antwort auf die drohenden Gefahren für Sicherheit, Demokratie und Zusammenhalt in unserer Gesellschaft zu finden.

Im Bereich Gesundheit empfehle ich die Schaffung eines Forschungsdatengesetzes. Exzellente wissenschaftliche Forschung ist auf qualitativ hochwertige Datengrundlagen angewiesen. Im Bereich Sicherheit ist zwingend

für eine europarechtskonforme Umsetzung der Aufsicht über die Bundespolizei zu sorgen. Meiner Behörde fehlen hier effektive Abhilfebefugnisse zur nachdrücklichen Rechtsdurchsetzung. Im Bereich KI empfehle ich die Schaffung von Rechtsgrundlagen zum Training von KI-Systemen.

Bei allen gesetzgeberischen Maßnahmen sollte der Gesetzgeber stets im Hinterkopf behalten, dass Datennutzbarkeit und Datenschutz nicht grundsätzlich im Widerspruch zueinanderstehen. Insbesondere die DSGVO ist niemals dafür angetreten, jegliche Datenverarbeitung zu verhindern, sondern steht für einen schonenden Grundrechtsausgleich. Sie definiert die grundlegenden Spielregeln, an die sich die Marktteilnehmer halten müssen. In einer Welt, die sich technisch rasant verändert, das gesellschaftliche und wirtschaftliche Verständnis von Freiheit und Selbstbestimmung zunehmend auseinanderfällt, digitale Monopole und Oligopole reifen, Vorboten einer zunehmenden De-Globalisierung sichtbar werden und die innere sowie äußere Sicherheit Deutschlands gefährdet ist, gilt es, den europäischen Freiheitsbegriff zu verteidigen und zu leben.

Wie Sie diesem Tätigkeitsbericht entnehmen können, hat sich meine Behörde auch im vergangenen Jahr wieder vielfältigen Aufgaben gestellt, um die Grundrechte der Bürgerinnen und Bürger zu schützen und unsere Freiheit zu verteidigen. Dies ist nur möglich durch die unermüdliche und engagierte Unterstützung meiner inzwischen rund 370 Mitarbeiterinnen und Mitarbeiter. Ich bedanke mich sehr herzlich bei ihnen allen für die vertrauensvolle, motivierende und stets konstruktive Zusammenarbeit.

Prof. Dr. Louisa Specht-Riemenschneider

2 Empfehlungen

2.1 Zusammenfassung der Empfehlungen des 33. Tätigkeitsberichts

Der Tätigkeitsbericht bezieht sich in großen Teilen auf den Zeitraum vor meinem Amtsantritt am 3. September 2024 und gibt damit auch auf Empfehlungen, die bereits vor meiner Amtsperiode ausgesprochen wurden. Andere sind maßgeblich seit dem 3. September 2024 entwickelt worden, so z. B. die Empfehlungen zur Einbindung meiner Behörde in die Umsetzung der KI-VO. Teilweise gehen meine Empfehlungen aber auch über die Arbeit der Fachebene hinaus und betreffen zukunftsgerichtete Aspekte. Zusammengefasst ergeben sich folgende Empfehlungen:

- Ich empfehle dem Gesetzgeber, die sich aus der KI-Verordnung der EU ergebende nationale KI-Aufsichtsstruktur möglichst zeitnah festzulegen und dabei die bei meiner Behörde vorhandene Expertise bestmöglich einzubeziehen. Nur so kann die Vorbereitung auf die komplexen mit der KI-Aufsicht einhergehenden Aufgaben gelingen und der Aufbau der erforderlichen Strukturen sichergestellt werden (s. Nr. 3.2.1).
- Ich empfehle dem Gesetzgeber, eine Rechtsgrundlage für das Training von KI zu schaffen, um hinreichend Rechtssicherheit für diese wichtige Zukunftstechnologie zu gewährleisten (s. Nr. 1).
- Wie bereits in meinem 32. Tätigkeitsbericht, empfehle ich dem Gesetzgeber, Abhilfebefugnisse auch im Bereich der Nachrichtendienste einzuführen (s. Nr. 3.3.1).
- Ich empfehle dem Gesetzgeber das Wiederaufgreifen mindestens der folgenden Gesetzgebungsvorhaben, wobei datenschutzrechtlich noch Nachschärfungen an den Gesetzesvorhaben erforderlich sind: Beschäftigtendatengesetz, Forschungsdatengesetz, Umsetzung der diversen EU-rechtlichen Gesetzgebungsakte mit daten- und datenschutzrechtlichem Bezug, BDSG-Novelle sowie SÜG-Novelle (s. Nr. 5.2.1, Nr. 5.3.1, Nr. 5.4.2, und Nr. 5.5.1).
- Ich empfehle die Zusammenlegung von Informationsfreiheitsgesetz und Umweltinformationsgesetz. Darüber hinaus empfehle ich die Weiterentwicklung zu einem Bundestransparenzgesetz mit proaktiven Veröffentlichungspflichten sowie Anordnungs- und Durchsetzungsbefugnisse für die Informationsfreiheitsbeauftragte, um im Konfliktfall handlungsfähig zu sein (s. Nr. 6.2.2).
- Ich empfehle der Bundesregierung und dem Gesetzgeber weiterhin, keine Parallelsysteme für den bereichsübergreifenden Datenaustausch und die Umsetzung des Once-Only-Prinzips zu schaffen. Stattdessen sollte mit Blick auf das bereits bestehende Fundament aus IDNrG, EGovG, OZG sowie dem NOOTS als zentraler Infrastruktur ein einheitlicher Ansatz verfolgt werden, bei dem für noch bestehende datenschutzrechtliche Probleme konstruktive Lösungen zu entwickeln sind (s. Nr. 7.2.1).
- Ich empfehle der Bundesregierung weiterhin, dem weiten Transparenzverständnis des Deutschen Bundestages im Rahmen der Verwaltungsdigitalisierung (siehe Ausschussdrucksache 20(4)258 vom 19. Juli 2023) Rechnung zu tragen und auch die erstmalige Einspeicherung der IDNr in ein Register gemäß § 2 Nr. 1 IDNrG im Datenschutzcockpit sichtbar zu machen. Zudem sollten frühzeitig die notwendigen Vorbereitungen getroffen werden, die (noch) mit der Steuer-ID versehenen Datenübermittlungen der Meldeämter transparent machen zu können, sobald diese in die IDNr umgewidmet wurde (s. Nr. 7.2.1).
- Ich empfehle dem Gesetzgeber, eine unverzügliche Meldepflicht für Sicherheitslücken mit dem Ziel der sofortigen Beseitigung an den Hersteller oder eine zentrale koordinierende Stelle gesetzlich zu verankern, um die IT-Sicherheit in Deutschland zu stärken (s. Nr. 7.2.4).

- → Ich empfehle dem Gesetzgeber, die Novellierung des FlugDaG unter Berücksichtigung der Vorgaben des EuGHs zügig abzuschließen (s. Nr. 7.4.3).
- → Für die datenschutzrechtliche Sicherheit und die Effizienz der Arbeit der Polizeibehörden empfehle ich, für das IT-Großprojekt Polizei 20/20 (P 20) klare gesetzliche Regelungen zu schaffen (s. Nr. 7.4.4).
- → Ich empfehle dem Deutschen Bundestag, gegenüber der Bundesregierung und dem EU-Gesetzgeber auf eine erhebliche, grundrechtskonforme Überarbeitung des Verordnungsentwurfs zur Chatkontrolle im Sinne des EP-Berichts von November 2023 zu drängen, der eine durchgehende Ende-zu-Ende-Verschlüsselung gewährleistet, ein Auslesen von Nachrichten auf dem Endgerät (Client-Side-Scanning) ausschließt, die deutschen und europäischen (Kommunikations-)Grundrechte wahrt und ein flächendeckendes und anlassloses Auslesen privater Kommunikation verbietet oder anderenfalls darauf hinzuwirken, den Verordnungsentwurf insgesamt abzulehnen (s. Nr. 7.3.8).
- → Ich empfehle dem Gesetzgeber, gemeinsam mit meiner Behörde und allen beteiligten Behörden über eine Reform der ATD und der RED zu sprechen (s. Nr. 8.1.3 – Kontrolle der ATD und RED).
- → Ich halte meine Forderung nach der Schaffung einer einfachgesetzlichen Rechtsgrundlage für das Militärische Nachrichtenwesen weiter aufrecht. Für die Handlungs- und zugleich Rechtssicherheit der Bundeswehr ist es erforderlich, notwendige Befugnisse in demokratisch legitimierten Gesetzen zu regeln (s. Nr. 8.1.7).

2.2 Empfehlungen des 32. Tätigkeitsberichts

	Empfehlungen des 32. Tätigkeitsberichts	Stand der Umsetzung
●	Die elektronische Gesundheitskarte (eGK) erhält durch das im Dezember 2023 beschlossene Digitalgesetz eine gesteigerte Bedeutung, weil das bloße Vorhandensein einer eGK in einer ärztlichen Praxis Zugriff zur elektronischen Patientenakte ermöglicht. Ich empfehle der Bundesregierung, eine Regelung zu treffen, dass eGKs nur sicher und persönlich zugestellt werden (32. TB Nr. 3.1.3).	Es wurde keine Regelung getroffen, die vorsieht, eGKs nur persönlich zuzustellen oder eGK-Besitzer nachträglich zu identifizieren.
●	Ich empfehle dem Gesetzgeber, die sich aus der KI-Verordnung der EU ergebende nationale KI-Aufsichtsstruktur zeitnah festzulegen und die dabei bei meiner Behörde vorhandene Expertise bestmöglich zu nutzen. Nur so kann die Vorbereitung auf die komplexen mit der KI-Aufsicht einhergehenden Aufgaben gelingen und der Aufbau der erforderlichen Ressourcen vor dem Inkrafttreten der Verordnung sichergestellt werden (32. TB Nr. 3.2.1).	Die KI-VO ist am 1. August 2024 in Kraft getreten. Zwar haben die Mitgliedstaaten bis zum 2. August 2025 Zeit, die nationalen Behörden zu benennen, die für den Vollzug der KI-VO zuständig sind. Allerdings werden bestimmte Bestimmungen der KI-VO, insbesondere über verbotene KI-Praktiken bereits am 2. Februar 2025 unmittelbar anwendbar. Außerdem bedürfen die Vorbereitung auf die neuen Aufgaben und der Aufbau der dafür erforderlichen Ressourcen eines Vorlaufs. Die Empfehlung, zeitnah eine nationale KI-Aufsichtsstruktur festzulegen, gilt deshalb umso dringender.

	Empfehlungen des 32. Tätigkeitsberichts	Stand der Umsetzung
🟡	Ich empfehle dem Deutschen Bundestag, gegenüber der Bundesregierung und dem EU-Gesetzgeber auf eine erhebliche, grundrechtskonforme Überarbeitung des VO-Entwurfs zur Chatkontrolle im Sinne des EP-Berichts von November 2023 zu drängen, der eine durchgehende Ende-zu-Ende-Verschlüsselung gewährleistet, die deutsche und europäische (Kommunikations-)Grundrechte wahrt und ein flächendeckendes und anlassloses Auslesen privater Kommunikation verbietet oder anderenfalls darauf hinzuwirken, den Verordnungsentwurf insgesamt abzulehnen (32. TB Nr. 3.2.4).	Die bisherige Empfehlung gilt weiter. Zwar hat die Bundesregierung im Rat der EU weiterhin keine Zustimmung zum VO-Entwurf erteilt, doch legt der Rat der EU regelmäßig neue Entwürfe vor, welche bisher nur wenige meiner Kritikpunkte berücksichtigen. Solange nicht alle Problemstellungen adressiert sind, halte ich an meiner Empfehlung fest: Eine durchgehende Ende-zu-Ende-Verschlüsselung muss gewährleistet bleiben, die deutschen und europäischen (Kommunikations-)Grundrechte müssen eingehalten werden und ein flächendeckendes und anlassloses Auslesen privater Kommunikation ist abzulehnen.
🔴	Ich empfehle, anstelle einer zunehmenden Zersplitterung des Sicherheitsüberprüfungsrechts in Einzeltatbestände ein schlüssiges Gesamtkonzept für alle Überprüfungsverfahren zu entwickeln. Hierzu bedarf es insbesondere einer Neudefinition und Ergänzung der sicherheitsempfindlichen Tätigkeit. Hierbei kann berechtigten Sicherheitsinteressen und zugleich dem Schutz betroffener und mitbetroffener Personen vor Überprüfungen auf Vorrat und Mehrfachüberprüfungen Rechnung getragen werden (32. TB Nr. 3.3.5).	Ein Gesetzesentwurf zur Änderung des Sicherheitsüberprüfungsgesetzes liegt vor. Im Rahmen des Gesetzgebungsverfahrens wurde jedoch kein schlüssiges Gesamtkonzept für alle Überprüfungsverfahren entwickelt.
🟡	Die reformierte eIDAS-Verordnung lässt Freiräume zur Ausgestaltung der nationalen, europäischen Brieftasche (EUDI-Wallet) zu. Ich empfehle der Bundesregierung, diese zu nutzen um Vorreiter in Europa zu werden mit einer Wallet-Infrastruktur, die auch vor Überidentifizierung schützt und Vorteile der Digitalisierung für die Datenminimierung nutzt (32. TB Nr. 3.4.1).	Zwar wurden Einzelentscheidungen zur deutschen EUDI-Wallet getroffen, für eine Bewertung des Gesamtbilds fehlen aber noch nationale Rechtsgrundlagen und Entscheidungen zur Ausgestaltung des Frontends für Bürgerinnen und Bürger.
🟡	Ich empfehle dem Gesetzgeber, in bereichsspezifischen Vorschriften klare Beschränkungen insbesondere hinsichtlich Zweck und Dauer einer elektronischen Weiterverarbeitung von Daten, die durch Polizei- und Verwaltungsbehörden aus dem Chip eines Passes oder Personalausweises ausgelesen wurden, festzulegen. Der Gesetzgeber sollte öffentlichen Stellen nur dann den Zugriff auf das biometrische Lichtbild im Chip eines Passes, Personalausweises oder elektronischen Aufenthaltstitels gestatten, wenn es für die Erfüllung besonders gewichtiger, im öffentlichen Interesse liegender Aufgaben zwingend notwendig ist und alternative, eingriffsmildere Verfahren nicht zur Verfügung stehen (32. TB Nr. 3.4.2).	Bisher hat der Gesetzgeber hier noch keine weiteren Schritte eingeleitet. Eine mögliche Gesetzgebung bleibt also noch abzuwarten.

	Empfehlungen des 32. Tätigkeitsberichts	Stand der Umsetzung
🟢	Ich empfehle der Bundesregierung, auf Nachbesserungen am Entwurf der Europäischen Kommission für eine Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO (COM(2023) 348 final) zu drängen, insbesondere durch verbindliche Vorgaben (einschließlich Fristen) für die federführende Aufsichtsbehörde zur beschleunigten Beschwerdebearbeitung in grenzüberschreitenden Fällen (32. TB Nr. 4.2.4).	Die Bundesregierung hat im Gesetzgebungsverfahren dazu beigetragen, dass in die allgemeine Ausrichtung des Rates erhebliche Verbesserungen aufgenommen wurden und sich dabei regelmäßig eng mit mir abgestimmt. Das Verfahren befindet sich nun im Trilog.
🟡	Ich empfehle der Bundesregierung, zeitnah einen Entwurf umfassender spezifischer Gesetzesregelungen zum Beschäftigtendatenschutz vorzulegen, etwa zum Einsatz von KI im Beschäftigungskontext, zu den Grenzen der Verhaltens- und Leistungskontrolle oder zum Umgang mit sensiblen Beschäftigtendaten. Berücksichtigt werden sollte dabei auch das Bewerbungs- und Auswahlverfahren (32. TB Nr. 5.2).	Die Bundesregierung hat ihre Arbeiten zu einem Beschäftigtendatenschutzgesetz fortgesetzt und einen Referentenentwurf eines Gesetzes zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt (Beschäftigtendatengesetz – BeschDG) vorgelegt. Das Gesetzgebungsverfahren wurde in der 20. Legislaturperiode jedoch nicht abgeschlossen.
🟡	Ich empfehle dem Deutschen Bundestag, sich selbst oder gegenüber der Bundesregierung für eine Gesetzesänderung des TTDSG einzusetzen, der meine Durchsetzungsbefugnisse verbessert, indem insbesondere eine Art. 27 DSGVO entsprechende Verpflichtung zur Benennung eines Vertreters in Deutschland in das TTDSG aufgenommen wird und eine Möglichkeit zur Durchsetzung gegenüber Niederlassungen von Diensteanbietern in Deutschland ergänzt wird (32. TB Nr. 5.5).	Die Empfehlung gilt für das TDDDG entsprechend und zunehmend dringlich, da viele nummernunabhängige interpersonelle Kommunikationsdienste (wie Messengerdienste) keinen Sitz in Deutschland, teilweise sogar keinen Sitz in der EU, haben.
🟡	Ich empfehle dem Gesetzgeber, die beschlossene Ausweitung der Videokonferenznutzung für mündliche Verhandlungen im Zivilprozess sowie verschiedener weiterer Fachgerichtsbarkeiten zeitnah zu evaluieren und bei Bedarf gesetzliche Ausnahmen vorzusehen, jedenfalls betreffend die Verhandlung über besonders sensible Daten gemäß Art. 9 Abs. 1 DSGVO. Dies gilt neben der Durchführung von Videokonferenzen insbesondere für deren mögliche Aufzeichnung zu Protokollzwecken (32. TB Nr. 5.8).	Der Gesetzgeber hat meine Hinweise aufgegriffen und entsprechende Ermessenserwägungen in der Gesetzesbegründung vorgesehen, welche den über die Durchführung von Videokonferenzen und deren Aufzeichnung zu Protokollzwecken entscheidenden Richterinnen und Richtern wichtige Orientierung geben können, um die Persönlichkeits- und Datenschutzrechte der Beteiligten zu wahren. Eine weitergehende Evaluation der Vorschriften und etwaige Ergänzung gesetzlicher Ausnahmetatbestände steht aber noch aus.

	Empfehlungen des 32. Tätigkeitsberichts	Stand der Umsetzung
🟡	Zudem fehlt es für die Teilnahme an gerichtlichen Videokonferenzen weiterhin an einer abschließenden Regelung zur sicheren elektronischen Identifikation der Verfahrensbeteiligten. Ich empfehle dem Gesetzgeber daher, die bestehende Regelungslücke zeitnah zu schließen und dabei auf das derzeit teilweise vorgesehene Video-Ident-Verfahren zu verzichten. Dieses birgt hohe Risiken und darf für Verfahren mit sehr hohem Schutzbedarf nicht genutzt werden (32. TB Nr. 5.8).	Der Gesetzgeber hat meine Hinweise aufgegriffen. Diese sollen im Zuge der laufenden Untersuchung zur Einführung einer sogenannten „Justizcloud“ geprüft werden. Diese ist Bestandteil der Digitalstrategie der Bundesregierung.
🔴	Ich empfehle die Zusammenlegung von Informationsfreiheitsgesetz und Umweltinformationsgesetz. Darüber hinaus empfehle ich die Weiterentwicklung zu einem Bundestransparenzgesetz mit proaktiven Veröffentlichungspflichten sowie Anordnungs- und Durchsetzungsbefugnisse für den Informationsfreiheitsbeauftragten, um im Konfliktfall handlungsfähig zu sein (32. TB Nr. 6.1.1).	Das BMI hat im Rahmen des BfDI-Symposiums zur Informationsfreiheit im Herbst 2023 über die Planungen und Überlegungen für ein Bundestransparenzgesetz berichtet. In der 20. Wahlperiode hat die Bundesregierung keinen Gesetzesentwurf vorgelegt. Ich empfehle auch für die 21. Wahlperiode, das Informationsfreiheitsgesetz zu einem Transparenzgesetz weiterzuentwickeln.
🔴	Soweit der Einsatz komplexer Datenanalysemethoden durch die Polizei und Nachrichtendienste für erforderlich erachtet wird, empfehle ich der Bundesregierung, klare Rechtsgrundlagen und geeignete Rahmenbedingungen dafür zu schaffen (vgl. auch DSK-Entschließung vom 11. Mai 2023) (32. TB Nr. 7.1).	Diese Empfehlung ist jedenfalls für den Bereich der Nachrichtendienste noch nicht umgesetzt. Das BVerfG hat im Februar 2023 zu den gesetzlichen Voraussetzungen für polizeiliche automatisierte Datenanalysen geurteilt und allgemeingültige Maßstäbe aufgestellt. Diese gelten im Grundsatz für die Nachrichtendienste genauso. Im Nachrichtendiensterecht fehlen bislang konkrete gesetzliche Befugnisse für derartige Datenverarbeitungen.
🔴	Ich empfehle, in dem für das Jahr 2024 geplanten zweiten Teil der Reform des Nachrichtendienstrechts für die Datenerhebung aus dem Internet und deren Weiterverarbeitung durch die Dienste genaue Vorgaben im Gesetz zu schaffen (32. TB Nr. 7.3).	Die Bundesregierung hat keinen Gesetzesentwurf in der 20. Wahlperiode vorgelegt. Der Tiefe des Eingriffs angemessen sollte eine spezielle und normenklare gesetzliche Grundlage geschaffen werden.
🟡	Ich empfehle dem Gesetzgeber, das Fluggastdatengesetz im Lichte der EuGH-Entscheidung zu überarbeiten. Es ist wichtig, Bürgerinnen und Bürgern, Verwaltung und Gerichten klare Regelungen an die Hand zu geben (32. TB Nr. 7.6).	Die Bundesregierung hat die geforderte Novellierung des Fluggastdatengesetzes zwar angestoßen, aber noch nicht abgeschlossen.

	Empfehlungen des 32. Tätigkeitsberichts	Stand der Umsetzung
🔴	Ich empfehle dem Gesetzgeber, Abhilfebefugnisse auch im Bereich der Nachrichtendienste einzuführen (32. TB Nr. 7.9).	Meine Empfehlung wurde nicht aufgegriffen. Nach geltendem Recht kann die Rechtmäßigkeit von Datenverarbeitungen durch Nachrichtendienste nur in Sonderfällen gerichtlich überprüft werden. Mit der Einführung von Anordnungsbefugnissen würde der Gesetzgeber die Möglichkeit schaffen, Datenverarbeitungen einer gerichtlichen Klärung zuzuführen.
🔴	Ich empfehle dem Gesetzgeber, eindeutige und umfassende Regelungen zur Zusammenarbeit der Aufsichtsorgane über die Nachrichtendienste zu schaffen (32. TB Nr. 7.12).	Wenn und weil die Aufsicht über die Nachrichtendienste auf verschiedene Institutionen verteilt ist, sollten diese für eine lückenlose und effektive Kontrolle auch normenklare und umfassende gesetzliche Grundlagen haben, um sich über ihre Tätigkeiten auszutauschen. Dies gebietet schon die „Waffengleichheit“ gegenüber den beaufsichtigten Stellen, die ansonsten immer behaupten könnten, dass ein Sachverhalt in die Zuständigkeit einer anderen Aufsichtsbehörde falle.
🟡	Werden Verwaltungsleistungen elektronisch angeboten, sollten die zuständigen Behörden in einem abgestuften Verfahren zunächst prüfen, ob die Leistung nicht auch ohne ein Nutzerkonto in Anspruch genommen werden kann. Ist ein Nutzerkonto erforderlich, sollte weiter geprüft werden, ob eine einfache Basisregistrierung ohne Authentifizierung mit der eID des Personalausweises ausreichend ist. Ich empfehle dem BMI und dem BMF, die Frist für die Verwendung von ELSTER-Softwarezertifikaten als Identifizierungsmittel in der BundID und im Organisationskonto nicht zu verlängern. Für das Organisationskonto sollte die Entwicklung geeigneter, ausreichend sicherer Identifizierungsmittel forciert werden (32. TB Nr. 8.1).	Im parlamentarischen Verfahren hat der Gesetzgeber die Verwendung von Elster-Softwarezertifikaten als Identifizierungsmittel auch für Verwaltungsleistungen, die das Vertrauensniveau „substantiell“ erfordern, dauerhaft zugelassen. In der Folge sind die Elster-Softwarezertifikate so weiterzuentwickeln, dass sie durchgehend den europäischen Vorgaben für Identifizierungsmittel auf dem Sicherheitsniveau substantiell genügen.
🟢	Ich empfehle dem Gesetzgeber, die so genannte Once-Only-Generalklausel (Entwurf von § 5 EGovG) so auszugestalten, dass alle darauf basierenden Übermittlungen von Nachweisen bei Nutzung der ID-Nummer im Datenschutzcockpit angezeigt werden müssen (32. TB Nr. 8.2).	Die Empfehlung wurde mit dem jetzt gültigen § 5 Abs. 3 EGovG vollumfänglich erfüllt. Der Gesetzgeber ging sogar noch darüber hinaus und erfasste nicht nur die Übermittlungen anhand der IDNr, sondern alle. Ganz gleich ob oder welchen Identifikator sie nutzen. Nicht aufgegriffen hat der Gesetzgeber, dass der Anschluss an das Datenschutzcockpit zur Rechtmäßigkeitsvoraussetzung für die betreffenden Übermittlungen sein sollte.

	Empfehlungen des 32. Tätigkeitsberichts	Stand der Umsetzung
🟡	Ich empfehle, sowohl den Abruf von Daten durch das Bundesverwaltungsamt vom Bundeszentralamt für Steuern als auch die Ersteinspeicherung von Daten bei den einzelnen Registern als Übermittlung im Sinne von § 9 IDNrG zu betrachten und deshalb im Datenschutzcockpit anzuzeigen (32. TB Nr. 8.2).	Durch eine Änderung des § 10 Abs. 2 OZG wurde diese Empfehlung vom Gesetzgeber zumindest teilweise umgesetzt. Es ist nunmehr klargestellt, dass auch die Übermittlungen zwischen BVA und BZSt auf Grundlage des IDNrG im Datenschutzcockpit transparent zu machen sind. Eine weitergehende, rechtliche Klarstellung, ob auch die Fälle des erstmaligen Abrufs der IDNr aus dem BZSt insofern anzuzeigen sind, blieb leider aus. Auch hat sich die Bundesregierung weiterhin nicht zu dieser bürgerfreundlichen Auslegung auf Grundlage des bereits geltenden Rechts bekannt. Hier sollte die Bundesregierung eine der letzten Transparenzlücken im IDNrG schließen.
🔴	Ich empfehle außerdem allen Ressorts sowie dem Gesetzgeber, bei der Verwendung der ID-Nummer oder der Steuer-ID durch Stellen außerhalb der Finanzverwaltung wenigstens die Sicherungen des IDNrG – insbesondere das Datenschutzcockpit – vorzusehen. Das Schutzniveau des IDNrG darf nicht zusätzlich dadurch unterlaufen werden, dass Stellen, die keine Finanzbehörden sind, gesetzlich zu solchen erklärt werden (32. TB Nr. 8.2).	Auch wenn einige entsprechende Gesetzesvorhaben scheiterten (z. B. Kindergrundsicherung), kann dennoch weiterhin ein generelles Interesse daran beobachtet werden, personenbezogene Daten außerhalb des Systems des IDNrG dauerhaft miteinander zu verknüpfen, teilweise unter Einsatz der nur rechtlich unterscheidbaren, aber inhaltlich völlig identischen Steuer-ID. Gesetzgeber und Bundesregierung sollten hiervon abkehren und sich deutlich für die Schaffung eines einheitlichen Once-Only-Systems aussprechen, an dem, trotz der noch bestehenden Probleme, gemeinsam effektiv gearbeitet werden kann.
🟡	Ich empfehle der Bundesregierung, sich bei der Diskussion um eine Vorratsdatenspeicherung für eine grundrechtsschonende Balance aus Freiheit und Sicherheit einzusetzen (32. TB Nr. 8.3).	Der EuGH hat entschieden, dass eine auf das absolut notwendige Maß begrenzte allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen nicht grundsätzlich unzulässig ist, aber unter hohen Voraussetzungen steht. Auf europäischer Ebene veröffentlichte die High-Level Group (HLG) on access to data for effective law enforcement im Sommer 2024 ein Empfehlungspapier, das u. a. europaweit einheitliche Maßstäbe für eine weitgehende Vorratsdatenspeicherung fordert. Auf nationaler Ebene gibt es einen intensiven politischen Diskurs, ob und gegebenenfalls wie mögliche Spielräume einer Speicherung von IP-Adressen genutzt werden können. Zu meiner Position und zur Erläuterung der Vorgaben des EuGH siehe die Beiträge Nr. 3.3.4 sowie 4.5.3.

	Empfehlungen des 32. Tätigkeitsberichts	Stand der Umsetzung
●	In Anbetracht der unmittelbar bevorstehenden Aufnahme des Regelbetriebs empfehle ich der Bundesregierung, endlich eine unabhängige Registerstelle für das Implantateregister zu schaffen (32. TB Nr. 8.14).	Der Gesetzgeber bzw. das BMG hat keine unabhängige Registerstelle für das Implantateregister geschaffen. Diese liegt weiterhin beim BMG.
●	Ich empfehle dem Gesetzgeber, die Speicherfristen für das steuerliche Identifikationsmerkmal gemäß § 139a AO (Steuer-ID) in der beim Bundeszentralamt für Steuern geführten Datenbank zu evaluieren und diese insbesondere mit Blick auf die zunehmende Nutzung der Steuer-ID im Kontext der Registermodernisierung angemessen festzusetzen (32. TB Nr. 9.2.3).	Der Gesetzgeber hat meine Empfehlung aus dem 32. TB, die Speicherfristen betreffend das steuerliche Identifikationsmerkmal zu evaluieren und insbesondere mit Blick auf dessen fortschreitende Nutzung im Kontext der Registermodernisierung angemessen festzusetzen, bislang nicht aufgegriffen.

3 Schwerpunktthemen

3.1 Gesundheit

3.1.1 Forschungsdatenzentrum Gesundheit

Die Inbetriebnahme des Forschungsdatenzentrums Gesundheit steht kurz bevor. Im Berichtsjahr hat es nicht zuletzt wegen diverser gesetzlicher Neuerungen engen Austausch zwischen den Verantwortlichen und mir gegeben. Hierbei stand insbesondere die Transparenz der zu verarbeitenden Daten im Vordergrund.

Das Vorhaben eines Forschungsdatenzentrums für Gesundheitsdaten (FDZ), einer beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) als Registerstelle geführten Datenbank, mit den pseudonymisierten Abrechnungsdaten aller gesetzlich Versicherten, nimmt weiter Gestalt an und nähert sich einem Meilenstein. Ab Frühjahr 2025 soll es möglich sein, mittels Abrechnungsdaten, die auf Grundlage der Datentransparenzverordnung von den Krankenkassen an das BfArM übermittelt werden, Forschung zu betreiben.

Über die Entwicklung des FDZ habe ich bereits in den vergangenen Jahren berichtet.[1] Das Inkrafttreten des Gesundheitsdatennutzungsgesetzes (GDNG) im März 2024[2] führte zu umfangreichen Anpassungen in den maßgeblichen §§ 303a bis 303e SGB V. Für die Antragsberechtigung ist danach nicht mehr entscheidend, wer den Antrag stellt, sondern der Zweck, für den der Antrag gestellt wird. Dieser muss für eine positive Antragsbescheidung dem in § 2 GDNG definierten Gemeinwohl dienen. Weitere wesentliche Rechtsgrundlage für das FDZ ist das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG),[3] welches ebenfalls seit März 2024 in Kraft ist. Durch das DigiG ist die ePA seit Anfang des Jahres 2025 für alle gesetzlich Versicherten, die nicht wiedersprechen, eingerichtet.

Dies ist für die Datenübermittlung an das FDZ eine wesentliche Erneuerung. Relevant ist außerdem die European Health Data Space Verordnung (EHDS).[4] Danach sollen künftig Forschende, Innovatoren und öffentliche Einrichtungen über ein europaweit einheitliches System einen Antrag auf die Nutzung von anonymen und pseudonymen Gesundheitsdaten stellen können, um diese für bestimmte, gesetzlich festgelegte Zwecke zu nutzen. Das FDZ, auf internationaler Ebene „Health Data Lab“ (HDL), ist am Pilotprojekt zur Ermöglichung und zum Aufbau eines solchen europaweiten Systems beteiligt. Im Rahmen des Pilotprojektes sollen verschiedene beteiligte Datenräume miteinander vernetzt werden. So soll Forschenden ermöglicht werden, über Landesgrenzen hinweg die Metadaten der Zentren zu durchsuchen, die benötigten Daten mithilfe eines einheitlichen Formulars zu beantragen und diese anschließend zu analysieren.

Auch in diesem Berichtsjahr habe ich die Arbeiten des BfArM eng begleitet und durch regelmäßige Austauschtermine auf die Beachtung datenschutzrechtlicher Grundlagen hingewirkt. Aufgrund des konstruktiven Austauschs konnte ich – ohne die Forschungsfunktionalität zu gefährden – sicherstellen, dass insbesondere die Grundsätze der Vertraulichkeit und Datenminimierung beachtet werden. Ein zentrales Element für die sichere Bereitstellung der Daten zu Forschungszwecken ist etwa ein geeignetes Anonymisierungsverfahren, das speziell auf die Struktur der Daten abgestimmt ist. Mittels dieses Verfahrens wurde in diesem Jahr das sogenannte Public Use File (PUF) erstellt und auf der Website des BfArM veröffentlicht. Das PUF ist für Forschende eine erste Anlaufstelle zur Prüfung, inwieweit ihre Forschungsfragen mit Hilfe der im FDZ vorhandenen Daten bearbeitet werden können. So können Forschende unter anderem Abfragen (Skripte) erstellen und auf ihre Validität prüfen, da die Dateistruktur des

1 31. TB Nr. 4.1.2
2 32. TB Nr. 3.1.2
3 32. TB Nr. 3.1.3
4 32. TB Nr. 3.1.1

PUF der Struktur der Originaldaten entspricht.[5] Aufgrund der Sensibilität der Gesundheitsdaten ist grundsätzlich eine vollständige Anonymisierung der Daten erforderlich. Das BfArM hat zu diesem Zweck ein überzeugendes Anonymisierungsverfahren vorstellen und umsetzen können. Tiefergehende Forschungsfragen können von Forschenden dann in einem streng geregelten Antragsverfahren eingereicht werden. Bei positiver Antragsbescheidung können die Forschenden mit Echtdaten, die auf ihre spezifischen Forschungsfragen zugeschnitten sind und die erforderlichen datenschutzrechtlichen Hürden genommen haben, Antworten auf diese Fragen suchen. Hierzu wurden gemeinsam mit dem BfArM technische und organisatorische Maßnahmen entwickelt.

Neben dem PUF betreibt das BfArM auch ein sogenanntes Statistikportal. Hierbei handelt es sich um eine Webanwendung, die stark vergröberte und aggregierte Daten des FDZ für Forschende und die interessierte Öffentlichkeit kostenlos bereitstellt. Auch hier habe ich das BfArM beraten, wie die Daten aufzubereiten sind, um sowohl eine zufriedenstellende Darstellung zu erhalten als auch das Reidentifikationsrisiko der Versicherten auf ein minimales Niveau zu reduzieren.

Neben dem BfArM habe ich außerdem das Robert-Koch-Institut, als Betreiber der Vertrauensstelle, und das Bundesministerium für Gesundheit, als Aufsichtsbehörde des BfArM, beraten.

Ich bin zuversichtlich, dass das FDZ zeitnah gewinnbringende Forschung unter gleichzeitiger Wahrung des Datenschutzes ermöglichen wird. Trotzdem bestehen noch Herausforderungen und offene Fragen. So stellt sich etwa die Frage, wie Anträge aus Drittstaaten mit oder ohne Niederlassung im europäischen Wirtschaftsraum datenschutzrechtlich gesichert bewilligt werden können. Die besondere Herausforderung besteht hier in der Ausarbeitung eines einheitlichen, niedrigschwelligen und dem hohen Vertrauensniveau genügenden Identifizierungsverfahren der Antragsstellenden. Ich stehe mit dem BfArM in einem engen Austausch hinsichtlich der Ausarbeitung möglicher Verfahrensoptionen, die dem europäischen datenschutzrechtlichen Sicherheitsstandard genügen müssen.

3.1.2 Taskforce Forschungsdaten

Die Nutzung von Gesundheitsdaten für Forschungszwecke stand auch im Jahr 2024 im Zentrum der politischen und wissenschaftlichen Diskussion.

Die Taskforce Forschungsdaten (TFFD) der DSK unter gemeinsamen Vorsitz meiner Behörde und des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) wurde durch Festlegung der 102. DSK im November 2021 als Fachgremium gegründet. Ziel ist die flexible und zeitnahe Möglichkeit zur Bearbeitung von auch kurzfristig auftretenden datenschutzrechtlichen Fragen der Forschung im Gesundheitsbereich sowie die Vorbereitung und gemeinsame Abstimmung entsprechender Veröffentlichungen für die DSK.

Im Berichtsjahr hat sich die TFFD insbesondere mit den Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken beschäftigt und herausgearbeitet, welche datenschutzrechtlichen Anforderungen der deutsche und der europäische Gesetzgeber bei der Regelung der Verarbeitung dieser Daten zu beachten haben.

Weitere Arbeitsschwerpunkte waren die Neuregelungen des Gesundheitsdatennutzungsgesetzes zur länderübergreifenden Verbundforschung und die komplexen Vorschriften zur Zuständigkeit der Datenschutzaufsichtsbehörden.

Zudem hat sich die TFFD intensiv mit den Anforderungen an Datenübermittlungen in Drittländer (außerhalb der EU/des EWR) zu wissenschaftlichen Forschungszwecken befasst. Für die wissenschaftliche Forschung spielt die internationale Zusammenarbeit eine immer wichtigere Rolle. Falls im Rahmen von internationalen Forschungskooperationen personenbezogene Daten in Drittländern verarbeitet werden, müssen insbesondere auch die Anforderungen des Kapitels V der DSGVO zur Übermittlung von personenbezogenen Daten in Drittstaaten beachtet werden.

3.1.3 European Health Data Space

Nachdem ich bereits im 31. und 32. Tätigkeitsbericht über die datenschutzrechtlichen Herausforderungen des European Health Data Space (EHDS) berichtet habe,[6] befindet sich das Gesetzgebungsverfahren nunmehr auf der Zielgeraden.

Die EU-Kommission hat im Mai 2022 ihren Vorschlag zum EHDS veröffentlicht. Mit dem EHDS soll ein rechtlicher Rahmen für die Bereitstellung und Nutzung von Daten in der Gesundheitsversorgung (Primärnutzung) sowie für Forschung, Innovation, Politikgestaltung und Steuerung der Gesundheitsversorgung geschaffen werden (Sekundärnutzung) – sowohl innerhalb der EU-Mitgliedstaaten als auch grenzüberschreitend.

5 Github-Seite des BfArM zum PUF: https://github.com/FDZ-Gesundheit/Public-Use-File
6 31. TB Nr. 5.1, 32. TB Nr. 3.1.1

Nach mehrmonatigen Verhandlungen in der Ratsarbeitsgruppe „Öffentliche Gesundheit“ und der entsprechenden inhaltlichen Befassung durch das Europäische Parlament, fanden im 1. Quartal 2024 insgesamt vier politische Triloge statt. Am 22. März 2024 stimmte der Ausschuss der Ständigen Vertreter dem finalen Gesamtkompromisstext des EHDS mehrheitlich zu. Das Europäische Parlament hat den noch unredigierten Text am 24. April 2024 angenommen. Die nunmehr sprachjuristisch redigierte Verordnung soll nach erneuter Annahme durch den Rat der Europäischen Union und das Europäische Parlament im 1. Quartal 2025 in Kraft treten.

Aus Sicht des Datenschutzes weist das im Trilog erzielte Ergebnis deutliche Verbesserungen gegenüber dem Ursprungsentwurf der EU-Kommission auf. Damit wurden wichtige Empfehlungen des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten aus ihrer gemeinsamen Stellungnahme vom 12. Juli 2022 wie auch diverse darüber hinaus gehende Forderungen meines Hauses umgesetzt.

So können die Mitgliedstaaten durch eine Öffnungsklausel national ein Widerspruchsrecht für ihre Bürgerinnen und Bürger für den Bereich der Primärnutzung ihrer Gesundheitsdaten festlegen. Dies hat Deutschland im Hinblick auf die elektronische Patientenakte mit dem Digital-Gesetz eingeführt.

Krankenkassen und private Versicherungen dürfen über den EHDS keinen Zugriff auf persönliche elektronische Gesundheitsdaten erhalten.

Bei der Sekundärnutzung von Gesundheitsdaten gewährt der EHDS den Bürgerinnen und Bürgern das unmittelbare Recht, der Nutzung ihrer Daten zu widersprechen.

Weitere auf nationalem oder Unionsrecht basierende Systeme für den Datenzugang von öffentlichen Stellen oder privaten Institutionen mit öffentlicher Aufgabe können ebenso erhalten bleiben wie Mechanismen, die eine Sekundärnutzung auf vertraglicher Basis vorsehen, wie beispielsweise die NAKO Gesundheitsstudie oder die Medizininformatik-Initiative.

Im Bereich der Primär- und Sekundärnutzung von genetischen Daten und Biobanken erlauben Öffnungsklauseln im EHDS den Mitgliedstaaten, höhere Anforderungen an die Rechtmäßigkeit der Verarbeitungen national zu regeln. Hiervon hat Deutschland im Gendiagnostikgesetz und im Gesundheitsdatennutzungsgesetz Gebrauch gemacht und das Erfordernis der Einwilligung durch die Betroffenen für die Verarbeitung ihrer genetischen Daten normiert.

Zudem wurden diverse Definitionen im EHDS in Einklang mit der DSGVO gebracht und die Rolle der datenschutzrechtlichen Aufsichtsbehörden gestärkt, indem die digitale Gesundheitsbehörde und die Zugangsstelle(n) verpflichtet werden, mit ihnen zusammenzuarbeiten.

Bedauerlicherweise gibt es jedoch auch datenschutzrechtliche Empfehlungen, die keinen Einzug in den EHDS gefunden haben.

Die Empfehlung, Hersteller von Electronic Health Record-Systemen wie der elektronischen Patientenakte zu verpflichten, diese von unabhängigen Stellen zertifizieren zu lassen, wurde nicht aufgegriffen. Es verblieb vielmehr bei den Regelungen aus dem Ursprungsentwurf der EU-Kommission zur Selbstzertifizierung unter bestimmten Auflagen.

Eine weitere Empfehlung war, Daten aus Wellness-Apps von der Sekundärnutzung auszuschließen. Auch dem wurde nicht gefolgt, jedoch können die Mitgliedstaaten aufgrund einer Öffnungsklausel strengere Anforderungen an den Zugang zu Daten aus solchen Apps national regeln.

Nach In-Kraft-Treten des EHDS mit den entsprechenden Implementierungsfristen für die Mitgliedstaaten, werde ich die weitere nationale Durchführung konstruktiv begleiten und darauf hinwirken, dass dieses wichtige Digitalisierungsprojekt das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung wahrt.

3.1.4 Die neue ePA auf Widerspruchsbasis

Die neugestaltete elektronische Patientenakte (ePA) kann Versicherten echte Vorteile der Digitalisierung bringen. Die Umstellung auf Widerspruch statt Einwilligung verpflichtet die Verantwortlichen, alle Betroffenen korrekt und verständlich über ihre Rechte aufzuklären. Die neue Systematik für Zugriffsrechte erschwert das Verbergen einzelner Diagnosen.

Im März 2024 wurde das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) im Bundesgesetzblatt verkündet. In meinem vorherigen Tätigkeitsbericht hatte ich über meine Beratung der Bundesregierung und des Gesetzgebers im parlamentarischen Verfahren zu diesem Gesetz berichtet. Eine digitalisierte, zentrale Akte kann Versicherten Überblick und Kontrolle über ihre Gesundheitsdaten geben und potentiell Doppeluntersuchungen vermeiden.

Durch das Gesetz wird die bereits seit mehreren Jahren existierende ePA, die Versicherte auf Antrag erhalten, durch eine widerspruchsbasierte ePA ersetzt. Seit dem 15. Januar 2025 erhalten alle Versicherte von ihrer Krankenkasse die ePA, wenn sie nicht widersprechen. Nachdem dieser Wechsel politisch beschlossen ist, ist es wichtig, dass die Versicherten über ihre Rechte zum

Widerspruch richtig informiert werden, damit diese tatsächlich für die Entscheidung über den Widerspruch befähigt sind. Dazu habe ich die unter meiner Datenschutzaufsicht stehenden Krankenkassen auf ihre Informationspflichten hingewiesen[7]: Widerspruch gegen die Einrichtung der ePA kann mittels sämtlicher Kommunikationskanäle (postalisch, telefonisch, elektronisch, App-gestützt, usw.) durch die Versicherten den Krankenkassen erklärt werden. In der Information über das Bestehen des Widerspruchsrechts darf dabei nicht der Eindruck erweckt werden, der Widerspruch könne nur auf einem Wege, beispielsweise nur online, eingelegt werden.

Außerdem wurden im Gesetz Grundlagen dafür geschaffen, Funktionen in der ePA über eine Dokumentensammlung hinaus zu schaffen. Mit der Einführung von Anwendungsfällen, die auf strukturierten Daten arbeiten, könnten Versicherte mehr Vorteile der Digitalisierung erfahren. Der erste dieser Anwendungsfälle, mit dem die neue ePA im Januar 2025 gestartet ist, ist die digitale Unterstützung des Medikationsprozesses. Dabei wird der E-Rezepte-Fachdienst, also der zentrale Speicher aller E-Rezepte, an die ePA angebunden und Daten zu ausgestellten Rezepten automatisch in die ePA kopiert. Dort werden sie zu einer Medikamentenliste aufbereitet. Bei Versicherten, die nach § 31a Abs. 1 S. 1 SGB V Anrecht auf einen Medikationsplan haben, kann dieser in elektronischer Form in der ePA geführt und mit der Medikamentenliste verknüpft werden. Überraschend könnte hier für Betroffene sein, dass ein Rezept, das sie aus dem E-Rezept-Fachdienst löschen, weil sie es beispielsweise nicht einlösen wollen, in der ePA erhalten bleibt. Es kann dort auch nicht einzeln gelöscht werden. Die Benutzerführung sollte daher so gestaltet werden, dass Versicherte in jeder Situation verstehen, welche Konsequenzen ihre Handlungen haben. Es ist seitens gematik geplant, ab 2026 weitere Anwendungsfälle zu definieren wie etwa digitale Unterstützung für die Verarbeitung von Ergebnissen aus Laboruntersuchungen.

Auf die widerspruchsbasierte ePA ab 2025 werden automatisch mehr ärztliche Praxen oder Apotheken Zugriff

Eine Übersicht über die verschiedenen Widerspruchsmöglichkeiten bietet die nachstehende Tabelle:

Widerspruch gegen…	Krankenkasse	Leistungserbringer	Ombudsstelle	ePA-App	Rechtsgrundlage SGB V
die Anlage der ePA	x				§ 342 Abs. 1 S. 2
eine existierende ePA	x		x	x	§ 344 Abs. 3 S. 1 und 2
Zugriff auf die ePA durch bestimmte Leistungserbringer			x	x	§ 353 Abs. 2
Einstellen von Behandlungsdaten insb. potentiell diskriminierender Daten		x			§ 346 Abs. 2, § 347 Abs. 1 und 2, § 348 Abs. 1 und 3 sowie § 349 Abs. 2
Verarbeitung von Daten für Anwendungsfälle (wie Medikationsprozess)			x	x	§ 353 Abs. 1 S. 1 und 2
Zugriff auf Daten in Anwendungsfällen durch bestimmte Leistungserbringer				x	§ 353 Abs. 1 S. 3 und 4
Datenübermittlung an das Forschungsdatenzentrum			x	x	§ 363 Abs. 5
Einstellen von Abrechnungsdaten der Krankenkassen	x			x	§ 350 Abs. 1 S. 2 und 3

7 Rundschreiben vom 15. Oktober 2024, sowie vom 26. November 2024, abrufbar unter: www.bfdi.bund.de/rundschreiben

haben. Gleichzeitig werden Daten ohne aktive Zustimmung der Versicherten in die ePA geladen. Das bedeutet, dass in der Grundeinstellung möglicherweise ein großer Personenkreis Zugang zu sensiblen Daten hat. Es gibt zwar begrenzte Einstellmöglichkeiten, um die Sichtbarkeit zu steuern. Diese setzen aber grundsätzlich eine hohe Digitalaffinität und aktiven Einsatz der Versicherten voraus. Sobald die Daten in einem Anwendungsfall verarbeitet werden, können sie nicht mehr einzeln verborgen werden. Ein einzelnes Rezept, aus dem sich eine potentiell stigmatisierende Diagnose ableiten lässt, kann beispielsweise nicht in der Medikationsliste verborgen werden. Um diese Diagnose zu verbergen, muss die betroffene Person in diesem Fall auf die Vorteile der digitalen Unterstützung des Medikationsprozesses ganz verzichten. Deshalb wäre es besser, wenn potentiell stigmatisierende Diagnosen nicht ohne aktive Zustimmung der Versicherten in die ePA gelangten.

Grundsätzlich haben Versicherte das Recht, der Anlage einer ePA jederzeit zu widersprechen: eine existierende ePA wird daraufhin gelöscht. Versicherte können auch dem Zugriff einzelner Leistungserbringer auf die ePA widersprechen. Außerdem können Versicherte gegen die Teilnahme an den einzelnen Anwendungsfällen Widerspruch einlegen. Der erste Anwendungsfall, der umgesetzt wird, ist die Unterstützung des Medikationsprozesses mit der Medikationsliste. Betroffene können auch nur widersprechen, dass bestimmte Leistungserbringer Daten aus den Anwendungsfällen verarbeiten – das allerdings nur über die ePA-App. Ab Juli 2025 muss die ePA in der Lage sein, pseudonymisierte Daten an das Forschungsdatenzentrum auszuleiten. Auch diese Funktion ist standardmäßig aktiviert und Versicherte können ihr widersprechen.

Die Krankenkassen müssen Ombudsstellen einrichten, um Versicherte bei Anliegen um die ePA zu unterstützen. Dort können auch Protokolle der Nutzung/Zugriffe auf die ePA angefordert und Widersprüche gegen die ePA oder einzelne Funktionen eingereicht werden. Für Versicherte, die keine eigene ePA-App benutzen, ist das ein wichtiger Schritt. Es ist nicht möglich, in der Ombudsstelle Einsicht in die Inhalte der ePA zu nehmen, die Zugriffsrechte auf einzelne Dateien (feingranular) einzustellen oder dem Zugriff eines bestimmten Leistungserbringers auf einen Anwendungsfall zu widersprechen.

Ich sehe bei den Einstellmöglichkeiten gerade für weniger digitalaffine Menschen ohne eigene App noch Verbesserungsbedarf.

Querverweis:

7.1.1 Authentifizierungsmöglichkeiten der gesetzlich Versicherten

3.2 Künstliche Intelligenz

3.2.1 KI-Verordnung

Am 1. August ist die Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (KI-VO) der EU in Kraft getreten. Die KI-VO stellt umfassende Regeln für KI-Systeme auf, welche die Einhaltung der Grundrechte gewährleisten und gleichzeitig Innovation fördern sollen. Viele der Vorgaben für Hochrisiko-KI-Systeme haben einen engen Bezug zum Datenschutzrecht. Noch nicht abschließend geklärt ist die Einbindung der Datenschutzaufsichtsbehörden in die Aufsichtstätigkeit der Bundesnetzagentur.

Ich begrüße die KI-Verordnung als einen wichtigen Grundstein für den Schutz der Grundrechte und Freiheiten sowie für die Innovationsförderung. Viele der Forderungen aus der gemeinsamen Stellungnahme des Europäischen Datenschutzausschusses (EDSA) und des Europäischen Datenschutzbeauftragten (European Data Protection Supervisor) im Jahr 2021 sind in der Verordnung berücksichtigt worden. Insbesondere die Verbote des Profilings im Hinblick auf künftige Straftaten und der Nutzung von KI zur Bewertung sozialen Verhaltens („Social Scoring“) sowie die Einschränkung der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme im öffentlichen Raum stärken den Schutz der Grundrechte.

Als für den Schutz von Grundrechten zuständige Behörde weist die KI-VO auch mir neue Aufgaben und Befugnisse zu. Beispielsweise erhält mein Haus zukünftig Zugriff auf die für die Erfüllung meiner Aufgaben erforderlichen Dokumente, die zur Einhaltung der KI-VO erstellt werden müssen und ist über Meldungen schwerwiegender Vorkommnisse zu informieren. Zudem müssen mir zusammengefasste Jahresberichte über die Verwendung von biometrischen Fernidentifizierungssystemen durch die Strafverfolgungsbehörden des Bundes vorgelegt werden. Die KI-VO sieht außerdem Reallabore zur Innovationsförderung vor. Reallabore sollen eine kontrollierte Umgebung bieten, die die Entwicklung, das Training, das Testen und die Validierung innovativer KI-Systeme für einen begrenzten Zeitraum erleichtert. Wenn in einem solchen Reallabor personenbezogene Daten verarbeitet werden, sind die Datenschutzaufsichtsbehörden einzubeziehen. Ich bin gerne bereit, an diesem vielversprechenden Instrument der Innovationsförderung und des Grundrechtsschutzes aktiv mitzuwirken und auch Reallabore in meiner Regie einzurichten.

Zentrale Rolle bei dem Vollzug der KI-VO kommt den Marktüberwachungsbehörden zu. Jeder Mitgliedstaat ist gehalten, mindestens eine notifizierende Behörde

und mindestens eine Marktüberwachungsbehörde als zuständige nationale Behörden zu benennen, die die Anwendung und Durchführung der KI-VO beaufsichtigen.

Die Verarbeitung von personenbezogenen Daten ist sowohl für die Entwicklung als auch für den Betrieb von KI-Systemen von zentraler Bedeutung. Zudem bleibt das Datenschutzrecht von der KI-VO unberührt. Eine konsistente und einheitliche Auslegung der datenschutzrechtlichen Bestimmungen und der KI-VO ist im Interesse der Rechtssicherheit unabdingbar. Ich setze mich deshalb dafür ein, dass die Zusammenarbeit zwischen den Datenschutzaufsichts- und Marktaufsichtsbehörden sowohl auf der Gesetzgebungsebene als auch in der praktischen Zusammenarbeit eindeutig und kooperativ geregelt und umgesetzt wird.

Im Interesse der Rechtssicherheit ist es aber auch, dass die Kompetenzen der relevanten Behörden eindeutig voneinander abgrenzbar sind. So muss legislativ klargestellt werden, dass die Datenschutzaufsichtsbehörden für die Auslegung und Anwendung der Datenschutzregelungen der KI-VO, wie z. B. Art. 59 KI-VO und Art. 10 Abs. 5 KI-VO zuständig sind. Ebenso bedarf es auch klarer Beteiligungs- und Kooperationsnormen. Datenschutzaufsichtsbehörden sollten bei Verfahren der Marktüberwachungsbehörden, in denen die Verarbeitung von personenbezogenen Daten eine Rolle spielen, so eingebunden werden, sodass sich widersprechende Entscheidungen ausgeschlossen sind.

Die Einschätzungsprärogative hinsichtlich der Rechtmäßigkeit der Verarbeitung personenbezogener Daten obliegt allein den Datenschutzaufsichtsbehörden.

Ich empfehle dem Gesetzgeber, die sich aus der KI-Verordnung der EU ergebende nationale KI-Aufsichtsstruktur möglichst zeitnah festzulegen und dabei die bei meiner Behörde vorhandene Expertise bestmöglich einzubeziehen. Nur so kann die Vorbereitung auf die komplexen mit der KI-Aufsicht einhergehenden Aufgaben gelingen und der Aufbau der erforderlichen Strukturen sichergestellt werden.

Querverweis:

3.2.2 KI als Fokusthema der Gremienarbeit

3.2.2 KI als Fokusthema der Gremienarbeit

Das Thema Künstliche Intelligenz (KI) war auch im Berichtsjahr ein Dauerbrenner in den nationalen und europäischen Datenschutzgremien. Neben Fragestellungen, die sich aus der nunmehr beschlossenen KI-Verordnung der EU ergeben, haben sich die Datenschutzaufsichtsbehörden ganz wesentlich damit befasst, was der Einsatz von KI für betroffene Personen, Verantwortliche und die Gesellschaft als Ganzes bedeutet. Ein wesentliches Augenmerk wird dabei einer konsistenten Positionierung zuteil, um Verantwortliche bei der rechtssicheren Implementierung von KI-Anwendungen zu unterstützten und den Gesetzgeber auf Handlungsbedarf aufmerksam zu machen.

Auch im Berichtsjahr haben sich nationale und europäische Datenschutzgremien intensiv mit KI beschäftigt. Der Fokus der deutschen Datenschutzkonferenz (DSK) lag dabei darauf, mehr Rechtssicherheit bei der Entwicklung und Anwendung von KI zu schaffen sowie die einheitliche Auslegung der Datenschutzbestimmungen im Hinblick auf KI zu verbessern. Zu diesem Zweck hat die DSK am 6. Mai 2024 die Orientierungshilfe „Künstliche Intelligenz und Datenschutz“[8] für den Einsatz von KI-Anwendungen veröffentlicht, an der meine Mitarbeitenden intensiv beteiligt waren. Vor dem Einsatz steht die Entwicklung, in der bereits wesentliche Weichen in Richtung Datenschutzkonformität gestellt werden müssen. Gerade bei KI-Systemen können zudem bereits in diesen frühen Lebenszyklusphasen auch personenbezogene Daten verarbeitet werden. Damit diese entstehenden Lösungen auch datenschutzkonform einsetzbar sind, erarbeitet der AK Technik der DSK derzeit ein Papier für Hersteller und Betreiber von KI-Anwendungen unter der Leitung meines Hauses.

Bei neuen Technologien wie KI stellt sich häufig die Frage, wie die bestehenden technologieneutralen Anforderungen der Datenschutzgesetzgebung umgesetzt werden können. Auf meine Initiative hin und mit meiner Beteiligung hat der EDSA im Rahmen seines Support-Pool-of-Experts-Programms (SPoE) insoweit zwei Expertisen zum Stand der Wissenschaft und Technik erarbeitet. Die erste Expertise widmet sich der Frage, wie die Betroffenenrechte im Kontext von KI-Systemen effektiv umgesetzt werden können. Ein besonderer Fokus liegt hier auf Möglichkeiten der Berichtigung und des Löschens von personenbezogenen Daten. Wenn ein KI-Modell erst einmal trainiert wurde, können sich besondere Herausforderungen ergeben. Ein einfaches „Suchen und Ersetzen“

8 Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ der DSK vom 6. Mai 2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

oder „Suchen und Löschen“ scheitert bereits daran, dass nicht immer klar ist, wie die entsprechende Information im Modell repräsentiert ist. Die Expertise geht daher auf die KI-spezifischen Herausforderungen ein, zeigt auf, welche Möglichkeiten Techniken wie etwa Filtern und Unlearning bieten und wo Grenzen liegen. Die zweite Expertise setzt sich damit auseinander, wie diskriminierende Verzerrungen (Bias) in KI-Systemen entstehen und wie sie automatisch erkannt und in unterschiedlichen Lebenszyklusphasen eines KI-Systems behoben werden können. Auf Basis publizierter wissenschaftlicher Erkenntnisse und verfügbarem Proof-of-Concept-Code wird zudem eine Einschätzung zum Stand von Wissenschaft und Technik in diesem Bereich dargelegt.

Die KI-VO enthält einige Regelungen mit Schnittstellen zum Datenschutz, insbesondere etwa zu Verzerrungen. Um Verantwortliche bei der Umsetzung ihrer hieraus erwachsenden Pflichten zu unterstützten, erarbeitet die Technology Expert Subgroup (TECH ESG) des EDSA unter Beteiligung meines Hauses Leitlinien zum Zusammenspiel der KI-VO und der europäischen Datenschutzbestimmungen. Die Leitlinie wird sich dabei mit grundlegenden Aspekten wie einer Gegenüberstellung der unterschiedlichen Rollen in der KI-VO und der datenschutzrechtlichen Regelungen befassen. Ein weiterer Schwerpunkt wird bei den Normen zu sog. Hochrisiko-KI-Systemen liegen. Wer ist hier wem gegenüber rechenschaftspflichtig, welche Transparenzanforderungen müssen umgesetzt werden und wie verhalten sich die Risikobegriffe von KI-VO und DSGVO zueinander? Nicht zuletzt werden auch die Fragen zu automatischer Entscheidungsfindung unter den beiden wechselwirkenden Rechtsregimen eine prominente Rolle spielen.

Auch auf europäischer Ebene ist die einheitliche Auslegung der DSGVO bei KI ein wichtiges Thema. Einige hochrelevante Grundsatzfragen unter anderem zu dem Personenbezug von KI-Modellen wurden auf Antrag der irischen Data Protection Commission (DPC) im Rahmen eines Art. 64(2)-Verfahrens vom EDSA diskutiert (Opinion 28/2024 veröffentlicht am 18. Dezember 2024).[9] Ich war mit der Unterstützung meiner Mitarbeitenden intensiv in die Erarbeitung und Verabschiedung der Stellungnahme zu den von der DPC eingereichten Fragestellungen involviert. Mein Haus hat sich außerdem spezifisch mit den Details der KI-Anwendung ChatGPT auseinandergesetzt. Da OpenAI, der Anbieter von ChatGPT, bis zum 15. Februar 2024 keine Niederlassung in der EU hatte, hat bis zu diesem Zeitpunkt der One-Stop-Shop-Mechanismus nicht gegriffen. Die Task Force ChatGPT des EDSA war daher mit der Koordinierung der Untersuchungen und der datenschutzrechtlichen Bewertung von ChatGPT befasst, um eine kohärente Anwendung der DSGVO zu gewährleisten. An dem am 23. Mai 2024 veröffentlichten Bericht[10] über die von der Task Force ChatGPT durchgeführten Arbeiten hat mein Haus mitgewirkt.

Querverweis:

3.2.1 KI-Verordnung

3.2.3 BfDI Prüfkatalog für KI-Anwendungen

Auch wenn meine Beratungs- und Kontrolltätigkeit schon länger zunehmend Datenverarbeitungen durch Systeme der Künstlichen Intelligenz (KI) umfasst, hat dieser Themenbereich vor allem durch die rasante Skalierung im Kontext der großen Sprachmodelle jüngst noch einmal an Bedeutung gewonnen. Grundsätzlich ist das Vorgehen, das meine Behörde bisher bei Kontrollen anwendet, auch auf den KI-Bereich übertragbar. An vielen Stellen wird es durch die technologische Entwicklung aber notwendig, ergänzende Einschätzungen zu treffen und Abwägungen auf die Besonderheiten von KI anzupassen. Im Berichtszeitraum hat eine zu diesem Zweck eingesetzte Projektgruppe meines Hauses ihre Arbeit abgeschlossen und einen Prüfkatalog entwickelt, der als Grundlage für meine künftige Kontrolltätigkeit im Bereich von KI-Anwendungen dient.

In meiner Aufsichtsfunktion muss ich mich mit den schnellen Entwicklungen im KI-Bereich intensiv befassen. Nur so ist gewährleistet, dass eine datenschutzrechtliche Beurteilung der oft komplexen Sachverhalte adäquat vorgenommen und die Einhaltung der datenschutzrechtlichen Vorgaben in diesem dynamischen Umfeld kontinuierlich gewährleistet wird. Um diese Aufgabe zu unterstützen, hat eine hierfür eingesetzte Projektgruppe, die sich interdisziplinär aus Mitgliedern ganz verschiedener Fachreferate meines Hauses zusammengesetzt hat, ein Prüfraster als Grundlage für meine Beratungs- und Kontrolltätigkeit im Hinblick auf KI-basierte Algorithmen und Anwendungen entwickelt. Im Ergebnis wurde ein Prüfkatalog erarbeitet, der auf einzelne Aspekte von Kontrollen eingeht, begleitet durch ein erläuterndes Dokument, das Hintergrundinformatio-

9 Opinion des EDSA vom 18. Dezember 2024, abrufbar unter: https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

10 Bericht der EDSA-Taskforce zu ChatGPT vom 23. Mai 2024, abrufbar unter: https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

nen liefert und bei der Bewertung von KI-Anwendungen unterstützt.

Der Prüfkatalog betrachtet neben dem KI-System auch dessen organisatorische Einbettung in Form von Rollen und Prozessen. Grundlage der Betrachtung bildet jeweils ein allgemeiner Steckbrief mit Fragen etwa zum Verantwortlichen, zum Zweck und zu betroffenen Personengruppen sowie zu technischen Details und Systemparametern. Hieran schließt sich ein modularer Baukasten an, der eine Fokussierung auf Kontrollschwerpunkte erlaubt. So können Aspekte wie die anwendbare Rechtsgrundlage der KI-basierten Datenverarbeitung, die Prozessgestaltung der effektiven internen Datenschutzaufsicht und die Umsetzung der Betroffenenrechte in der Anwendung in angemessener Tiefe geprüft werden. Auch zu KI im Auftragsverarbeitungsverhältnis, zur Verarbeitung nach Treu und Glauben und Diskriminierungsfreiheit sowie zu Transparenz, Verlässlichkeit und Sicherheit der Verarbeitung finden sich spezifische Fragenkomplexe. Diese Granularität erlaubt es meinen Mitarbeitenden, Kontrolle und Beratung spezifisch auf den Entwicklungsgrad und etwa besonders kritische Aspekte einer KI-Anwendung zuzuschneiden und so gemeinsam mit den beaufsichtigten Stellen effizient zu Ergebnissen zu kommen.

Der Fragenkatalog und die Hinweise bieten wichtige Referenzpunkte bei der Ausgestaltung von Beratungen und Kontrollen. In mehreren Bereichen konnte der Prüfkatalog bereits erfolgreich eingesetzt werden.

Aus der dynamischen Entwicklung im Bereich der KI-unterstützten Verarbeitungen ergibt sich selbstverständlich die Notwendigkeit, die Ansätze fortlaufend zu evaluieren und zu aktualisieren sowie dort anzupassen, wo neue rechtliche und technologische Entwicklungen und Regulierungsvorgaben Auswirkungen auf meine aufsichtsbehördlichen Aufgaben haben werden. Um dies zu gewährleisten und der zunehmenden Bedeutung des Themenbereichs KI auch künftig gerecht werden zu können, wurde Mitte des Berichtsjahres in meiner Behörde ein eigenes Referat für das Thema KI eingerichtet.

Querverweise:

3.2.1 KI-Verordnung, 3.2.2 KI als Fokusthema der Gremienarbeit

3.3 Sicherheit

3.3.1 Klage gegen den BND

Erstmalig habe ich Klage zur Durchsetzung meiner Kontrollbefugnisse erhoben. Die Klage richtet sich gegen den Bundesnachrichtendienst (BND) und wurde vor dem zuständigen Bundesverwaltungsgericht erhoben. Der BND verwehrt mir die Einsichtnahme in Unterlagen, die meinem gesetzlich geregelten Einsichtsrecht unterliegen und deren Kenntnis zur Durchführung meiner Kontrollen erforderlich ist.

Der Klage gingen mehrere Gespräche auf Behördenleitungsebene und in der Folge eine Beanstandung nach dem BDSG voraus. Die Beanstandung, in der meine Behörde die im Rahmen einer Kontrolle erfolgte Verweigerung der Einsichtnahme für rechtswidrig erklärt hat, wurde von der zuständigen Fachaufsicht des BND, dem Bundeskanzleramt (BKAmt), als rechtlich unzutreffend zurückgewiesen. Sie blieb in der Folge unberücksichtigt. Durch die verweigerte Einsichtnahme greift der BND in meine Unabhängigkeit ein: Er nimmt für sich in Anspruch, selbst über die notwendigen Grundlagen, den Umfang und den Inhalt der Kontrolle entscheiden zu dürfen.

Zur Durchsetzung meines gesetzlichen Auftrags bin ich daher auf den Rechtsweg angewiesen. Gegenstand des Klageverfahrens sind die Reichweite meines Einsichtsrechts sowie die Frage nach der Geltung der sog. Third Party Rule gegenüber meiner Behörde als unabhängiger Kontrollinstanz. Der Rechtsweg steht mir in diesem Fall offen, weil ich meine eigenen Kontrollrechte geltend mache.

Der Klagegegenstand zeigt ein Grundsatzproblem auf: Ich habe derzeit nur die Möglichkeit, nicht durchsetzbare Beanstandungen gegenüber dem BKAmt als für den BND zuständige fachaufsichtliche oberste Bundesbehörde auszusprechen. Dies gilt auch für die anderen Nachrichtendienste des Bundes, also das Bundesamt für Verfassungsschutz und das Bundesamt für den Militärischen Abschirmdienst sowie deren Fachaufsichtsbehörden, das Bundesministerium des Innern und für Heimat und das Bundesministerium der Verteidigung. Teilen diese als Fachaufsichten über die Nachrichtendienste meine Rechtsauffassung nicht, so steht mir im Regelfall keine Möglichkeit zur Durchsetzung meiner Feststellungen zu und die Beanstandung läuft ins Leere. Dies widerspricht der Forderung nach einer effektiven Kontrolle der Nachrichtendienste. Aus diesem Grund fordere ich für meine Behörde seit vielen Jahren dem BKAG entsprechende Anordnungsbefugnisse gegenüber den Nachrichtendiensten des Bundes.

Wie bereits in meinem 32. Tätigkeitsbericht empfehle ich dem Gesetzgeber, Abhilfebefugnisse auch im Bereich der Nachrichtendienste einzuführen.

3.3.2 BfDI droht Verlust der Aufsicht über die Nachrichtendienste

Durch die für die Nachrichtendienste des Bundes zuständigen Ressorts wird die Überlegung verfolgt, mir die Zuständigkeit für die datenschutzrechtliche Aufsicht über den Bundesnachrichtendienst (BND), das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für den Militärischen Abschirmdienst (BAMAD) zu entziehen. Dies wäre Teil einer Novelle geworden, die im Wesentlichen mit der Umsetzung höchstrichterlicher Entscheidungen begründet worden wäre. Während das Bundesverfassungsgericht (BVerfG) auch im Bereich der Kontrolle Änderungen anmahnt, ist aber gerade diese Zuständigkeitsänderung vom Gericht nicht vorgegeben.

Verlagerung meiner datenschutzrechtlichen Kontrollzuständigkeit über die Nachrichtendienste des Bundes

Die datenschutzrechtliche Aufsicht über die Nachrichtendienste des Bundes liegt bislang in meiner Zuständigkeit. In der 20. Wahlperiode habe ich vernommen, dass diese Zuständigkeit auf das administrative Kontrollorgan des Unabhängigen Kontrollrates (UKRat) verlagert werden soll. Der UKRat ist bislang in erster Linie für die Vorabkontrolle bestimmter nachrichtendienstlicher Maßnahmen beim BND zuständig.

Gegenüber den für die Fachaufsicht über die Nachrichtendienste zuständigen obersten Bundesbehörden habe ich auf die Risiken einer solchen Aufsichtsverlagerung aufmerksam gemacht. Neben dem Verlust einer völlig unabhängigen Datenschutzaufsicht und einer damit einhergehenden Verschlechterung des Grundrechtsschutzes führt eine Aufsichtsverlagerung zu einem Verlust meiner einzigartigen und über viele Jahre aufgebauten umfassenden Expertise im nachrichtendienstlichen Bereich.

Eine effektive Datenschutzkontrolle im Sicherheitsbereich kann nur dann sichergestellt werden, wenn ich für alle Sicherheitsbehörden des Bundes zuständig bleibe. Denn für eine derartige Kontrolle bedarf es einer im deutschen und europäischen Kontext einheitlichen Auslegung und Durchsetzung des Datenschutzrechts sowie eines Gesamtüberblicks über alle Sicherheitsbehörden und deren Datenverarbeitungssysteme. Diese Voraussetzungen werden von mir erfüllt. Insbesondere der Gesamtüberblick über die Systemlandschaften der Nachrichtendienste und der anderen Sicherheitsbehörden ermöglicht es mir, der mir vom Bundesverfassungsgericht (BVerfG) zugesprochenen Kompensationsfunktion bei der Kontrolle geheimer Datenverarbeitungen gerecht zu werden. Nur auf Grundlage dieses Gesamtüberblicks über die Nachrichtendienste und die weiteren Sicherheitsbehörden des Bundes kann ich den Lebenszyklus personenbezogener Daten und damit behördenübergreifend die konkrete Verwendung der personenbezogenen Daten vollständig nachvollziehen.

Um der Besorgnis etwaiger Doppelkontrollen zu begegnen, habe ich einen praktischen, kostengünstigen und leicht umsetzbaren gesetzlichen Gestaltungsvorschlag gemacht, welcher zudem den Anforderungen des BVerfG an eine wirksame objektiv rechtliche Kontrolle gerecht wird. Ich habe vorgeschlagen, dass ein inhaltlicher Austausch zwischen dem UKRat und mir ermöglicht wird. Derzeit ist mir sowie auch dem UKRat ein solcher inhaltlicher Austausch verboten. Durch einen inhaltlichen Austausch über Kontrollinhalte sollen Kontrolllücken, aber auch unnötige Doppelbelastungen der kontrollierten Stellen vermieden werden.

BVerfG mahnt (nur) eine unabhängige Vorab-Kontrolle eingriffsintensiver Maßnahmen der Nachrichtendienste an

Die Aufsichtsverschiebung sollte Teil einer Novellierung der Gesetze über die Nachrichtendienste werden, deren Notwendigkeit sich aus der aktuellen Rechtsprechung des BVerfG ergibt. So hat das BVerfG nun auch für den Tätigkeitsbereich des BfV entschieden, dass eingriffsintensive Maßnahmen wie die Observation von Personen oder die Online-Durchsuchung vor ihrem Einsatz von einer unabhängigen Instanz außerhalb des Nachrichtendienstes genehmigt werden müssen. Zu der Frage, wie die anschließende Kontrolle in Bezug auf diejenigen personenbezogenen Daten, die durch eine solche Maßnahme erlangt werden, aussehen muss, hat das Gericht nichts gesagt. Das musste es auch nicht, denn diese Form der Kontrolle ist eine objektiv rechtliche Datenschutzkontrolle wie sie von mir seit langem mit der Abteilung 3 „Polizei und Nachrichtendienste“ durchgeführt wird.

Mit dem vorzeitigen Koalitionsende ist die Umsetzung dieser sowie weiterer Forderungen des BVerfG[11] zunächst einmal vom Tisch. In der nächsten Wahlperiode ist ein neuer Anlauf wahrscheinlich – und anlässlich der Forderungen des BVerfG auch notwendig. Ich vertraue darauf, dass die neue Regierung die überwiegenden Vor-

11 32. TB Nr. 3.3.1

teile erkennt, die mit dem Verbleib der Kontrolle bei mir verbunden sind.

Novellierung der Nachrichtendienstgesetze leider erneut verschoben

Nicht nur die gerade erwähnte Forderung nach einer Vorabkontrolle konnte nicht umgesetzt werden. Das BVerfG hat, teilweise wiederholt, weitere Forderungen aufgestellt, die der Gesetzgeber angehen muss. Die Systematik der nachrichtendienstlichen Befugnisse muss neu geregelt werden. Sie muss sich an sog. Eingriffsschwellen ausrichten. Das bedeutet, dass eine Maßnahme, die tiefer in Grundrechte eingreift, auch höheren Anforderungen unterliegt. Dies muss die dazugehörige Rechtsgrundlage berücksichtigen. Weiter muss der Kernbereichsschutz beim Einsatz sämtlicher nachrichtendienstlicher Mittel sichergestellt werden. Ein weiterer Punkt war die Loslösung des Gesetzes über den Militärischen Abschirmdienst (MADG) vom Bundesverfassungsschutzgesetz (BVerfSchG). Bislang gibt es viele Verweise vom MADG ins BVerfSchG, die aber für Rechtsanwender kaum noch zu verstehen sind. Das Bundesministerium der Verteidigung hat mich bei der Erarbeitung eines eigenständigen MADG frühzeitig in konstruktive Gespräche eingebunden, was ich sehr begrüße. Ich stehe für einen weiteren lösungsorientierten und konstruktiven Austausch gerne bereit.

3.3.3 Gründlichkeit und Verhältnismäßigkeit beim „Sicherheitspaket“

Mit dem Gesetzesentwurf „zur Verbesserung der Terrorismusbekämpfung“ (einem Teil des sogenannten Sicherheitspakets) reagierte die Bundesregierung auf den Anschlag in Solingen vom 23. August 2024. Der Gesetzesentwurf enthielt Ermächtigungsgrundlagen, die massive Eingriffe in die Grundrechte datenschutzrechtlich betroffener Personen zuließen.

Hauptaugenmerk des Gesetzesentwurfs für ein sog. „Sicherheitspaket“ war es, den automatisierten Abgleich biometrischer Daten (Gesichtsbilder und Stimmen) mit öffentlich zugänglichen Daten im Internet zu ermöglichen. Ferner sollte eine Rechtsgrundlage für die automatisierte Datenanalyse geschaffen und dazu eine umfassende Datensammlung aufgebaut werden. Dies hätte – für die politische Debatte habe ich das zugespitzt formuliert – eine „Super-Datenbank“ beim Bundeskriminalamt bedeutet. Aufgrund des politischen Zeitdrucks wurde keine Ressortabstimmung durchgeführt, in der ich beratend meine datenschutzrechtliche Expertise hätte einbringen können. Stattdessen wurde den Fraktionen von SPD, FDP und Bündnis 90/Die Grünen eine nur zwischen dem Bundesministerium des Innern und dem Bundesministerium der Justiz abgestimmte „Formulierungshilfe“ zur Verfügung gestellt, welche dann als Gesetzesentwurf aus der Mitte des Bundestages unmittelbar dort beraten wurde. Auch aufgrund meiner kritischen Stellungnahmen wurden die Befugnisse dann aber grundrechtskonformer gefasst und entsprechend vom Bundestag verabschiedet. Diese Fassung wurde jedoch im Bundesrat abgelehnt. Das Gesetzgebungsverfahren ist zum Ende der 20. Wahlperiode zum Stillstand gekommen, es ist zum Redaktionsschluss dieses Berichts unklar, ob das Vorhaben politisch weiterverfolgt werden wird.

Diese Neuregelungen des sog. „Sicherheitspakets“ ist aus datenschutzrechtlicher Perspektive weiterhin kritisch: Mit einer biometrischen Identifizierung und einer automatisierten Datenanalyse würden schwerwiegende Grundrechtseingriffe normiert werden, meiner Ansicht nach in unverhältnismäßiger Weise. Denn der Kreis der Personen, die potenziell von einem biometrischen Abgleich betroffen sein könnten, war im Gesetzesentwurf zu weit gefasst war. Zum Beispiel hätten auch Zeugen einen biometrischen Abgleich fürchten müssen. Ferner fehlte es an Festlegungen und Anforderungen zur technischen Umsetzung. Da moderne Gesichtserkennungssysteme zukünftig in aller Regel unter die KI-Verordnung der EU fallen dürften, bliebe eine Prüfung der Vereinbarkeit auch mit diesen Vorschriften notwendig. Ebenso waren die Regelungen im Gesetzesentwurf zur automatisierten Datenanalyse technikoffen, so dass selbstlernende (KI-)Systeme hätten eingesetzt werden können. Dies erhöht nach der Rechtsprechung des Bundesverfassungsgerichts die Intensität der mit der Analyse einhergehenden Grundrechtseingriffe, was eine besondere verfassungsrechtliche Rechtfertigung und hinreichende gesetzliche Schutzvorkehrungen erfordert. Ich appelliere an die politischen Verantwortungsträgerinnen und Verantwortungsträger, dass Gesetze, die derart weitreichend in Grundrechte der Bürger und Bürgerinnen eingreifen, mit der gebotenen Sorgfalt und Gründlichkeit erarbeitet sowie in dem Gesetzgebungsverfahren eines Regierungsentwurfs beraten werden.

3.3.4 Debatte um Quick Freeze und Vorratsdatenspeicherung versachlichen

Das Thema Vorratsdatenspeicherung polarisiert: Für die einen ist die Vorratsdatenspeicherung ein unerlässliches Instrument für eine effektive Aufklärung internetbezogener Straftaten. Für andere wird ihr Nutzen überschätzt und in ihr eine Bedrohung für Freiheiten und Bürgerrechte gesehen, diese sehen im sog. Quick Freeze eine verhältnismäßige Alternative.

Wenn eine Sache über Jahrzehnte diskutiert wird, ist eines augenfällig: Es geht um eine komplexe Fragestellung, die mit schwierigen Abwägungsprozessen verbunden ist. Dies gilt auch für die Einführung der Vorratsdatenspeicherung und des sog. „Quick Freeze". Erstere setzt – holzschnittartig – für bestimmte Zwecke auf die präventive Speicherung von Verkehrs- und Standortdaten. Letztere basiert darauf, diese Daten erst bei Verdacht einer erheblichen Straftat bei einem Telekommunikationsanbieter einzufrieren, um sie – bei konkretem Verdacht gegen eine bestimmte Person – später auswerten zu können.

Während auf europäischer Ebene zum Teil für eine umfassende Vorratsdatenspeicherung geworben wird, fokussiert sich die politische Debatte in Deutschland zunehmend auf die Einführung einer Vorratsdatenspeicherung von IP-Adressen. In dieser laufenden Diskussion veröffentlichte das BMJ im Oktober 2024 –als Alternative zur Vorratsdatenspeicherung – einen zweiten Referentenentwurf für die skizzierte „Quick-Freeze"-Regelung.

Mir ist wichtig, die Debatte zu versachlichen, sie anhand objektiver Argumente zu führen und hierbei die Leitplanken der Rechtsprechung des Europäische Gerichtshofs (EuGH) im Blick zu halten. Diese zeigen, was rechtskonform möglich ist und was nicht:

Grundlegend für die rechtliche Beurteilung sind zwei Urteile des EuGHs in Sachen Spacenet[12]. In der Rechtssache Spacenet hat der EuGH die allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen auf das absolut notwendige Maß beschränkt. Ob eine solche anlasslose und unterschiedslose Vorratsdatenspeicherung nach Auffassung des EuGHs zulässig oder unzulässig ist, ist abhängig davon, wie schwer der Grundrechtseingriff der IP-Adressspeicherung im Rahmen der durchzuführenden Verhältnismäßigkeitsprüfung wiegt und ob das verfolgte Gemeinwohlziel in angemessenem Verhältnis zur Schwere des Eingriffs steht („Zweck-Mittel-Relation"). In dieser Entscheidung hat der EuGH es aber bereits für zulässig erachtet, bei einem Verdacht einer konkreten Straftat, eine umgehende Sicherung von Daten anzuordnen und hat damit den Weg für „Quick Freeze" geebnet.

Das Urteil in der Rechtssache Hadopi[13] kehrt diese Rechtsprechung nicht etwa um – wie dies in der öffentlichen Diskussion aber zum Teil dargestellt wird. Der EuGH entschied vielmehr klarstellend, dass dann, wenn gespeicherte IP-Adressen allein genutzt werden, um die Identitätsdaten einer Person in Erfahrung zu bringen und wenn – was sicherzustellen ist – mit der Speicherung oder Verwendung der Daten das Online-Verhalten von Betroffenen nicht nachvollzogen werden kann, es an einem schweren Grundrechtseingriff fehlt, IP-Adressen also unter geringeren Voraussetzungen gespeichert werden dürfen. Aber auch dann müssen Speicherung und Zugriff zwingend notwendig sein und es bedarf einer evidenzbasierten Rechtsgrundlage.

Zu einer sachlichen Diskussion des Themas Vorratsdatenspeicherung und „Quick Freeze" gehört auch die Frage, ob eine Vorratsdatenspeicherung angesichts vorhandener Umgehungsmöglichkeiten tatsächlich einen Mehrwert für Strafverfolgungsbehörden generiert. Auch mit Blick auf das „wie" einer Vorratsdatenspeicherung bedürfte insbesondere die Festlegung eines absolut notwendigen Speicherzeitraums einer empirisch nachweisbaren Grundlage. Hier weise ich darauf hin, dass selbst Strafverfolgungsbehörden auf empirischer Grundlage angeben, dass die Erfolgsquote bei Ermittlungen nach einem Zeitraum von etwa 2–3 Wochen nicht mehr merklich ansteigt[14]. Eine empirische Grundlage für eine Forderung für die zum Teil diskutierte Speicherdauer von IP-Adressen für mehrere Monate fehlt insofern. In der Diskussion sind auch die Potenziale des „Quick-Freeze" mit einzustellen, das verfassungsrechtlich weniger eingriffsintensiv wäre. Anlasslose IP-Adressspeicherung – egal ob durch den EuGH für zulässig erklärt oder nicht, verstärkt das Gefühl von Überwachtheit in der Bevölkerung. Allein dieser Eindruck ist geeignet, angepasstes Verhalten auszulösen, was einer freiheitlichen Gesellschaft nicht zuträglich ist. Ich werde die Diskussion und mögliche Gesetzgebungsprozesse um IP-Adressspeicherung daher weiter begleiten und alles dafür tun, grundrechtsschonende Lösungen zu finden.

Querverweis:

4.5.3 High-Level Expert Group zur EU-Vorratsdatenspeicherung

12 Urteil des EuGH vom 20. September 2022 Az. C 793/19 und C 794/19

13 Urteil des EuGH vom 30. April 2024 – C-470/21

14 Positionspapier des BKA zu erforderlichen Speicherfristen von IP-Adressen, abrufbar unter: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html

4 Gremien

4.1 Bericht aus der DSK

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) verfolgt das Ziel, die Datenschutzgrundrechte zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts in Deutschland zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Hierfür nimmt die DSK unter anderem in Entschließungen zu datenschutzpolitischen Fragen Stellung, fasst Beschlüsse zur Auslegung datenschutzrechtlicher Regelungen oder gibt Stellungnahmen, Orientierungshilfen und Anwendungshinweise heraus. Der Vorsitz der DSK wechselt grundsätzlich jährlich. 2024 wurde der Vorsitz nacheinander von den Landesbeauftragten für Datenschutz aus Bremen, Schleswig-Holstein und Hessen wahrgenommen.

Die DSK hat im Berichtszeitraum drei Entschließungen verabschiedet. Diese betreffen den besseren Schutz von Patientendaten bei Schließung von Krankenhäusern, das Recht auf kostenlose Erstkopie der Patientenakte sowie den Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden.

Zudem hat sie einen Beschluss gefasst. Dieser betrifft die Übermittlung personenbezogener Daten im Rahmen eines Asset-Deals. Ein Asset-Deal ist die Veräußerung eines Unternehmens in der Weise, dass hier Wirtschaftsgüter und Vermögenswerte auf das erwerbende Unternehmen übertragen werden. Davon zu unterscheiden ist der Share Deal, bei dem lediglich Anteile an einem Unternehmen übertragen werden. Darüber hinaus erarbeitete die DSK vier Positionspapiere zu den Themen „Nationale Zuständigkeit für die Verordnung zur Künstlichen Intelligenz“, „Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken“, „Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz“ sowie „Privilegierung der wissenschaftlichen Forschung durch die DSGVO“.

Des Weiteren legte die DSK fünf Orientierungshilfen zu den Schwerpunkten der Aufsichtsbehörden vor: die „Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen“, die „Orientierungshilfe zu Künstlicher Intelligenz und Datenschutz“, die „Orientierungshilfe zu Datenverarbeitungen im Zusammenhang mit funkbasierten Zählern“, die „Orientierungshilfe für die Anbieter von Digitalen Diensten“ sowie die Orientierungshilfe „Ausgewählte Fragestellungen des neuen Onlinezugangsgesetzes“.

Außerdem wurde eine neue Version des Standard-Datenschutzmodells erarbeitet.

Zu allen von der DSK bearbeiteten Themenfeldern sind weitere Informationen auf der Internetseite www.datenschutzkonferenz-online.de veröffentlicht.

4.2 Europäischer Datenschutzausschuss

4.2.1 Allgemeiner Bericht aus dem EDSA

Der Europäische Datenschutzausschuss (EDSA) hat auch in diesem Berichtsjahr seine Arbeit an einer europaweit harmonisierten Anwendung der Datenschutz-Grundverordnung (DSGVO) weiter fortgesetzt, wobei er u. a. den Blick auf die Wechselwirkung mit neuen Rechtsakten zur Regelung Künstlicher Intelligenz, der Umsetzung der europäischen Datenstrategie und des Pakets für digitale Dienste gelenkt hat. Anders als in den vergangenen Berichtsjahren lag der Schwerpunkt der Veröffentlichungen des EDSA auf der Verabschiedung von Stellungnahmen und weniger auf der Annahme von Leitlinien.

2024 hat der EDSA seine hohe Dichte an Plenarsitzungen verfestigt und insgesamt zwölf Mal getagt. Die Sitzungen finden grundsätzlich im Wechsel in Form von Videokonferenzen und Präsenzveranstaltungen in Brüssel statt. Hinzu kommen zahlreiche Sitzungen der Arbeitsgrup-

pen (Expert Subgroups) des EDSA, an denen sich meine Mitarbeitenden aktiv beteiligen.

Stellungnahmen im Kohärenzverfahren

Im sog. **Kohärenzverfahren** nach Art. 4 Abs. 1 DSGVO hat der EDSA – wie in den vergangenen Jahren – zahlreiche Stellungnahmen verfasst.[15] Diese betreffen zum großen Teil:

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

Zudem hat der EDSA vier wichtige **Stellungnahmen im fakultativen Verfahren nach Art. 64 Abs. 2 DSGVO** veröffentlicht. Die Entscheidungen betreffen Fragen mit weitreichendem Effekt, z. B. wenn eine Auswirkung in mehreren Mitgliedstaaten zu erwarten ist.

Die **Stellungnahme 04/2024 zum Begriff der Hauptniederlassung eines Verantwortlichen in der Union gemäß Art. 4 Abs. 16 lit. a) der DSGVO**[16] legt unter anderem fest, dass Entscheidungen über Mittel und Zwecke der Datenverarbeitung in einer in der EU liegenden Hauptverwaltung getroffen werden müssen, damit diese als „Hauptniederlassung" im Sinne der DSGVO verstanden werden kann.

In seiner **Stellungnahme 08/2024 zur „Wirksamkeit von Einwilligungen im Kontext von „Consent or Pay"-Modellen großer Online-Plattformen"**[17] vertritt der EDSA die Auffassung, dass das Angebot nur einer kostenpflichtigen Alternative zu Dienstleistungen, die die Verarbeitung personenbezogener Daten für verhaltensbezogene Werbezwecke beinhalten, nicht der Standardansatz für die Verantwortlichen sein sollte. Bei der Entwicklung von Alternativen sollten große Online-Plattformen in Erwägung ziehen, Einzelpersonen eine „gleichwertige Alternative" zur Verfügung zu stellen, die nicht die Zahlung einer Gebühr beinhaltet. Darüber hinaus liefert der EDSA Elemente zur Bewertung der Kriterien für eine informierte, spezifische und eindeutige Zustimmung, die große Online-Plattformen bei der Umsetzung von „Zustimmungs- oder Entgeltmodellen" berücksichtigen sollten.

In der **Stellungnahme 11/2024 zum Einsatz von Gesichtserkennungstechnologien durch Flughafenbetreiber und Fluggesellschaften zur Straffung des Passagierflusses auf Flughäfen**[18] wird die Vereinbarkeit der Verarbeitung biometrischer Daten mit dem Grundsatz der Speicherbegrenzung, dem Integritäts- und Vertraulichkeitsgrundsatz, dem Datenschutz durch Technik und Voreinstellungen und der Sicherheit der Verarbeitung analysiert. Hierzu prüft der EDSA, ob die Verarbeitung biometrischer Daten der Fluggäste mit vier verschiedenen Arten von Speicherlösungen vereinbar ist, von solchen, die die biometrischen Daten nur in den Händen des Einzelnen speichern, bis hin zu denjenigen, die auf eine zentralisierte Speicherarchitektur mit unterschiedlichen Modalitäten angewiesen sind. In allen Fällen sollten biometrische Daten von Fluggästen nur dann verarbeitet werden, wenn diese sich aktiv angemeldet und der Teilnahme zugestimmt haben.

In der **Stellungnahme 22/2024**[19] hat sich der EDSA zum Verhältnis eines Verantwortlichen zu seinen (Unter-) Auftragsverarbeitern positioniert. Die Stellungnahme erfolgte auf Antrag der dänischen Datenschutzaufsichtsbehörde im Rahmen eines Verfahrens nach Art. 64 Abs. 2 DSGVO, das jede Aufsichtsbehörde einleiten kann, wenn die gestellten Fragen von europaweiter Relevanz sind. Die dänische Aufsichtsbehörde stellte mehrere Fragen zur Auslegung der Art. 28 und 44 DSGVO, die insbesondere die Rechenschaftspflicht des Verantwortlichen beim Einsatz mehrerer „in Kette" hintereinander geschalteter (Unter-)Auftragsverarbeiter betrafen. Daneben ging es um Fragen der vertraglichen Ausgestaltung der Vereinbarung zur Auftragsverarbeitung. Die Fragen betrafen sowohl Verarbeitungen innerhalb des Europäischen Wirtschaftsraums (EWR) als auch Konstellationen mit Drittlandsbezug.

Die **Stellungnahme 28/2024** behandelt bestimmte datenschutzrechtliche Aspekte im Zusammenhang mit der **Verarbeitung von personenbezogenen Daten im**

15 Alle Stellungnahmen des EDSA (nur teilweise übersetzt) sind abrufbar unter: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en

16 EDSA-Stellungnahme 04/2024 vom 13. Februar 2024 zum Begriff der Hauptniederlassung, abrufbar unter: https://www.edpb.europa.eu/system/files/2024-08/edpb_opinion_202404_mainestablishment_de.pdf

17 EDSA-Stellungnahme 08/2024 vom 17. April 2024 zu „Consent or Pay", abrufbar unter: https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_de.pdf

18 EDSA-Stellungnahme 11/2024 vom 23. Mai 2024 zur Gesichtserkennung, abrufbar unter: https://www.edpb.europa.eu/system/files/2025-01/edpb_opinion_202411_facialrecognitionairports_de.pdf

19 EDSA Stellungnahme 22/2024 vom 9. Oktober 2024 zu Auftragsverarbeitern, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222024-certain-obligations-following_en

Kontext von KI-Modellen. Nähere Ausführungen hierzu finden sich im Themenbereich der nationalen und europäischen Gremienarbeit zu KI.

Leitlinien des EDSA im Jahr 2024

Der EDSA hat im Berichtsjahr drei Leitlinien verabschiedet:

Die **Leitlinien 01/2023 zu Art. 37 JI-Richtlinie**[20]**, an deren Erstellung meine Behörde federführend beteiligt war,** wurden nach Durchführung einer öffentlichen Konsultation ohne wesentliche Änderungen bestätigt. Erörtert wird insbesondere der Begriff der „geeigneten Garantien", die in Art. 37 JI-Richtlinie als zentrale Voraussetzung für Drittstaatenübermittlungen durch Strafverfolgungsbehörden genannt werden. In diesem Zusammenhang stellt der EDSA heraus, dass das in der EU gewährleistete Schutzniveau durch die Übermittlung personenbezogener Daten in ein Drittland nicht untergraben werden darf. Ich begrüße, dass damit auch bei Übermittlungen im JI-Bereich hohe Datenschutzstandards gesichert werden.

Die **Leitlinien 01/2024 zur Verarbeitung personenbezogener Daten auf der Rechtsgrundlage eines berechtigten Interesses nach Art. 6 Abs. 1 lit. f) DSGVO,**[21] an denen meine Mitarbeitenden als Co-Berichterstatter mitgearbeitet haben, wurden im Oktober 2024 durch den EDSA verabschiedet. Die Leitlinien enthalten Klarstellungen dazu, welche Aspekte Verantwortliche bei der Prüfung der Voraussetzungen von Art. 6 Abs. 1 lit. f) DSGVO berücksichtigen sollten. Zugleich geben sie Hinweise, wie Art. 6 Abs. 1 lit. f) DSGVO in spezifischen Verarbeitungskontexten angewendet werden kann (bspw. im Bereich von Betrugsprävention, Direktwerbung oder Informationssicherheit). Schließlich stellen die Leitlinien das Verhältnis zwischen Art. 6 Abs. 1 lit. f) DSGVO und Betroffenenrechten klar. Sie leisten damit einen wichtigen Beitrag zur einheitlichen Anwendung von Art. 6 Abs. 1 lit. f) DSGVO innerhalb der EU. Mit einer Annahme des endgültigen Textes durch den EDSA ist nach Abschluss der öffentlichen Konsultation Anfang 2025 zu rechnen.

Die **Leitlinien 02/2023 zur Anwendbarkeit von Art. 5(3) ePrivacy Richtlinie**[22] wurden im Anschluss an eine öffentliche Konsultation angenommen. Ausdrücklich klargestellt ist nunmehr, dass die Leitlinien nicht dazu gedacht sind, die Anwendung der Ausnahmen von der Einwilligungspflicht gemäß Art. 5 Abs. 3 e-Privacy-Richtlinie zu analysieren, und dass die Anwendbarkeit von Art. 5 Abs. 3 e-Privacy-Richtlinie nicht zwingend bedeutet, dass eine Einwilligung eingeholt werden muss.

EDSA-Taskforce zum Zusammenspiel zwischen Datenschutz, Wettbewerb und Verbraucherschutz

Die im März 2023 gegründete EDSA-Taskforce zum Zusammenspiel zwischen Datenschutz, Wettbewerb und Verbraucherschutz hat sich im Berichtsjahr mit den Verbindungen und Synergien zwischen diesen Rechtsgebieten auseinandergesetzt und Positionen und Hilfestellungen hierzu erarbeitet. Unter Co-Federführung meiner Behörde hat sie für die interne Verwendung bei den Datenschutzaufsichtsbehörden ein Papier mit häufig gestellten Fragen (FAQ) zur Kooperation von Datenschutzbehörden mit Wettbewerbs- und Verbraucherschutzbehörden erstellt. Dieses dient der Orientierung der Datenschutzaufsichtsbehörden und legt dar, aus welchen Gründen und in welchen Situationen eine Kooperation zwischen den Behörden sinnvoll ist. Hierbei werden die Vorgaben des Urteils des Europäischen Gerichtshofs in dem Verfahren Meta gegen Bundeskartellamt[23] für die Zusammenarbeit zwischen Datenschutzaufsichts- und Wettbewerbsbehörden für die Praxis nutzbar gemacht, indem unterschiedliche Möglichkeiten zur Kooperation dargestellt und praktische Hilfestellungen geboten werden. So enthalten die FAQ beispielsweise eine Checkliste für nächste Schritte innerhalb der Datenschutzaufsichtsbehörde sowie eine Vorlage für Kooperationsvereinbarungen.

Außerdem wird in der Taskforce, ebenfalls unter Co-Federführung meiner Behörde, ein Positionspapier zu dem Zusammenspiel zwischen Datenschutz- und Wettbewerbsrecht erarbeitet. Dieses wird in Teilen die FAQ spiegeln und als öffentliche Positionierung des EDSA dienen.

Weiterhin werden in der Taskforce in Zusammenarbeit mit der EU-Kommission Leitlinien zum Zusammenspiel zwischen dem EU-Gesetz über Digitale Märkte (DMA) und der DSGVO erarbeitet. Die Leitlinien sollen klären, wie sog. Torwächter, also Unternehmen, die zentrale

20 Leitlinie 01/2023 vom 19. Juni 2024, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012023-article-37-law-enforcement-directive_en

21 Leitlinie 01/2024 vom 20. November 2024, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en

22 Leitlinie 02/2023 vom 7. Oktober 2024, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_en

23 Urteil des EuGHs vom 4. Juli 2023, C-252/21, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0252

Plattformdienste bereitstellen und von der EU-Kommission als Torwächter benannt worden sind, die DSGVO bei der Verarbeitung personenbezogener Daten im Anwendungsbereich des DMA auslegen und anwenden sollten.

Eine wiederkehrende Aufgabe der Taskforce ist die Vorbereitung und Konsolidierung gemeinsamer Standpunkte des EDSA und des Europäischen Datenschutzbeauftragten zur Vorbereitung der Teilnahme an den Sitzungen des im DMA vorgesehenen Beratungsgremiums der EU-Kommission, der sog. High Level Group. So verabschiedete das Beratungsgremium eine Stellungnahme zur Anwendung von Künstlicher Intelligenz durch Torwächter. Außerdem bespricht es in seinen Sitzungen die Berichte seiner Untergruppen zu aus dem DMA erwachsenden Verpflichtungen für Torwächter, wie der Interoperabilität verschiedener Messengerdienste.

EDSA-Strategie 2024–2027

Der EDSA hat seine **Strategie für die Jahre 2024 bis 2027** festgelegt. Diese orientiert sich strukturell an den vier Säulen der vorherigen Strategie, so dass Kontinuität besteht:

- Die 1. Säule beinhaltet eine Verbesserung der Harmonisierung und Förderung der Einhaltung der Vorschriften der DSGVO
- Die 2. Säule beinhaltet eine Stärkung einer gemeinsamen Durchsetzungskultur und effektiven Zusammenarbeit
- Die 3. Säule beinhaltet Datenschutz bei der Entwicklung des digitalen und regulierungsübergreifenden Bereichs
- Die 4. Säule beinhaltet einen Beitrag zum globalen Dialog über Datenschutz

Neben einem inhaltlichen **Schwerpunkt auf Künstlicher Intelligenz** lenkt die Strategie den Blick des EDSA u. a. auf die **Wechselwirkung mit neuen Rechtsakten zur Regelung Künstlicher Intelligenz, der Umsetzung der europäischen Datenstrategie und des Pakets für digitale Dienste**.

Mir ist in diesem Zusammenhang wichtig, dass auf Kohärenz der Digital-Gesetze der EU hingewirkt wird. Die aus der EU-Digitalstrategie hervorgegangenen Rechtsakte, insbesondere Digital Services Act, Data Governance Act, Data Act und KI-Verordnung, sind untereinander und auch in Bezug auf die DSGVO nicht hinreichend abgestimmt. Es gibt Überschneidungen, abweichende Definitionen und ungeklärte Abgrenzungen in den Aufsichtsstrukturen. Dies erschwert den Anbietern und Akteuren sowie den befassten Behörden die Einhaltung und Überwachung der Vorgaben und den betroffenen Personen die Ausübung ihrer Rechte.

Querverweis:

3.2.2 KI als Fokusthema der Gremienarbeit

4.2.2 Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO

Mit dem Vorschlag für eine Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO reagierte die Europäische Kommission auf den Wunsch des Europäischen Datenschutzausschusses (EDSA) nach einer Harmonisierung nationaler Verfahrensregeln und einer Verbesserung der Zusammenarbeit unter den Aufsichtsbehörden in grenzüberschreitenden Fällen. Das Gesetzgebungsverfahren schreitet durch die Positionierungen des Europäischen Parlaments und des Rats der Europäischen Union mit vielen Verbesserungen gegenüber dem Vorschlag der Europäischen Kommission voran.

Der Vorschlag der Europäische Kommission für eine „Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679“ vom 4. Juli 2023 (COM(2023) 348 final, im Folgenden „VVO“) ist eine Reaktion auf die sogenannte Wiener Erklärung des EDSA, mit der eine Verbesserung der Zusammenarbeit bei der Durchsetzung des Datenschutzes in der EU[24] bezweckt wird. Dazu sollen auch Aspekte des nationalen Verfahrensrechts harmonisiert werden.[25] [26]

Das Vorhaben ist von erheblicher Bedeutung für eine bessere und zügigere Durchsetzung der DSGVO bei der Bearbeitung von grenzüberschreitenden Fällen. Ich habe deshalb auch in diesem Jahr das Gesetzgebungsverfahren intensiv begleitet und an der Stellungnahme des EDSA zu den Verhandlungspositionen des Europäischen

24 Wiener Erklärung des EDSA vom 28. April 2022, abrufbar unter: https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf

25 Siehe dazu Annex des EDSA vom 10. Oktober 2022, abrufbar unter: https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf

26 32. TB Nr. 4.2.4

Parlaments und des Rates in Hinblick auf den Trilog[27] mitgearbeitet.

Es ist erfreulich, dass sowohl Parlament als auch Rat Verbesserungen vorgeschlagen und dabei auch die Positionen des EDSA und der Aufsichtsbehörden berücksichtigt haben. Dazu gehören insbesondere die Einführung von verbindlichen Verfahrensfristen, besser aufeinander abgestimmte Regeln im Kooperationsverfahren, die Stärkung der prozessualen Positionen der Beschwerdeführenden sowie die Vermeidung von unnötigen zusätzlichen bürokratischen Schritten.

Ich werde den Gesetzgebungsprozess weiter intensiv beobachten und mich für die nötigen Verbesserungen einsetzen. Durch schnellere und verstärkt gemeinsame Rechtsdurchsetzung und Kooperation können die Grundrechte der Bürgerinnen und Bürger effektiver geschützt werden.

4.2.3 Bericht aus dem CSC

Im Coordinated Supervision Committee (CSC) koordinieren die nationalen Aufsichtsbehörden und der Europäische Datenschutzbeauftragte ihre Aufsichtstätigkeit zu den europäischen IT-Großsystemen und bestimmten EU-Institutionen. Der stellvertretende Vorsitz des CSC wird seit 2021 durch einen meiner Mitarbeitenden wahrgenommen. Der zunehmende Umfang von Zuständigkeiten stellt das CSC vor große organisatorische Herausforderungen, besonders mit Blick auf die nötigen Ressourcen.

Das CSC dient dem Informationsaustausch, der Sicherstellung einer einheitlichen Interpretation der jeweiligen Rechtsgrundlagen sowie der Koordinierung gemeinsamer Kontrollen. Gemeinsam mit der jeweiligen Ländervertretung beteilige ich mich aktiv an den regelmäßigen Sitzungen des CSC und der Ausarbeitung gemeinsamer Dokumente. Zudem wurde einer meiner Mitarbeitenden zum Ende des vorigen Berichtszeitraums als stellvertretender Vorsitzender des Gremiums wiedergewählt.

Der Zuständigkeitsbereich des CSC umfasst insbesondere das Schengener Informationssystem (SIS), Europol, Eurojust, die Europäische Staatsanwaltschaft und das Internal Market Information System (IMI). Das CSC hat in diesem Berichtsjahr auch die Koordinierung für das Visa-Informationssystem (VIS) von der sog. VIS Supervision Coordination Group (SCG) übernommen. Das CSC wird künftig auch die Koordinierung zu Eurodac und zu Teilbereichen des Zollinformationssystems (CIS) von den bisherigen SCGs übernehmen.

Zudem wird das CSC auch für die geplanten EU-Systeme Einreise-/Ausreisesystem (EES), Europäisches Reiseinformations- und -genehmigungssystem (ETIAS), Europäisches Strafregisterinformationssystem für Drittstaatsangehörige und Staatenlose (ECRIS-TCN), die polizeiliche Zusammenarbeit nach der Prüm-II-Verordnung sowie den EU-Interoperabilitätsrahmen zuständig sein. Zwar sind diese Systeme noch nicht in Betrieb gegangen; mit Blick auf die fortschreitende Implementierung nimmt das CSC seine Rolle als Forum zum Informationsaustausch und zur Koordinierung aber bereits aktiv wahr.

Die zunehmende Größe macht Änderungen in der Organisation erforderlich. Künftig sollen Diskussionen und Arbeit vermehrt in Arbeitsgruppen stattfinden. Auch hat das CSC seit diesem Berichtsjahr zwei stellvertretende Koordinatoren. Insgesamt lässt sich festhalten, dass das CSC zwar kontinuierlich weitere Zuständigkeiten für neue und bestehende EU-Systeme erhält, jedoch kaum weitere Ressourcen. Der Möglichkeit, diesem Mangel durch interne Maßnahmen zu begegnen, sind jedoch Grenzen gesetzt.

Im Folgenden möchte ich eine kurze Auswahl aus der Arbeit im CSC darstellen:

Im Bereich **SIS** wurden zum Ende des Berichtszeitraums erstmalig die jährlichen Statistiken über die Wahrnehmung der Betroffenenrechte aus den Mitgliedstaaten gemäß den Verordnungen zum SIS zusammengeführt und ausgewertet. Zudem werden derzeit unter Beteiligung meiner Mitarbeitenden Informationen zur Auslegung von Art. 12 der Verordnung (EU) 2018/1861 zur Nutzung von Protokolldaten durch die Aufsichtsbehörden erhoben. Ferner wurde der Bericht zu den europaweit koordinierten Kontrollen von Ausschreibungen zur verdeckten bzw. gezielten Kontrolle gem. Art. 36 SIS II Beschluss fertiggestellt und angenommen.[28] Auch hieran waren meine Mitarbeitenden direkt beteiligt.

Im Bereich **EES** tauschten sich die Mitglieder regelmäßig zum Sachstand der Implementierung aus. Ebenso berichteten die EU-Kommission zur EES-Informationskampagne und Frontex zur Entwicklung einer EES-App. Das CSC adressierte zudem zwei Schreiben an die

27 Stellungnahme des EDSA 4/2024, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-42024-recent-legislative-developments-draft_en

28 Bericht zur Kontrolle der Ausschreibungen im SIS vom 21. Oktober 2024, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/csc-documents/report-article-36-alerts-schengen-information-system_de

EU-Kommission, in dem an die Pflicht zur Einbeziehung der Aufsichtsbehörden in die Informationskampagne erinnert wurde.[29] Im Bereich **ETIAS** nahm das CSC eine beratende Funktion in Bezug auf Herausforderungen bei der Implementierung von ETIAS wahr, etwa durch internen Austausch zum Thema Betroffenenrechte, aber auch extern durch Teilnahme an Technical Expert Groups und Workshops sowie durch Adressierung der EU-Kommission zu drängenden Problemen bei ETIAS-Datenschutzfolgenabschätzung, Betroffenenrechten und Verantwortlichkeiten.[30] Im CSC koordiniert der EDSA die Vertretung des EDSA im sog. ETIAS-Beratungsgremium für Grundrechte.

Im Bereich **Eurojust** werden derzeit Informationen zu zwei Themenfeldern eingeholt und ausgewertet, einerseits, um mögliche Probleme der Datenqualität des sog. Counter Terrorism Register zu erkennen und andererseits, um Herausforderungen im Bereich der Durchführung der Aufsichtstätigkeit gezielt angehen zu können. Zu Europol hatten die Mitglieder des CSC im vorigen Berichtsjahr koordinierte Kontrollen zur Übermittlung von Daten Minderjähriger an Europol eingeleitet. Derzeit werden Informationen zu den Ergebnissen zusammengeführt und auswertet. Weiterhin arbeitet das CSC an einem internen Leitfaden zur Kooperation der Aufsichtsbehörden bei Auskunftsersuchen. Wiederholt wurde auch die zunehmende Bedeutung von Europol im Bereich der Verarbeitung großer Datenmengen und biometrischer Daten diskutiert.

Im Bereich **IMI** wurden Empfehlungen zu IMI-Transparenzverpflichtungen und der Gewährleistung von Betroffenenrechten in IMI angenommen, die unter Beteiligung meiner Mitarbeitenden entwickelt wurden.[31] Zudem wurde ein Fragebogen entwickelt, der den Bereich der Rechtevergabe für Nutzende und Administration durch die Nationale IMI-Koordination und durch die zuständigen Behörden betrifft. Ziel ist es u. a., systematische Probleme zu erkennen.

Weitere Informationen zum CSC, dem Arbeitsprogramm sowie Sitzungs- und Tätigkeitsberichte des CSC sind online verfügbar.[32]

Querverweise:

4.5.1 ETIAS-Beratungsgremium für Grundrechte, 8.1.10 Datenschutz im Schengen-Raum: Aufsicht über das SIS

4.2.4 Entwicklungen im Bereich internationaler Datenübermittlungen

Auch im Jahr 2024 fanden bedeutsame Entwicklungen im Bereich internationaler Datenübermittlungen statt. Zu Beginn des Jahres hat die Europäische Kommission ihren Bericht zur Überprüfung der elf noch vor Geltung der DSGVO erlassenen Angemessenheitsbeschlüsse veröffentlicht. Im Juli folgte unter maßgeblicher Beteiligung meines Hauses die erste Überprüfung des Angemessenheitsbeschlusses zum EU-U.S. Data Privacy Framework, zu dem die Europäische Kommission ihren Bericht im Oktober und der EDSA seinen Bericht im November veröffentlichte. Auf internationaler Ebene hat mein Haus zwei wichtige Dokumente zur weiteren Förderung des Konzepts Data Free Flow with Trust (DFFT) initiiert und ausgearbeitet, die durch den Roundtable der G7-Datenschutzbehörden im Oktober in Rom und durch die Global Privacy Assembly im Oktober in Jersey verabschiedet wurden.

1. Entwicklungen zum EU-U.S. Data Privacy Framework

Im vorherigen Tätigkeitsbericht hatte ich ausführlich über den Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework (DPF)[33] berichtet, der im Juli 2023 in Kraft getreten ist. Der Angemessenheitsbeschluss zum DPF ist der Nachfolger des Angemessenheitsbeschlusses zum „Privacy Shield", der vom Europäischen Gerichtshof im Jahr 2020 für ungültig erklärt worden war.[34] Seit Inkrafttreten des Angemessenheitsbeschlusses zum DPF können personenbezogene Daten im Anwendungsbereich des Angemessenheitsbeschlusses wieder an US-

29 Schreiben des CSC, abrufbar unter: https://www.edpb.europa.eu/csc/our-work-tools/letters-coordinated-supervision-committee_de
30 Schreiben zur Einführung von ETIAS vom 27. September 2024, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/csc-letters/letter-commission-implementation-etias_de
31 Empfehlungen des CSC zu IMI-Transparenzverpflichtungen, abrufbar unter: https://www.edpb.europa.eu/csc/our-work-tools/imi-reports-coordinated-supervision-committee_de
32 Informationen über die Arbeit des CSC, abrufbar unter: https://www.edpb.europa.eu/csc/about-csc/who-we-are-coordinated-supervision-committee_en
33 Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA (Bekannt gegeben unter Aktenzeichen C(2023) 4745) (Text von Bedeutung für den EWR), abrufbar unter: https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj
34 Urteil des EuGHs vom 16. Juli 2020, 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

Unternehmen und Organisationen, die nach dem DPF zertifiziert sind, übermittelt werden, ohne dass weitere Übermittlungsinstrumente gemäß Kapitel V DSGVO erforderlich sind.

Ein Jahr nach dem Inkrafttreten des Angemessenheitsbeschlusses fand dessen erstmalige Überprüfung im Juli 2024 in Washington, D.C. statt. Daran nahmen Vertreter von US-Behörden und auf Seiten der EU die Europäische Kommission sowie Vertreter des EDSA teil. Wie in meinem vorigen Tätigkeitsbericht angekündigt, habe ich mich durch Mitarbeitende an dieser ersten Überprüfung intensiv beteiligt, federführend zum Themenkomplex „Government Access".

Im Anschluss an die Überprüfung haben sowohl die Europäische Kommission [35] als auch der EDSA [36] einen Prüfbericht veröffentlicht. Die Europäische Kommission stellt in ihrem Bericht fest, dass die US-Behörden die erforderlichen Strukturen und Verfahren eingerichtet haben, um eine effektive Funktionsweise des DPF zu gewährleisten. Sie weist gleichzeitig darauf hin, dass Erfahrungen mit der praktischen Anwendung nach einem Jahr noch limitiert waren und erläutert, welche Entwicklungen sie für erforderlich hält und überwachen wird. Der EDSA führt in seinem Bericht aus, dass bereits viele Umsetzungsschritte vorgenommen worden sind. Gleichzeitig merkt er an, dass künftig weitere Umsetzungsmaßnahmen zu treffen, in einzelnen Punkten Klarstellungen notwendig und die Entwicklungen im US-Recht zu beobachten sind.

Im Hinblick auf die datenschutzrechtlichen Grundsätze, an die sich die zertifizierten US-Unternehmen halten müssen (sog. „commercial part"), kommt der Bericht des EDSA zu dem Ergebnis, dass die Umsetzung der wesentlichen Schritte des Zertifizierungsverfahrens und der unterschiedlichen Rechtsbehelfsmöglichkeiten erfolgt ist. Weiterer Umsetzungsbedarf wird im Hinblick auf eine Verstärkung proaktiver Kontrollen zur Einhaltung der datenschutzrechtlichen Grundsätze durch die US-Behörden gesehen. Gleichzeitig hält der EDSA es für erforderlich, dass weitere Hilfestellungen zum Verständnis der datenschutzrechtlichen Grundsätze veröffentlicht werden. Dies betrifft insbesondere Fragen zur Weiterübermittlung und zum Begriff der Personaldaten [37].

Wesentlicher Gegenstand der ersten Überprüfung im Bereich „Government Access" war die Umsetzung der Datenschutzstandards, die infolge des sogenannten Schrems II-Urteils des EuGHs (Rechtssache C-311/18) in das US-Recht eingeführt worden waren. Die vom EuGH in dieser Entscheidung aufgezeigten Defizite sollen durch einen von den US-Nachrichtendiensten zu beachtenden Grundsatz der Verhältnismäßigkeit und ein neues Beschwerdeverfahren ausgeräumt werden. Für den EDSA ist besonders wichtig, ob diese Änderungen im US-Recht nun auch praktisch wirksam sind. Dabei konnte die Umsetzung des neuen Beschwerdeverfahrens positiv bewertet werden. So ist das für dieses Verfahren zentrale Data Protection Review Court nach der Benennung von acht Richtern voll besetzt und arbeitsfähig. Bei der konkreten Anwendung des neuen Verhältnismäßigkeitsgrundsatzes durch die US-Nachrichtendienste gibt es allerdings noch Klarstellungsbedarf. Dieser Gesichtspunkt ist weiter sorgfältig zu beobachten.

Eine bedeutsame datenschutzrelevante Rechtsentwicklung zu Government Access erfordert ebenfalls genaue Beobachtung. Im April 2024 wurde eine der maßgeblichen Rechtsgrundlagen für die nachrichtendienstliche Erhebung von aus der EU in die USA übermittelter personenbezogener Daten novelliert. Der EDSA macht hier Bedenken zu mangelnder Rechtsklarheit geltend, die Unsicherheit über die tatsächliche Reichweite der zulässigen Datenerhebung schaffen könnte.

Gemäß der DSGVO müssen Angemessenheitsbeschlüsse im Hinblick auf ihre Funktionsweise mindestens alle vier Jahre überprüft werden. Bezüglich des Angemessenheitsbeschlusses zum DPF halten sowohl der EDSA als auch die Europäische Kommission eine frühere Überprüfung für sinnvoll.

Publikationen des EDSA zum DPF

Um Betroffene zu informieren, wie sie ihre Rechte nach dem DPF geltend machen können, hat der EDSA verschiedene Dokumente publiziert. Hierbei handelt es sich um Formulare und Informationen zum Beschwerdever-

35 Bericht der Kommission an das europäische Parlament und den Rat über die erste regelmäßige Überprüfung der Funktionsweise des Angemessenheitsbeschlusses zum Datenschutzrahmen EU-USA, Brüssel, den 9. Oktober 2024, COM(2024) 451 final, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52024DC0451&qid=1731661085429

36 Bericht des EDSA zum ersten Review des EU-U.S. Data Privacy Framework, Version 1.1 vom 4. November 2024, abrufbar unter: https://www.edpb.europa.eu/system/files/2024-11/edpb_report_20241104_reportonfirstreviewofeu-u.s.dpf_en.pdf

37 a. a. O. insbesondere. Seite 4, Rn. 7 ff., Rn. 64 ff.

fahren gegenüber US-Organisationen/-Unternehmen in gewerblichen Angelegenheiten [38] und zum Beschwerdeverfahren bzgl. der Verarbeitung personenbezogener Daten durch US-Nachrichtendienste [39]. Sofern Betroffene eine Rechtsverletzung im Hinblick auf Datenübermittlungen nach dem DPF geltend machen möchten, stehen dazu unterschiedliche Wege offen. Betroffene können sich u. a. unmittelbar an das DPF-zertifizierte Unternehmen wenden oder eine Beschwerde beim Department of Commerce (US-Handelsministerium) oder der Federal Trade Commission (US-Wettbewerbs- und Verbraucherschutzbehörde) vorbringen.

Zudem hat der EDSA ein Papier mit Antworten auf häufig gestellte Fragen (FAQ) zum DPF erarbeitet, das nützliche Informationen für Privatpersonen [40] und Unternehmen [41] bereitstellt.

Eine Übersicht über die o. g. Publikationen des EDSA und weitere Informationen zur Thematik, insbesondere auch zu den verschiedenen Beschwerdeverfahren, sind auf meiner Webseite [42] abrufbar.

2. Bericht der Europäischen Kommission zu den unter der Richtlinie 95/46/EG erlassenen Angemessenheitsbeschlüssen

Im Januar 2024 hat die Europäische Kommission einen Bericht [43] und das dazugehörige Arbeitsdokument [44] zur Überprüfung der elf bereits vor Geltung der DSGVO erlassenen Angemessenheitsbeschlüsse veröffentlicht. Diese Beschlüsse waren noch unter der Datenschutz-Richtlinie 95/46/EG verabschiedet worden. Hierbei handelt es sich um Angemessenheitsbeschlüsse für die Länder Andorra, Argentinien, Kanada (nur in Bezug auf den Privatsektor), Färöer, Guernsey, Isle of Man, Israel, Jersey, Neuseeland, die Schweiz und Uruguay. Die Europäische Kommission hat diese Beschlüsse überprüft und kommt in ihrem Bericht zu dem Ergebnis, dass in allen elf Ländern weiterhin ein angemessenes Datenschutzniveau besteht. In einem Schreiben [45] an die Europäische Kommission hebt der EDSA, der an der Prüfung der Angemessenheitsbeschlüsse formell nicht beteiligt gewesen ist, verschiedene Gesichtspunkte hervor, die bei künftigen Überprüfungen und Beschlüssen besonders berücksichtigt werden sollten. Unter anderem plädiert der EDSA dafür, dass die Kommission künftig die Prüfung der Rechtsstaatsprinzipien ausführlicher darlegen sollte.

3. Data Free Flow with Trust

Die Frage vertrauenswürdiger internationaler Datenübermittlung stand unter dem Konzept des sogenannten Data Free Flow with Trust (DFFT) auch in diesem Jahr im Fokus der Diskussionen wichtiger internationaler Foren im Bereich des Datenschutzes. Mein Haus hat hierzu zwei Dokumente initiiert und federführend ausgearbeitet, die im Rahmen des diesjährigen Roundtable-

---

38 Formular zumEU Beschwerdeverfahren gegenüber US-Organisation/-Unternehmen in gewerblichen Angelegenheiten, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en
Verfahrensregeln des „Informal Panel of EU DPAs“ gemäß EU-US Data Privacy Framework, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-informal-panel-eu-dpas-according-eu-us_en

39 Information Note on the redress mechanism for EU/EEA individuals in relation to alleged violations of U.S. law with respect to their data collected by U.S authorities competent for national security, abrufbar unter https://www.edpb.europa.eu/system/files/2024-04/edpb_information-note_dpf-redress-mechanism-national-security-purposes_en.pdf; Template Complaint Form to the U.S. Office of the Director of National Intelligence's Civil Liberties Protection Officer (CLPO)1 Redress mechanism for EU/EEA individuals in relation to alleged violations of U.S. law with respect to their data collected by U.S authorities competent for national security Adopted on 17 April 2024, abrufbar unter: https://www.edpb.europa.eu/system/files/2024-04/edpb_dpf_template-complaint-form_national-security-purposes_en.pdf; Rules of Procedure on the cooperation and respective roles of national SAs and the EDPB Secretariat regarding the submission of complaints in the redress mechanism available to EU individuals in relation to alleged violations of U.S law with respect to their data collected by U.S. authorities competent for national security Adopted on 17 April 2024, abrufbar unter: https://www.edpb.europa.eu/system/files/2024-04/edpb_rules-of-procedure_national-security-purposes_en.pdf

40 EU-US Data Privacy Framework FAQ für europäische Bürgerinnen und Bürger, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en

41 EU-US Data Privacy Framework FAQ für europäische Unternehmen, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en

42 Informationen zum Beschwerdeverfahren nach EU-U.S.-DPF, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Beschwerdeverfahren-DPF.html
Informationen zur Datenübermittlung in die USA nach dem Schrems-II Urteil, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Auswirkungen-Schrems-II-Urteil.html

43 Bericht der Europäischen Kommission zu Angemessenheitbeschlüssen nach Richtlinie 95/46/EG vom 15. Januar 2024, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0007

44 Arbeitsdokument der Europäischen Kommission zu Angemessenheitbeschlüssen nach Richtlinie 95/46/EG vom 15. Januar 2024, abrufbar unter: https://commission.europa.eu/document/download/f8229eb2-1a36-4cf5-a099-1cd001664bff_en?filename=JUST_template_comingsoon_Commission%20Staff%20Working%20Document%20-%20Report%20on%20the%20first%20review%20of%20the%20functioning.pdf

45 Schreiben des EDSA zum angemessenen Datenschutzniveau vom 5. Dezember 2024, abrufbar unter: https://www.edpb.europa.eu/system/files/2024-12/edpb_letter_20241205_european-commission-review-of-11-existing-adequacy-decisions_en.pdf

Treffens der G7-Datenschutzbehörden und der Global Privacy Assembly verabschiedet wurden.

Querverweise:

4.5.2 G7 DPA Roundtable, 4.3 46. Jahreskonferenz der Global Privacy Assembly

4.2.5 Coordinated Enforcement Framework Action 2024

Die europäischen Datenschutzaufsichtsbehörden führten auch in diesem Berichtszeitraum eine gemeinsame Durchsetzungsmaßnahme („Coordinated Enforcement Action", CEA) durch. Diese erfolgt auf Basis eines Beschlusses des Europäischen Datenschutzausschusses (EDSA) vom Oktober 2020 mit dem Zweck, einen koordinierten Durchsetzungsrahmen (Coordinated Enforcement Framework – CEF)[46] einzurichten. Als Thema für seine dritte koordinierte Durchsetzungsmaßnahme hat der EDSA auf meinen Vorschlag hin die Umsetzung des Auskunftsrechts gemäß Art. 15 DSGVO durch die für die Verarbeitung Verantwortlichen gewählt.

Das Auskunftsrecht ist eines der wichtigsten Datenschutzrechte betroffener Personen. Es ermöglicht ihnen, sich der Verarbeitung ihrer personenbezogenen Daten durch Verantwortliche bewusst zu werden und zu überprüfen, ob diese Verarbeitung rechtmäßig erfolgt. Damit kann das Auskunftsrecht Betroffenen als Grundlage dafür dienen, weitere Rechte auszuüben, wie etwa auf Berichtigung oder Löschung ihrer personenbezogenen Daten. Zudem ist das Auskunftsrecht eines der am häufigsten ausgeübten Betroffenenrechte. Die entsprechenden Vorgänge sind oft Gegenstand von Beschwerden bei den Datenschutzaufsichtsbehörden.

Der EDSA hat Leitlinien zum Auskunftsrecht[47] beschlossen, um zu einer einheitlichen Umsetzung dieses Rechts beizutragen. An der Erarbeitung dieser Leitlinien war meine Behörde als Co-Berichterstatter im EDSA maßgeblich beteiligt.[48] Auch die jüngste Rechtsprechung des Europäischen Gerichtshofs (EuGH) hat die Maßstäbe zur Umsetzung des Auskunftsrechts weiter vereinheitlicht.

Ziel der CEA 2024 war es, zu untersuchen, wie Verantwortliche das Auskunftsrecht in der Praxis umsetzen. Dabei sollte auch beurteilt werden, ob in den EDSA-Leitlinien einzelne Aspekte angepasst oder klargestellt werden müssten, und ob eine weitere Sensibilisierung von Verantwortlichen oder Betroffenen durch die Datenschutzaufsichtsbehörden sinnvoll sein kann.

Meine Behörde hat die Rolle des Hauptberichterstatters im EDSA für die CEA 2024 übernommen. Darüber hinaus habe ich im Rahmen meiner Zuständigkeit für die Datenschutzaufsicht über die Bundesverwaltung verschiedene Verantwortliche zu deren Umsetzung des Auskunftsrechts befragt. Meine hieraus gewonnenen Erkenntnisse flossen – ebenso wie die Ergebnisse von sieben weiteren an der CEA 2024 beteiligten deutschen Aufsichtsbehörden und von 22 Aufsichtsbehörden anderer europäischer Länder – in einen gemeinsamen Bericht des EDSA ein. In diesem Bericht[49] wurden Handlungsempfehlungen für den EDSA, für Verantwortliche und Betroffene erarbeitet. Daneben können nationale Aufsichts- und Durchsetzungsmaßnahmen auf Basis der gewonnenen Erkenntnisse erfolgen.

4.3 46. Jahreskonferenz der Global Privacy Assembly

Im Herbst 2024 hat der Information Commissioner von Jersey die 46. Jahreskonferenz der Global Privacy Assembly (GPA) ausgerichtet. Im Mittelpunkt der Beratungen standen Grundsatzfragen zum internationalen Datenschutz und zum Umgang mit neuen digitalen Technologien. Die Konferenz hat eine von mir vorgeschlagene Entschließung zu vertrauenswürdigen grenzüberschreitenden Datentransfers („Data Free Flow with Trust") angenommen.

Die GPA ist die größte internationale Vereinigung von Datenschutzbehörden und umfasst über 130 Mitglieder aus aller Welt. Auf der Kanalinsel Jersey fand vom 28. Oktober bis zum 1. November 2024 die 46. Jahreskonferenz der GPA statt, organisiert vom Büro des Jersey Information Commissioner.

Schwerpunkt der Reden und Podiumsdiskussionen der Konferenz waren Fragen der datenschutzgerechten Ausgestaltung von Anwendungen, die Funktionen und Algorithmen der Künstlichen Intelligenz nutzen. Ein wichtiger Aspekt in diesem Zusammenhang war der Schutz vulnerabler Gruppen. Zudem wurde beleuchtet,

---

46 Beschluss des EDSA vom 20. Oktober 2020, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en

47 Leitlinien 01/2022 zu den Rechten der betroffenen Personen – Auskunftsrecht, Version 2.1, angenommen am 28. März 2023, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_de

48 31. TB Nr. 3.3.5

49 Bericht des EDSA zur CEA 2024 – Umsetzung des Auskunftsrechts durch Verantwortliche, vom 16. Januar 2025, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-implementation-right-access_en

was die Datenschutzaufsichtsbehörden tun müssen, um für die Herausforderungen der Zukunft gut aufgestellt zu sein. Dazu gehört auch eine verstärkte Zusammenarbeit untereinander und mit Aufsichtsbehörden anderer Sektoren, z. B. den Wettbewerbsbehörden.

In einer der geschlossenen Sitzungen der Konferenz habe ich an einer Podiumsdiskussion zum Thema „LLMs (Large Language Models): Innovative Technologies and the Future of Privacy“ teilgenommen und dabei auf die Risiken, aber auch auf mögliche Lösungswege hingewiesen, die sich aus datenschutzrechtlicher Sicht für diese Technologie ergeben können.

Zudem habe ich, wie in jedem Jahr üblich, zu den Aktivitäten und neuesten Papieren der „International Working Group on Data Protection in Technology“ berichtet, die unter Leitung meines Hauses steht und eine unabhängige Arbeitsgruppe im Umfeld der GPA ist.

Die 46. Jahreskonferenz der GPA hat insgesamt fünf Entschließungen angenommen:

- → Entschließung zu „Data Free Flow with Trust“ (DFFT)
- → Entschließung zu datenschutzrechtlichen Zertifizierungsverfahren
- → Entschließung zu Neurotechnologie und Datenschutz
- → Entschließung zu Überwachungstechnologien
- → Entschließung zu den Regeln und Verfahren der GPA

Die Entschließung zu DFFT wurde durch mein Haus initiiert und zusammen mit dem Europäischen Datenschutzbeauftragtem erarbeitet. Sie erkennt die Notwendigkeit internationaler Datenströme für die Gesellschaft, Forschung und Wirtschaft an, betont aber auch, dass sich hieraus Risiken für den Schutz personenbezogener Daten und der Privatsphäre ergeben können. Die Entschließung ruft daher Gesetzgeber und Behörden dazu auf, Instrumente für sichere grenzüberschreitende Datenübermittlungen zu entwickeln und dabei die folgenden Kern-Elemente von DFFT besonderes zu beachten (sog. „essential elements of DFFT“): Betroffenenrechte, Sicherheit der Verarbeitung, Zugang zu wirksamen und durchsetzbaren Rechtsbehelfen, unabhängige Aufsicht und den Zugang staatlicher Stellen zu personenbezogenen Daten. Die Entschließung ist die erste Erklärung der GPA, die ausdrücklich dem Konzept DFFT gewidmet ist. DFFT ist ein zentrales Thema auch auf Ebene der Digitalminister der G7-Staaten und der OECD.

Da gemäß Satzung der GPA nur zwei aufeinanderfolgende Mandate im Leitungsgremium der GPA zulässig sind, bin ich nach vier Jahren Zugehörigkeit als gewähltes Mitglied mit Ablauf der 46. Jahreskonferenz aus dem sog. Executive Committee ausgeschieden. Als neues Mitglied wurde die Datenschutzbehörde von Südafrika gewählt. Für Europa bzw. die Länder der EU wird weiterhin die Datenschutzbehörde Bulgariens dem Executive Committee angehören.

Die nächste Jahreskonferenz der GPA wird im September 2025 in Seoul, Republik Korea, stattfinden.

Querverweise:

4.4 Berlin Group, 4.5.2 G7 DPA Roundtable

4.4 Berlin Group

Die Internationale Arbeitsgruppte für Datenschutz in der Technologie (International Working Group on Data Protection in Technology, IWGDPT), die auch unter der Bezeichnung „Berlin Group“ bekannt ist, hat unter der Leitung meines Hauses zwei Treffen durchgeführt und vier thematische Arbeitspapiere verabschiedet. Die Gruppe hat ihren Fokus auf wichtige Zukunftstechnologien weiter geschärft.

Die IWGDPT wurde 1983 auf Initiative des damaligen Berliner Datenschutzbeauftragten als unabhängige Experten-Gruppe zum Thema „Datenschutz in der Telekommunikation“ gegründet und ist daher auch als „Berlin Group“ bekannt. Der Arbeitsbereich der Gruppe hat sich in den vergangenen Jahren auf den gesamten Bereich der Technologie erweitert, mit einem speziellen Fokus auf wichtige Zukunftstechnologien, die innerhalb der nächsten Jahre Marktreife erlangen und damit für eine Vielzahl von Nutzenden relevant werden können. Zu diesem Zweck wird regelmäßig eine „Future Foresight“-Diskussion durchgeführt.

Ein besonderes Kennzeichen der Berlin Group ist ihre heterogene Zusammensetzung aus Mitgliedern der Bereiche Datenschutzbehörden, Wissenschaft, Forschung, Nichtregierungsorganisationen und internationalen Organisationen. Dadurch gelingt es, eine vielfältige und hervorragende Expertise für die verschiedenen Arbeitspapiere der Gruppe zusammenzubringen.

Das Ziel der Berlin Group besteht darin, in ihren Arbeitspapieren zielgruppenorientierte Empfehlungen und Leitlinien für einen datenschutzgerechten Umgang mit relevanten Zukunftstechnologien zu einem frühen Zeitpunkt vorzulegen, so dass die betroffenen Beteiligten, z. B. Gesetzgeber oder Entwickler von neuen Angeboten und Dienstleistungen, diese für ihre weiteren Entscheidungen und Verfahren entsprechend frühzeitig bereits berücksichtigen können.

Seit 1989 steht die Berlin Group in einem besonderen Verhältnis zur Global Privacy Assembly (GPA) mit einem regelmäßigen „Update-Report“ des Vorsitzes während der regelmäßigen Jahreskonferenzen der GPA. Im Rahmen der 46. GPA Jahreskonferenz 2024 habe ich diesen Bericht der Berlin Group vorgestellt. Meine Behörde hat im März 2021 den Vorsitz der Berlin Group übernommen.

Vier Arbeitspapiere der Berlin Group veröffentlicht

Unter meinem Vorsitz konnten wir in der Berlin Group im Juni 2024 Arbeitspapiere zur Gesichtserkennungstechnologie und zum Digitalen Zentralbankgeld abstimmen und veröffentlichen. Im Dezember 2024 konnten wir weitere Arbeitspapiere zu Large Language Models (LLMs) und Data Sharing veröffentlichen. [50]

Technologien zur **Gesichtserkennung** finden weltweit zunehmend Verbreitung, gerade angesichts der aktuellen Entwicklungen im Bereich der Künstlichen Intelligenz. Es handelt sich um eine biometrische Technologie, welche Gesichtsmerkmale von Personen analysiert und zur Identifizierung mit entsprechenden Datenbanken vergleicht. Auf diese Weise können Personen nicht nur in Einzelfällen erkannt, sondern auch über längere Zeiträume Informationen etwa zu ihren Bewegungsabläufen, politischen Ansichten oder Gesundheitsdaten mit ihnen verknüpft werden. So können viele verschiedene personenbezogene Daten ohne das Wissen der Betroffenen gesammelt und dabei individuelle Profile einzelner Personen erstellt werden. Vor allem der Einsatz im öffentlichen Raum birgt hohe Risiken für die Freiheiten und Rechte der betroffenen Personen. Das Gleiche gilt für Gesichtserkennungstechnologien, die Emotionen erkennen oder gar Charakterzüge aus bestimmten biometrischen Eigenschaften ableiten sollen und aufgrund der Ungenauigkeit und der extrem hohen Diskriminierungsrisiken von der Berlin Group abgelehnt werden.

Bei **digitalem Zentralbankgeld** handelt es sich um von Zentralbanken gestützte digitale Währungen. Im Gegensatz zu dem sonst im digitalen Zahlungsverkehr üblichen Geschäftsbankengeld handelt es sich aber um echtes Zentralbankgeld, welches nur von der Zentralbank geschaffen werden kann. Es kann somit als eine digitale Version des Bargelds angesehen werden. Digitales Zentralbankgeld liegt weltweit zunehmend im Trend. Auch die EU hat die Einführung des Digitalen Euros vorgeschlagen. [51] Bei unzureichender Beachtung des Datenschutzes könnten Regierungen, Zentralbanken und involvierte Finanzinstitutionen jedoch einen noch nicht dagewesenen Zugang zu den Finanzinformationen von Personen und Personengruppen erhalten. Wenn der Digitale Euro ein Erfolg werden soll, müssen die Bürgerinnen und Bürger darauf vertrauen können, dass die datenschutzfördernden Eigenschaften des Bargelds soweit wie möglich erhalten bleiben und nicht sämtliche ihrer Transaktionen überwacht und gar einer Vorratsdatenspeicherung zugeführt werden.

LLMs sind mathematische Modelle, die mithilfe von Datenverarbeitungstechniken der Künstlichen Intelligenz (KI) entwickelt werden, um Aufgaben im Zusammenhang mit natürlicher Sprache auszuführen. Der Stand der Technik hat sich in den vergangenen Jahren erheblich weiterentwickelt, wobei einige LLMs für bestimmte Aufgaben Fähigkeiten zur Verarbeitung natürlicher Sprache auf menschlicher und sogar Expertenebene demonstrieren. Da es sich bei LLMs um komplexe Technologien handelt, die verschiedene Risiken für den Datenschutz und die Privatsphäre mit sich bringen, muss jede verhältnismäßige Analyse die Technologie aus mehreren Perspektiven betrachten. Es ist nicht nur notwendig, LLMs aus der Sicht der Technologie selbst zu analysieren, sondern gleichermaßen aus der Perspektive der von ihnen ausgehenden Risiken für Privatsphäre und Datenschutz unter Einbeziehung von Empfehlungen zur Reduzierung oder Beseitigung dieser Risiken. Nur mit einem Verständnis von LLMs aus der Sicht dieser verschiedenen Perspektiven können sich Datenschutzbehörden in die Lage versetzen, diese neue Situation effektiv zu regulieren und darauf zu reagieren.

Die Idee von **„Data Sharing“** basiert auf der Beobachtung, dass Daten mit anderen Datenquellen kombiniert werden können, um neue Erkenntnisse zu gewinnen, neue Produkte und Dienstleistungen zu entwickeln und das soziale und wirtschaftliche Wachstum voranzutreiben. Durch die Erfassung umfangreicherer und vielfältigerer Datensätze können Unternehmen Innovation und Wachstum auch im breiteren gesellschaftlichen Interesse vorantreiben. Ebenso kann der Austausch von Daten durch öffentliche Behörden eine bessere Koordinierung und Reaktion auf Krisen wie Pandemien oder Naturkatastrophen ermöglichen. Gleichzeitig geht mit der Datenweitergabe häufig die Verarbeitung personenbezogener Daten einher. Bei der Weitergabe personenbezogener Daten ist die strikte Einhaltung datenschutzrechtlicher Grundsätze von größter Bedeutung. Es stellt

50 Die Papiere stehen auf meiner Website unter www.iwgdpt.org zum Download bereit.

51 Kommissionsvorschlag zur Einführung des Digitalen Euros, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52023PC0369

eine wesentliche Säule für die Wahrung des Vertrauens zwischen betroffener Person und Datennutzer dar. Der „By-design"-Ansatz beinhaltet die Einbettung von Datenschutz- und ethischen Gesichtspunkten schon in die Gestaltung von Datensystemen und stellt so sicher, dass von Anfang an verantwortungsvoll mit Daten umgegangen wird. Durch die Übernahme dieses Ansatzes können Unternehmen ihre Datenverwaltung verbessern und Vertrauen bei den betroffenen Personen aufbauen, was letztendlich zu einer effektiveren und verantwortungsvolleren Nutzung und Weitergabe von Daten führt.

Die veröffentlichten Arbeitspapiere beschreiben Nutzungsmöglichkeiten der betrachteten Technologien und stellen sowohl Risiken und Herausforderungen als auch praktische Empfehlung für eine datenschutzkonforme Umsetzung vor.

Treffen der Berlin Group in Oslo und Brüssel

Bei den Treffen der Berlin Group im Juni 2024 in Oslo und im November 2024 in Brüssel wurden neben der Arbeit an Arbeitspapieren neue Arbeitsschwerpunkte ausgewählt. Hierzu gehören die Themen „Global Opt-Out-Preference Signals" (z. B. in Internet-Browsern), „Confidential Cloud Computing / Trusted Execution Environments", Digitaler Nachlass („Data after life" bzw. „Data post mortem") und Gemeinsame Funk-Kommunikation und Sensorik („Joint Communication and Sensing")

Zudem hat die Gruppe eine Diskussion zu „Future Foresight" durchgeführt, die u. a. mein Haus mit einer Präsentation unterstützt hat. Dies soll dazu dienen, mittelfristig relevante Zukunftstechnologien zu identifizieren.

Querverweis:

9.6 Future Foresight

4.5 Weitere Gremien

4.5.1 ETIAS-Beratungsgremium für Grundrechte

Das künftige Europäische Reiseinformations- und -genehmigungssystem (ETIAS) wird etwa 1,4 Milliarden Drittstaatsangehörige aus über 60 Staaten betreffen, wenn sie in eines von 30 europäischen Ländern reisen. Derzeit erfolgt die organisatorische und technische Umsetzung. Das ETIAS-Beratungsgremium für Grundrechte setzt sich dabei für die Wahrung der Grundrechte, und insbesondere den Schutz personenbezogener Daten und die Nichtdiskriminierung ein.

ETIAS richtet sich an Drittstaatsangehörige, die in die EU einreisen möchten und von der Visumspflicht befreit sind.[52] Mit dem System soll überprüft werden, ob die Anwesenheit dieser Personen ein Risiko für die Sicherheit, ein Risiko der illegalen Einwanderung oder ein hohes Epidemierisiko bedeutet. Diese Prüfung erfolgt insbesondere mittels sog. ETIAS-Überwachungsregeln. Das ist ein Profiling-Algorithmus, der auf spezifischen Risikoindikatoren beruht. Die Nutzung der Großdatenbank ETIAS wird auch zum Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten möglich sein.

Derzeit erfolgt auf EU-Ebene und in den Mitgliedstaaten die Konkretisierung und Umsetzung der Vorgaben der sog. ETIAS-Verordnung. Das betrifft auch zahlreiche Bundes- und Landesbehörden in Deutschland.[53] Die Vorbereitungen für die Inbetriebnahme des ETIAS werden seit einigen Jahren vorangetrieben. Der Termin für die Inbetriebnahme wurde bereits mehrfach verschoben. Noch im Berichtsjahr wurde verkündet, dass ETIAS voraussichtlich im Jahr 2025 in Betrieb gehen soll.

Im November 2022 wurde das ETIAS-Beratungsgremium für Grundrechte eingerichtet.[54] In dem Gremium sind der Europäische Datenschutzbeauftragte, die Agentur der Europäischen Union für Grundrechte und der Europäische Datenschutzausschuss (EDSA) sowie der Grundrechtsbeauftragte und ein Vertreter des Konsultationsforums für Grundrechte von Frontex, der Europäischen Agentur für die Grenz und Küstenwache, vertreten. Den EDSA vertritt einer meiner Mitarbeitenden, der zudem im Berichtsjahr als Vorsitzender des ETIAS-Beratungsgremiums für Grundrechte wiedergewählt wurde.

Das Gremium hat sich im Berichtsjahr viermal am Sitz von Frontex getroffen und in beratender Funktion an zahlreichen weiteren Frontex-Arbeitsgruppen teilgenommen. Es berät ad hoc in den jeweiligen Treffen, entwickelt und verabschiedet aber auch auf Anfrage oder initiativ Positionen und Leitlinien zu verschiedenen Fragestellungen, die von Bedeutung für die Implementierung von ETIAS sind. So wurde etwa die Leitlinie zu Diskriminierungsrisiken im Kontext der ETIAS-Überwachungsregeln verabschiedet und an einer zweiten

52 Verordnung (EU) 2018/1240 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32018R1240&qid=1739900858368

53 Vgl. Artikel 2 §§ 1 und 2 BGBl. 2023 Teil I Nr. 106, abrufbar unter: https://www.recht.bund.de/bgbl/1/2023/106/VO.html

54 31. TB Nr. 3.5.3

Leitlinie zur Wahrung des Rechts auf einen wirksamen Rechtsbehelf und ein faires Verfahren gearbeitet. Weitere Schwerpunkte der Beratungstätigkeit des Gremiums betrafen Datenschutzfolgenabschätzung, Verantwortlichkeiten und Betroffenenrechte sowie die Methodologie zu den ETIAS-Überwachungsregeln.

Weitere Informationen zum ETIAS-Beratungsgremium für Grundrechte, Jahresberichte sowie das Arbeitsprogramme sind auch online einsehbar. [55]

Querverweis:

4.2.3 Bericht aus dem CSC

4.5.2 G7 DPA Roundtable

Die Datenschutzbehörden der G7-Staaten (G7 Data Protection Authorities – DPA) sind im Rahmen der italienischen G7-Präsidentschaft im Oktober 2024 zu ihrem jährlichen Roundtable-Treffen in Rom zusammengekommen. Im Fokus der Diskussionen standen insbesondere die Themen Data Free Flow with Trust (DFFT), also die Frage vertrauenswürdiger internationaler Datenübermittlung, sowie aktuelle Entwicklungen und datenschutzrechtliche Herausforderungen im Bereich der Künstlichen Intelligenz (KI).

Zur Vorbereitung der Konferenz in Rom haben die Datenschutzbehörden der G7- Staaten in drei Arbeitsgruppen zu den Themenkomplexen „Data Free Flow with Trust“ (DFFT), „Emerging Technologies“ (aktuelle technologische Entwicklungen) und „Enforcement Cooperation“ (internationale Kooperation im Bereich der Rechtsdurchsetzung) zusammengearbeitet. Die Ergebnisse der Arbeitsgruppen wurden, wie schon in den Jahren zuvor, in einem Communiqué [56] zusammengefasst.

Data Free Flow with Trust

Im Hinblick auf DFFT erkennt das Communiqué die wirtschaftlichen und gesellschaftlichen Vorteile an, die sich durch grenzüberschreitende Datenflüsse ergeben. Gleichzeitig weisen die G7 DPAs aber auch auf die Risiken für den Schutz personenbezogener Daten und der Privatsphäre hin, die entsprechende Datentransfers mit sich bringen. Die G7-Datenschutzbehörden betonen daher erneut, dass Vertrauen („Trust“) ein wesentlicher Bestandteil des Konzeptes des DFFT ist und hohe Datenschutzstandards Grundvoraussetzung für den freien Datenverkehr sind. Zu diesem Zweck bekräftigen die G7-Datenschutzbehörden den Ansatz, auf Gemeinsamkeiten und Elemente der Übereinstimmung (Konvergenz) zwischen bestehenden Regulierungsansätzen und Transferinstrumenten hinzuarbeiten, um das Zusammenwirken (Interoperabilität) von verschiedenen Rechtssystemen und –instrumenten zu fördern.

Um diesen insbesondere auch von den Digitalministern der G7-Staaten geteilten Ansatz zur Umsetzung des DFFT-Konzepts weiterzuentwickeln, hat der G7 DPA Roundtable im Jahr 2024 eine vergleichende Analyse unterschiedlicher Zertifizierungsmechanismen für grenzüberschreitende Datentransfers [57] erarbeitet, die in Rom einstimmig angenommen wurde. Das Projekt wurde durch mein Haus initiiert und gemeinsam mit der französischen Datenschutzbehörde (Commission Nationale de l’Informatique et des Libertés - CNIL) federführend im Rahmen der DFFT-Arbeitsgruppe der G7 DPAs ausgearbeitet. Die Analyse weist auf Gemeinsamkeiten und Unterschiede zwischen Zertifizierungen nach der DSGVO und den sogenannten Global Cross-Border Privacy Rules (CBPR) hin und leistet damit einen praktischen Beitrag, um die Konvergenz zwischen diesen Transferinstrumenten zu fördern. In diesem Kontext nimmt mein Haus darüber hinaus als bisher einzige EU-Datenschutzbehörde beratend an den Treffen der Mitglieder des Global CBPR-Systems [58] teil (sog. Global CBPR Forum), um die G7-Arbeit zu präsentieren und im Sinne der Konvergenz für ein höheres Schutzniveau der CBPR-Regeln zu werben.

Meine Behörde hat 2024 zusammen mit der britischen Datenschutzbehörde (Information Commissioner‘s Office des Vereinigten Königreichs - ICO UK) den Co-Vorsitz über die DFFT-Arbeitsgruppe des G7 DPA Roundtables übernommen.

Künstliche Intelligenz

Der G7 DPA Roundtable hat seine Arbeiten zu KI auch im vergangenen Jahr fortgesetzt und sich aufbauend auf dem 2023 in Tokio verabschiedeten „Statement on Gene-

55 ETIAS Fundamental Rights Guidance Board auf der Webseite von Frontex: https://www.frontex.europa.eu/what-we-do/etias/etias-fundamental-rights-guidance-board/

56 Communiqué zum G7 Roundtabel 2024 vom 11. Oktober 2024, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/2024_Communique.pdf

57 Analyse unterschiedlicher Zertifizierungsmechanismen für grenzüberschreitende Datentransfers des G7 Roundtable vom 11. Oktober 2024 abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/2024_Comparative-analysis.pdf

58 Aktuell Vereinigte Staaten, Kanada, Japan, Australien, Südkorea, Singapur, Taiwan, Mexiko und Australien sowie Vereinigtes Königreich, Dubai, Bermuda und Mauritius als „Associates“.

rative AI“ [59] insbesondere mit Fragen der KI-Governance und spezifischen Auswirkungen von KI-Technologien auf Kinder und Heranwachsende beschäftigt. Hierzu hat der Roundtable zwei Erklärungen verabschiedet, an denen mein Haus maßgeblich beteiligt war.

Mit dem „Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI” [60] machen die G7 DPAs deutlich, dass Datenschutzbehörden eng in die Regulierung von KI-Technologien einbezogen werden müssen, um eine rechtmäßige und grundrechtswahrende Nutzung von KI zu ermöglichen und sicherzustellen. Datenschutzbehörden verfügen bereits jetzt über umfassende Expertise in Bereichen, die für die KI-Regulierung zentral sind, etwa in Bezug auf datengestützte Verarbeitungsprozesse und Fragen der Fairness, Transparenz und Sicherheit technologischer Systeme. Das „Statement on AI and Children“ [61] weist hingegen auf potenzielle datenschutzbezogene Auswirkungen und Risiken von KI-Technologien für Kinder und Heranwachsende hin und ruft Entwicklerinnen und Entwickler sowie Nutzerinnen und Nutzer von KI-Systemen auf, diese Aspekte bei der Entwicklung von KI-Systemen miteinzubeziehen und KI-Systeme altersgerecht zu gestalten.

Ergänzend zu dem in Rom verabschiedeten Communiqué hat der G7 DPA Roundtable in einem Aktionsplan [62] konkrete Maßnahmen festgelegt, um die Positionen der G7-Datenschutzbehörden in praktische Ergebnisse umzusetzen.

4.5.3 High Level Group zur EU-Vorratsdatenspeicherung

Die EU-Arbeitsgruppe „High Level Group on access to data for effective law enforcement“ hat Empfehlungen zum Zugriff von Strafverfolgungsbehörden auf Daten im Netz entwickelt. Meine Behörde entsendet für den Europäischen Datenschutzausschuss (EDSA) einen Experten. Neue Vorschläge müssen insbesondere die Rechtsprechung des Europäischen Gerichtshofs (EuGH) zur Vorratsdatenspeicherung beachten.

Auf Initiative der schwedischen Ratspräsidentschaft und der Europäischen Kommission wurde im Juni 2023 die sog. „High Level Group on access to data for effective law enforcement“ (HLG) ins Leben gerufen. Die HLG verfolgt dabei gemäß ihrem Mandat das Ziel, die Verfügbarkeit wirksamer Strafverfolgungsinstrumente zur Kriminalitätsbekämpfung sicherzustellen und zur Verbesserung der öffentlichen Sicherheit im digitalen Zeitalter unter uneingeschränkter Achtung der Grundrechte beizutragen. Dafür soll das Gremium Empfehlungen für die Weiterentwicklung der Unionsrechts aussprechen. [63]

Die HLG tagt auf Ebene eines Plenums sowie in drei Arbeitsgruppen. Ihre Arbeit wurde im Wesentlichen von Vertretern der Strafverfolgungsbehörden in den Mitgliedstaaten getragen. Zudem entsendete auch der EDSA Experten. Ich bin durch einen meiner Mitarbeitenden als Experte des EDSA in der Arbeitsgruppe 2 („Access to data at rest in a provider’s system“) vertreten, die sich mit dem Zugang von Strafverfolgungsbehörden zu Daten in den Systemen von Dienstanbietern beschäftigt.

Im Juni 2024 hat die HLG als vorläufiges Ergebnis ihrer Arbeit 42 Empfehlungen („Recommendations“) für die weitere Entwicklung der Politik und Gesetzgebung der Europäischen Union veröffentlicht. [64] Die Empfehlungen betreffen insbesondere die Themen Verschlüsselung, Zusammenarbeit zwischen Wirtschaft und Strafverfolgungsbehörden sowie die Notwendigkeit harmonisierter Regeln für die Vorratsdatenspeicherung.

Der EDSA hat am 4. November 2024 ein Statement zu den Empfehlungen verabschiedet. [65] Meine Mitarbeitenden waren hierbei als federführende Berichterstatter im EDSA tätig. Mit dem Statement werden erste, nicht abschließende Bedenken des EDSA adressiert, da einige der von der HLG vorgeschlagenen Maßnahmen zu erheblichen Eingriffen in die Grundrechte der Betroffenen führen könnten. Der EDSA äußert Verständnis für den Wunsch nach Harmonisierung der Regelungen in der EU, doch mahnt er zugleich die strenge Beachtung der

---

59 G7 Rountable Stellungnahme zu generativer KI vom 21. Juni 2023, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/2023_Statement-AI.pdf

60 G7 Roundtable Stellungnahme zur Regulieurng von KI-Technologien vom 11. Oktober 2024, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/2024_Statement-Trustworthy-AI.pdf

61 G7 Roundtable Stellungnahme zu Künstlicher Intelligenz und Kindern vom 11. Oktober 2024, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/2024_Statement-AI-Children.pdf

62 Action Plan 2024 des G7 Roundtable vom 11. Oktober 2024, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/2024_Action-Plan.pdf

63 Weiter Informationen auf der Website der HLG, abrufbar unter https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en

64 Empfehlungen der HLG, abrufbar unter https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en?filename=Recommendations%20of%20the%20HLG%20on%20Access%20to%20Data%20for%20Effective%20Law%20Enforcement_en.pdf

65 Statement 5/2024 des EDSA vom 4. November 2024, abrufbar unter https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf

Vorgaben der EuGH-Rechtsprechung an. Außerdem fordert der EDSA, dass alle technischen Anforderungen an Anbieter elektronischer Kommunikationsdienste, die das Potential haben, in individuelle Grundrechte einzugreifen, nur auf der Grundlage einer gesetzlichen Regelung erfolgen dürfen, die die Grundrechte wahrt und als notwendig und verhältnismäßig in einer demokratischen Gesellschaft angesehen werden kann, damit nicht eine Maßnahme, die sich nur gegen Einzelne oder kleine Personengruppen richtet, den Schutz der Vertraulichkeit der Kommunikation unterschiedslos für alle Nutzenden schwächt. Unter Verweis auf die Podchasov-Rechtsprechung des EGMR weist der EDSA außerdem in seinem Statement auf mögliche unverhältnismäßige Grundrechtseingriffe und Gefahren für die technische Sicherheit hin, die von einer Durchbrechung der Ende-zu-Ende-Verschlüsselung gegenüber allen Nutzenden von elektronischer Kommunikation ausgehen können.

Die im Statement geäußerten Bedenken des EDSA wurden nur teilweise in dem Ende November veröffentlichten „Concluding Report“ der HLG aufgegriffen.[66] Der Report fordert die Europäische Kommission auf, entsprechend der unterbreiteten Vorschläge der HLG europäische Rechtsakte – allem voran harmonisierte Regelungen zur Vorratsdatenspeicherung – auf den Weg zu bringen. Ich werde den Fortgang kritisch begleiten und mich dafür einsetzen, dass der Schutz der Privatsphäre nicht durch eine Schwächung der Sicherheit der Kommunikation auf technischer Ebene ausgehebelt wird.

66 „Concluding Report“ der HLG vom 15. November 2024, abrufbar unter https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data%20for%20effective%20law%20enforcement_en.pdf

5 Gesetzgebung

5.1 Gesundheit und Forschung

5.1.1 Bundesinstitut für Prävention und Aufklärung in der Medizin

Mit dem Gesetz zur Stärkung der Öffentlichen Gesundheit hat die Bundesregierung in diesem Jahr ein Gesetz auf den Weg gebracht, um das Bundesinstitut für Prävention und Aufklärung in der Medizin (BIPAM) zu errichten. Das BIPAM soll die bisher von der Bundeszentrale für gesundheitliche Aufklärung (BZgA) wahrgenommenen Aufgaben sowie Teile des bisherigen Aufgabenspektrums des Robert Koch-Instituts (RKI) übernehmen. Die mit dieser Aufgabenübertragung einhergehende Datenverarbeitung sehe ich in Teilen kritisch.

Das BIPAM-Errichtungsgesetz ermöglicht dem neu zu errichtenden Bundesinstitut eine umfassende Verarbeitung von Daten, insbesondere Gesundheitsdaten, die als besondere Kategorie personenbezogener Daten gemäß Art. 9 DSGVO nur unter strengen Voraussetzungen verarbeitet werden dürfen. Die Datenverarbeitung durch BIPAM soll zum Zwecke der Analyse des Gesundheitszustands der Bevölkerung, zu den gesundheitlichen Auswirkungen durch Klima und Umwelt sowie zu gesundheitsrelevanten Verhaltensweisen erfolgen, um auf die gewonnenen Erkenntnisse gestützte Präventionsmaßnahmen zu entwickeln.

Zur Legitimation jeder Verarbeitung von Gesundheitsdaten, die das BIPAM zukünftig vornehmen soll, bedarf es einer konkreten Rechtsgrundlage, die den Anforderungen der DSGVO genügt. Dies gilt auch und insbesondere für personenbezogene Daten, die bisher vom RKI auf Grundlage von Einwilligungserklärungen der Betroffenen verarbeitet wurden und nunmehr an das BIPAM übertragen und dort weiterverarbeitet werden sollen. Sowohl im Vorfeld als auch während der Ressortberatungen habe ich wiederholt darauf hingewiesen, dass die Heranziehung der bereits bestehenden Einwilligungserklärungen Rechtsunsicherheiten birgt, da nicht feststeht, inwieweit diese einer entsprechenden Auslegung (Wechsel der verantwortlichen Stelle) zugänglich sind – insbesondere im Hinblick auf die strengen Vorgaben des Art. 9 Abs. 2 lit. a) DSGVO.

Hierdurch konnte ich zumindest erreichen, dass die Gesetzesbegründung insoweit um einen Hinweis ergänzt wurde, als dass es jeweils noch einer konkreten Prüfung im Einzelfall bedarf, ob die konkreten Einwilligungserklärungen tatsächlich als Rechtsgrundlage für eine Datenverarbeitung durch das BIPAM herangezogen werden können.

Am 17. Juli 2024 wurde der Entwurf des Gesetzes zur Stärkung der Öffentlichen Gesundheit vom Bundeskabinett beschlossen. Danach sollte das Bundesinstitut zum 1. Januar 2025 errichtet werden, wobei die Diskussion um eine mögliche Namensänderung des Instituts in „Bundesinstitut für öffentliche Gesundheit (BIÖG)“ noch nicht abgeschlossen war.

Nach dem Bruch der Regierungskoalition Ende 2024 kam es nicht mehr zu einer Verabschiedung des Gesetzes durch den Bundestag, so dass offen ist, ob und inwieweit das Gesetzesvorhaben in der 21. Legislaturperiode wieder aufgegriffen wird.

5.1.2 Gesundheitsversorgungsstärkungsgesetz

Mit dem Gesetz zur Stärkung der Gesundheitsversorgung in der Kommune (Gesundheitsversorgungsstärkungsgesetz – GVSG) werden zusätzliche Rechtsgrundlagen geschaffen, um Fehlverhalten im Gesundheitswesen gezielter bekämpfen zu können.

Durch das GVSG werden in § 197a SGB V die bestehenden Rechtsgrundlagen zur Bekämpfung von Fehlverhalten im Gesundheitswesen erweitert. Dies betrifft in erster Linie Daten von Leistungserbringern, wobei auch Versichertendaten betroffen sein können. Der anlassbezogene Datenaustausch zwischen sog. „Fehlverhaltensbekämpfungseinrichtungen“ und anderen öffentlichen Stellen des Gesundheitswesens wird ausgeweitet unter strikter Beachtung der Zweckbindung, dass der Datenaustausch zur Verhinderung, Aufdeckung, Feststellung

oder Bekämpfung von Fehlverhalten im Gesundheitswesen erforderlich sein muss. Anlassunabhängig dürfen Fehlverhaltensbekämpfungseinrichtungen ihre eigenen Datenbestände mit denen anderer Krankenkassen sowie den Landesverbänden der Krankenkassen und dem GKV-Spitzenverband (GKV-SV) zusammenführen, damit diese als Trainingsmaterial für eine Künstliche Intelligenz dienen können, die später einmal wiederkehrende Fehlverhaltensmuster erkennen können soll.

Parallel enthält die Vorschrift einen Auftrag an den GKV-SV, dem Bundesministerium für Gesundheit (BMG) ein Konzept für den Aufbau einer zentralen bundesweiten Betrugspräventionsdatenbank vorzulegen, die den Krankenkassen Hinweise über Sachverhalte oder Auffälligkeiten gibt, die auf Fehlverhalten im Gesundheitswesen hindeuten. Für dieses Konzept soll der GKV-SV ein externes Gutachten vergeben, das auch auf datenschutzrechtliche Aspekte und weiteren gesetzgeberischen Regelungsbedarf eingehen soll. Im Austausch mit dem BMG wurde mir zugesagt, mich bei der Prüfung des Konzepts zur Betrugspräventionsdatenbank einzubeziehen.

Des Weiteren hat das BMG auf meine Anregung hin den Datenschutz an zwei Stellen nachjustiert: Bei der anlassabhängigen Übermittlung von Versichertendaten werden diese bereits vor der Übermittlung pseudonymisiert, wenn keine Hinweise auf eine eigene Mitwirkung am Fehlverhalten vorliegen, und anonymisiert, sobald es der Verarbeitungszweck zulässt. Bei der anlassunabhängigen Übermittlung von Versichertendaten an den zusammengeführten Datenbestand zum Training der Künstlichen Intelligenz muss der Versichertenbezug bereits vor der Übermittlung gelöscht werden.

5.1.3 Gesetz zur Reform der Notfallversorgung

Im laufenden Gesetzgebungsverfahren zur Reform der Notfallversorgung wurden einige meiner Kritikpunkte aufgegriffen – andere hingegen sind noch offen.

Mit dem Gesetz zur Reform der Notfallversorgung werden mehrere gesundheitspolitische Reformvorhaben verfolgt: Zum einen sollen mit der bisherige Terminservicenummer 116117 Aufgaben im Bereich der Akutfallvermittlung (Akutleitstelle) verbunden werden. Als Baustein eines Gesundheitsleitsystems soll die Akutleitstelle mit den Rettungsleitstellen vernetzt werden. Dazu wird auch eine gesetzliche Grundlage geschaffen, um personenbezogene Daten zu verarbeiten. In diesem Rahmen wird es den Akutleitstellen ermöglicht, Anrufe aufzuzeichnen und zu speichern. Hier war zunächst vorgesehen, dass auch Gespräche, die lediglich der Terminvereinbarung dienen, aufgezeichnet werden. Dies habe ich im Rahmen meiner Stellungnahme sowie im Austausch mit dem Bundesministerium für Gesundheit (BMG) kritisiert. Das BMG hat hier nachgeschärft, sodass aktuell lediglich vorgesehen ist, solche Anrufe aufzuzeichnen, bei denen es sich um Akutfälle handelt.

Ein weiterer Bestandteil des Reformvorhabens umfasst Integrierte Notfallzentren, die bei den zugelassenen Krankenhäusern angesiedelt werden. Sie bestehen aus der Notaufnahme eines zugelassenen Krankenhauses, einer Notdienstpraxis der Kassenärztlichen Vereinigung und einer zentralen Ersteinschätzungsstelle und stellen rund um die Uhr eine bedarfsorientierte medizinische Erstversorgung zur Verfügung. Die Notaufnahme, die Notdienstpraxis und die Ersteinschätzungsstelle sollen digital vernetzt werden, um eine medienbruchfreie Weitergabe von personenbezogenen Daten der Patientinnen und Patienten zu ermöglichen. Diesbezüglich habe ich wiederholt Kritik an der Normenklarheit einzelner Vorschriften geübt. In Bezug auf die Vorschrift des § 123 Abs. 2 S. 5 SGB V neue Fassung (n. F.) wurde meine Kritik jedoch nicht aufgegriffen. Mit dieser Norm wird vorgesehen, dass die Kooperationspartner des Integrierten Notfallzentrums befugt sind, die für eine bedarfsgerechte Steuerung der Hilfesuchenden erforderlichen personenbezogenen Daten zu verarbeiten und sich wechselseitig zu übermitteln. Im Rahmen meines Beratungsauftrags habe ich den Gesetzgeber darauf hingewiesen, dass sich aus dem Regelungstext meines Erachtens nicht eindeutig ergibt, ob lediglich Stammdaten oder auch Gesundheitsdaten Gegenstand der Übermittlung sein können.

Ebenfalls nicht aufgegriffen wurde meine Kritik an § 133a Abs. 3 S. 3 SGB V n. F., wonach Leistungserbringende unter bestimmten Voraussetzungen personenbezogene Daten der vermittelten Hilfesuchenden an die Leitstelle übermitteln. Auch hier ist davon auszugehen, dass sensible Gesundheitsdaten Gegenstand der Übermittlung sein werden. Auch für die Anrufenden ist nicht ersichtlich, welche ihrer Daten hier übermittelt werden sollen. Vor diesem Hintergrund wäre eine Regelung, die die Weiterverarbeitung der Daten transparent macht, wünschenswert gewesen. Ich habe dem BMG zugesichert, für weitere Beratungen zur Verfügung zu stehen.

5.2 Sicherheit

5.2.1 Der Vorschlag zur Novelle des Sicherheitsüberprüfungsgesetzes

In vielen Bereichen ist das Sicherheitsüberprüfungsgesetz (SÜG) nicht praxistauglich. Im Anschluss an seine Evaluierung legte die Bundesregierung einen Gesetzentwurf vor, der leider die Chance verpasste, das Regelwerk hinreichend zu aktualisieren und fit für

die Zukunft zu machen. Insbesondere in datenschutzrechtlicher Hinsicht gelang es diesem Entwurf nicht, Rechtssicherheit und damit Vertrauen zu schaffen. So bleibt die Initiative trotz einiger brauchbarer Ansätze weit hinter ihren Möglichkeiten zurück.

In meinem vorherigen Tätigkeitsbericht hatte ich schon die Sorge geäußert, dass der Gesetzgeber in Bezug auf eine Modernisierung des SÜG Chancen verpassen könnte.[67] Dabei macht nicht nur eine erhöhte Gefährdungslage eine grundlegende Überarbeitung erforderlich, sondern insbesondere auch eine sachgerechte Digitalisierung.

Meine Kontroll- und Beratungstätigkeit erlaubt mir eine umfassende Einsicht in das Sicherheitsüberprüfungsverfahren. Meine Erfahrungen konnte ich hier zwar in die Ressortberatungen einbringen und es wurden auch einige meiner Anregungen aufgenommen. In diesem Kontext begrüße ich insbesondere Maßnahmen, Mehrfachüberprüfungen zu reduzieren. Durch die Neufassung des § 20 SÜG wird das SÜG zudem praxistauglicher; die Schaffung einer Rechtsgrundlage zur digitalen Datenverarbeitung zum Zwecke der Aufgabenerfüllung war lange überfällig.

Insgesamt bleibt der Entwurf jedoch weit hinter seinen Möglichkeiten zurück. So fehlt dem SÜG weiter ein schlüssiges Gesamtkonzept. Auch in der Zukunft soll danach von der Rechtsnormverweisung auf den § 1 Abs. 2 Nr. 4 SÜG Gebrauch gemacht werden. Diese dient insbesondere dazu, alle Mitarbeitenden einer Behörde zu überprüfen. Unklar bleibt dabei, ob es sich um eine einmalige oder dauerhafte Überprüfung handeln soll. Überdies ist die Chance nicht ergriffen worden, die Definition der sicherheitsempfindlichen Tätigkeit i. S. d. § 1 Abs. 2 SÜG neu zu fassen und der Lebensrealität anzupassen. Dies hätte den Anwendungsbereich des SÜG auf ein neues tragfähiges Fundament gehoben und seinen Anwendungsbereich erweitert.

Im Rahmen einer umfassenden Neuordnung hätte es sich zudem angeboten, die erst kürzlich im BVerfSchG und BNDG geschaffenen Vorschriften zur Eigensicherung hier ebenfalls mit aufzunehmen. Diese ergänzen § 4 SÜG (i. V. m. der Verschlusssachenanweisung des Bundes) und sind Teil des materiellen Geheimschutzes, der seit 2017 neben dem personellen Geheimschutz im SÜG geregelt ist.

Die Einbeziehung der mitbetroffenen Person bei gleichzeitiger Erweiterung des Prüfungsumfanges erachte ich im geplanten Umfang überdies als unverhältnismäßig. Die Zahl neuer mitbetroffener Personen wird vermutlich deutlich höher liegen als die Zahl der mit der Neuregelung verhinderten Mehrfachüberprüfungen im Geheim- und Sabotageschutz. Eine gesetzliche Gleichsetzung der mitbetroffenen Person im Sabotageschutz gegenüber dem Geheimschutz ist nicht nachvollziehbar. Es ist nicht ersichtlich, dass Sicherheitsrisiken im Bereich Sabotageschutz in dem Maße auf die betroffene Person durchschlagen wie im Geheimschutz.

Es wäre zudem angemessen, mich mit wirksamen Abhilfebefugnissen auszustatten. Da mir bisher nur die Instrumente der Beanstandung, Aufforderung zur Stellungnahme sowie Warnung zustehen, besteht hier weiter eine inkohärente Rechtslage. Bei Datenschutzverstößen gegenüber Unternehmen kann im Anwendungsbereich der DSGVO ein Bußgeld verhängt werden. Dies gilt nicht, wenn personenbezogenen Daten im Zusammenhang mit einer Sicherheitsüberprüfung verarbeitet worden sind. Im Ergebnis kann die Verarbeitung im Rahmen der Sicherheitsüberprüfung erheblich schlechter kontrolliert werden, als jede sonstige Datenverarbeitung.

Internetrecherche

Ferner ist die deutliche Ausweitung der Internetrecherche aus datenschutzrechtlicher Sicht in ihrer Kumulation bedenklich. Die wegfallende Abstufung führt zu einem zusätzlichen Eingriff für Personen, die einer einfachen Sicherheitsüberprüfung unterzogen werden. Darüber hinaus wird zusätzlich doppelt so häufig überprüft (bei jeder Aktualisierung). Die mitbetroffene Person wird der betroffenen Person gleichgestellt. Die bisherige Regelung zur Recherche im Ausnahmefall gem. § 12 Abs. 5 S. 2 SÜG bewerte ich als ausreichend.

Hinzu kommen die erweiterten Angabepflichten von Benutzernamen, elektronischer Erreichbarkeiten und die erstmalige Möglichkeit zum automatisierten Lichtbild-Abgleich bei Personen i. S. d. § 3 Abs. 3 SÜG. Die Angabepflicht ohne zeitliche Beschränkung kann zur Nennung einer hohen Anzahl von E-Mailadressen führen, wenn aus Gründen der Datensicherheit für jede Nutzung eine neue E-Mailadresse verwendet wurde. Sinnvoll wäre es m. E. gewesen, die Pflicht auf Benutzernamen und Erreichbarkeiten zu beschränken, die in den letzten zwölf Monaten genutzt worden sind.

Die Ausweiterung der Recherche auf alle öffentlich zugänglichen Internetplattformen einschließlich sozialer Netzwerke sehe ich mangels konkreter Definitionen ebenfalls als zu weit an. Für die einzelne Person ist

67 32. TB Nr. 3.3.5

nunmehr völlig unklar, welche Bereiche im Internet durchsucht und welche Mittel angewendet werden. Eigene Privatsphäre-Einstellungen oder ein Austausch in geschlossenen Bereichen schützen nur bedingt. Wenn nicht mehr klar ist, wo geschützte Räume in der digitalen Welt bestehen, kann dies aber zu einem sogenannten „chilling effect" führen, ähnlich wie bei der Videoüberwachung im öffentlichen Raum. Betroffene passen ihr Verhalten an und verzichten bewusst oder unbewusst darauf, ihre Grundrechte und Freiheiten auszuüben aus der Angst, dass das eigene Abweichen von „normalem" Verhalten als „verdächtig" angesehen werden könnte. Gerade eine lückenlose Überwachung will das SÜG jedoch nicht. Entsprechende Definitionen würden Rechtssicherheit schaffen, auf welche Inhalte mit welchen Mitteln zugegriffen werden darf. Unklar ist nicht nur, was noch öffentlich zugänglich ist, z. B. bei einer Anmeldung oder einem Aufnahmeverfahren, sondern auch die Abgrenzung zwischen sozialen Netzwerken und Individualkommunikation.

Digitalisierung

Das SÜG unterscheidet zwischen Akte (Sicherheitsakte bzw. Sicherheitsüberprüfungsakte) sowie Datei. Die Akte durfte bisher schon gem. § 18 Abs. 6 S. 1 SÜG elektronisch geführt werden. Eine Änderung war demnach nicht erforderlich. Akte und Datei sind voneinander abzugrenzen. Die Datei diente bislang bei öffentlichen Stellen ausschließlich dem Ziel, die Akte schneller auffinden, identifizieren und bearbeiten zu können (Vorgangsverwaltung). Künftig sollen Dateien auch zur leichteren Bearbeitung (Aufgabenerfüllung) zulässig sein.

Der Gesetzesentwurf suggeriert unter dem Deckmantel der Digitalisierung eine Vermischung verschiedener Verarbeitungszwecke. Dadurch besteht die Gefahr, dass an verschiedenen Orten personenbezogene Daten aus der Sicherheitsüberprüfung gesammelt werden, ohne diese aktenmäßig zu verwalten. Dies wäre bspw. der Fall, wenn einzelne Dokumente unsortiert auf einem Laufwerk gespeichert, das E-Mailpostfach zur Aufbewahrung von Schreiben verwendet oder Schreiben je nach Ersteller oder Format sortiert unabhängig von der jeweiligen Sicherheitsüberprüfung aufbewahrt werden. Bei mehreren Kontrollen zeigte sich, dass genau diese Fälle bereits vorkommen. Auch hier hätte eine moderne Struktur des Gesetzes entlang der Verarbeitungszwecke Vorgangsverwaltung, Aufgabenerfüllung und Dokumentation für mehr Klarheit gesorgt.

Verarbeitung personenbezogener Daten Dritter

Die zusätzliche Erlaubnis personenbezogene Daten unbeteiligter Dritter zu speichern, die nicht erforderlich sind, stößt auf starke datenschutzrechtliche Bedenken. Gegen die Speicherung von beteiligten Dritten, Verfahrensbeteiligten, Urhebern oder Adressaten von behördlichen oder sonstigen Schreiben bestanden schon bisher keine Bedenken, wenn diese Angaben zur Bewertung der jeweiligen Information erforderlich waren. Anders verhält sich dies mit personenbezogenen Daten, die nach erfolgter Prüfung keine Rolle spielen und nicht benötigt werden. Eine Verarbeitung greift unverhältnismäßig in das Grundrecht auf informationelle Selbstbestimmung Dritter ein, die überhaupt keinen Bezug zu der konkreten Sicherheitsüberprüfung haben. Zwar dürfen deren Daten nicht gezielt abgefragt werden. Dem Grundsatz der Datensparsamkeit wird hier jedoch eine klare Absage erteilt.

5.2.2 Modernisierung des Bundespolizeigesetzes steht weiter aus

Das Bundespolizeigesetz ist dringend überarbeitungsbedürftig, nicht nur aufgrund europa- und verfassungsrechtlicher Vorgaben für den Datenschutz. Ich habe den Gesetzgebungsprozess von Beginn an begleitet. 2024 fand die erste Lesung im Deutschen Bundestag sowie eine Sachverständigenanhörung statt. Bis zum Ende der 20. Wahlperiode ist weiter nichts passiert, das Vorhaben bleibt wieder unvollendet.

Erneut ist es dem Gesetzgeber leider nicht gelungen, die 2022 neuerlich angelaufene – und bereits in der 19. Legislaturperiode gescheiterte – Neustrukturierung des Bundespolizeigesetzes (BPolG) zum Abschluss zu bringen. Dabei ist die Überarbeitung des zu großen Teilen noch aus dem Jahr 1994 (damals hieß die Bundespolizei noch Bundesgrenzschutz) stammenden Gesetzes weiterhin dringend geboten:

Die Umsetzung der Richtlinie (EU) 2016/680 vom 27. April 2016 (JI-Richtlinie) in Bezug auf wirksame Abhilfebefugnisse der Datenschutzaufsichtsbehörden ist bis heute im BPolG nicht erfolgt; Verstöße in diesem Bereich kann ich derzeit nur gegenüber dem Bundesministerium des Innern und für Heimat förmlich beanstanden. Art. 47 Abs. 2 JI-Richtlinie sieht dagegen weitere wirksame Abhilfebefugnisse wie die Anordnung der Berichtigung oder Löschung personenbezogener Daten sowie eine Beschränkung der Verarbeitung vor. Die Umsetzungsfrist lief bereits im Mai 2018 ab, die EU-Kommission

hat in diesem Zusammenhang bereits zwei Vertragsverletzungsverfahren gegen die Bundesrepublik eröffnet.[68] Darüber hinaus hat auch die Rechtsprechung des Bundesverfassungsgerichts zur hypothetischen Datenneuerhebung[69] bislang keinen Eingang in das BPolG gefunden.

Beide Punkte waren im Entwurf eines Gesetzes zur Neustrukturierung des BPolG[70] enthalten, wenngleich die für meine Behörde vorgesehenen Abhilfebefugnisse meiner Auffassung nach nicht den europarechtlichen Vorgaben entsprachen. Neben einer zusätzlichen Erheblichkeitsschwelle würden auch die Pflicht zur vorherigen Beanstandung von Datenschutzverstößen sowie der ausdrückliche Ausschluss einer Löschanordnung in der Gesetzesbegründung die Wirksamkeit von Abhilfebefugnissen unangemessen und europarechtswidrig einschränken. Dies hatte mein Haus in der Vergangenheit bereits in Bezug auf die entsprechenden Vorschriften im Bundeskriminalamtsgesetz und Zollfahndungsdienstegesetz kritisiert.

Ich habe den Gesetzgebungsprozess seit der Ressortabstimmung konstruktiv begleitet, einige meiner Anregungen wurden in der jüngsten Entwurfsfassung berücksichtigt.[71] Zu verbleibenden Kritikpunkten konnte ich mich in einer öffentlichen Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages im April 2024 äußern.

Hier habe ich unter anderem den Wegfall der sog. Errichtungsanordnung (§ 36 BPolG) bei Einführung neuer IT-Systeme kritisiert, im Rahmen derer ich nach derzeitiger Rechtslage vorher anzuhören bin. Die frühzeitige Einbindung meiner Behörde stellt sicher, dass datenschutzrechtliche Belange von Anfang an berücksichtigt werden, wodurch sich aufwändige und kostenintensive nachträgliche Anpassungen vermeiden lassen.

Stellung genommen habe ich u. a. auch zur geplanten Ausweitung des Einsatzes sogenannter Bodycams auf nicht öffentlich zugängliche Orte, zur Ausweitung der Übermittlung von Fluggastdaten und zur zukünftig vorgesehenen Pflicht zur Sicherheitsüberprüfung aller Personen, die für die Bundespolizei tätig werden.

Positiv ist an dem Gesetzentwurf hervorzuheben, dass auf die besonders eingriffsintensiven Instrumente der Quellen-Telekommunikationsüberwachung sowie der Online-Durchsuchung verzichtet wurde.[72]

Bedauerlicherweise konnte das Gesetzesvorhaben auch in der 20. Wahlperiode des Deutschen Bundestages nicht zu Ende gebracht werden. Nicht nur aus den genannten datenschutzrechtlichen Erwägungen ist eine Überarbeitung des BPolG jedoch weiterhin dringend angezeigt. Das Gesetz hat allgemein großen Modernisierungsbedarf. Ich appelliere daher an den Gesetzgeber, das Vorhaben im dritten Anlauf endlich zu einem Abschluss zu bringen. Für die Belange des Datenschutzes stehe ich hierbei gern weiter beratend zur Verfügung.

5.2.3 BKA II-Entscheidung des Bundesverfassungsgerichts

Das Bundesverfassungsgericht (BVerfG) hat eine grundlegende Entscheidung zu Daten getroffen, die das Bundeskriminalamt (BKA) zur Vorsorge auf Vorrat im polizeilichen Informationsverbund speichert. Diese bestätigt meine Beratungs- und Kontrollpraxis und wird sich weitreichend auswirken.

Das BVerfG hat die Regelungen, nach denen das BKA personenbezogene Daten in dem polizeilichen Informationsverbund speichert, teilweise für nicht mit dem Grundgesetz vereinbar erklärt.[73] Dies betrifft vor allem die Speicherung von Beschuldigten zum Zweck der Vorsorge. Hierbei ist nämlich zu beachten, dass Beschuldigte auch dann im Informationsverbund gespeichert werden können, wenn sich der gegen sie gerichtete Verdacht einer Straftat nicht erhärten lässt. Wer also im Informationsverbund gespeichert ist, ist nicht unbedingt ein verurteilter Straftäter. Zudem sind prinzipiell auch Bagatelldelikte betroffen.

Die Daten Beschuldigter für Vorsorgezwecke auf Vorrat zu speichern, bedarf einer besonderen Rechtfertigung. Das Gericht hat klargestellt, dass die Vorsorgespeicherungen ein eigenständiger Grundrechtseingriff sind und der Gesetzgeber dies nur zulassen darf, wenn die Polizeibehörde eine eigenständige Prognoseentscheidung trifft.

---

68 31. TB Nr. 4.5

69 Urteil des Bundesverfassungsgerichts vom 20. April 2016 (Az. 1 BvR 966/09, 1 BvR 1140/09), abrufbar unter: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html

70 BT-Drs. 20/10406, abrufbar unter: https://dserver.bundestag.de/btd/20/104/2010406.pdf

71 32. TB Nr. 3.3.2

72 BfDI-Stellungnahme vom 18. April 2024, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Neustrukturierung-Bundespolizeigesetz.html

73 Urteil des BVerfG vom 1. Oktober 2024 – 1 BvR 1160/19, abrufbar unter: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2024/10/rs20241001_1bvr116019.html

Damit verbunden sind Grundaussagen zur Zweckbindung, zu den Speicherschwellen sowie Löschregelungen.

Ich sehe mich durch das Urteil in meinen bisherigen Rechtsauffassungen bestätigt, die sich so auch in der langjährigen Beratungs- und Kontrollpraxis niedergeschlagen haben. Insbesondere auf den polizeilichen Informationsverbund wird sich das Urteil unmittelbar und erheblich auswirken.

Das Ergebnis der Entscheidung wird deshalb auch Einfluss auf die Neugestaltung der BKA-Datenverordnung haben. Hier setze ich mich dafür ein, dass die Datenkategorien nicht gegen die oben genannte Entscheidung verändert werden können. Es ist insbesondere zu vermeiden, dass die vom Gericht geforderte Prognoseentscheidung – die sogenannte Negativprognose – umgangen werden könnte. Ferner spreche ich mich für eine klare Datenstruktur aus. Diese muss die polizeiliche Arbeit ermöglichen. Sie darf aber nicht über den Bedarf zur Aufgabenerfüllung hinausgehen und muss stets diskriminierungsfrei sein.

Daneben hat das Gericht eine Vorschrift zu verdeckten Eingriffen gegenüber Kontaktpersonen von Gefährdern für unwirksam erklärt. Dies werde ich in meinen Kontrollen verdeckter Ermittlungsmaßnahmen berücksichtigen.

5.3 Inneres und Justiz

5.3.1 Erstes Gesetz zur Änderung des Bundesdatenschutzgesetzes

Die Bundesregierung hat Anfang 2024 ihren Gesetzesentwurf „zur Änderung des Bundesdatenschutzgesetzes“ in den Deutschen Bundestag eingebracht. Meine Behörde begleitete das Gesetzgebungsverfahren und setzte sich insbesondere für die Umsetzung der im Rahmen der Evaluierung des Bundesdatenschutzgesetzes (BDSG) durch die Datenschutzkonferenz (DSK) ausgemachten Änderungsbedarfe ein.

Der Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes soll die datenschutzrechtlich relevanten Vereinbarungen des Koalitionsvertrags der 20. Wahlperiode aufgreifen sowie Ergebnisse umsetzen, die sich aus der Evaluierung des BDSG durch das BMI ergeben haben. Dazu gehört etwa eine Institutionalisierung der DSK, die im Gesetzesentwurf vorgenommen wird. Zudem soll der DSK ausdrücklich die Hoheit über ihre Geschäftsordnung verliehen werden. Weitere Schritte – wie etwa eine stärkere Verbindlichkeit der DSK-Entscheidungen gegenüber ihren Mitgliedern oder die Einrichtung einer Geschäftsstelle – hatte die Bundesregierung nicht vorgesehen.

Der Gesetzesentwurf enthält einige notwendige Klarstellungen, die ich begrüße. Er greift jedoch insbesondere bezüglich der im Rahmen der Evaluierung des BDSG durch die DSK ausgemachten Überarbeitungsbedarfe zu kurz.

Der Gesetzesentwurf enthält zu § 18 BDSG von mir vorgeschlagene wichtige Klarstellungen für die Zusammenarbeit der deutschen Aufsichtsbehörden in europäischen Angelegenheiten. Die Aufsichtsbehörden der Länder und meine Behörde sollten auch auf europäischer Ebene immer mit einer Stimme sprechen, um den deutschen Positionen dort mehr Gewichtung beizumessen. Folglich begrüße ich die Klarstellung, dass es eines gemeinsamen Standpunkts der deutschen Aufsichtsbehörden in europäischen Angelegenheiten nicht nur im Kohärenzverfahren (Art. 63 bis 65 DSGVO), sondern bereits im Kooperationsverfahren (Art. 60 DSGVO) und auch im Dringlichkeitsverfahren (Art. 66) DSGVO bedarf.

Nötig sind darüber hinaus jedoch weitere Korrekturen nicht zufriedenstellender Regelungen im BDSG. Wesentliche aus meiner im parlamentarischen Verfahren abgegebenen Stellungnahme zu nennende Punkte sind:

- Die aufsichtsbehördlichen Befugnisse im BDSG dahingehend zu erweitern und zu stärken, dass gegenüber öffentlichen Stellen die Durchsetzung von Maßnahmen mit Zwangsmitteln, beispielsweise durch Schaffung einer bereichsspezifischen Ausnahmeregelung i. S. v. § 17 VwVG, sowie die Anordnung der sofortigen Vollziehung durch Streichung des § 20 Abs. 7 BDSG ermöglicht wird. Zudem sollte die Regelung des § 43 Abs. 3 BDSG aufgehoben und damit eine Verhängung von Geldbußen gegen öffentliche Stellen ermöglicht werden. Bislang können datenschutzrechtliche Verstöße öffentlicher Stellen lediglich mit einer Verwarnung geahndet werden. Nach der Konzeption der DSGVO ist die Verwarnung lediglich für geringfügige Verstöße gedacht, während bei schwerer wiegenden Verstößen Geldbußen zu verhängen sind. Derzeit fehlt es gegenüber öffentlichen Stellen an dieser zweiten Sanktionsstufe.
- Erweiterung meiner Aufsichtszuständigkeit für Verstöße durch Beschäftigte öffentlicher Stellen des Bundes, die sich selbst als Verantwortliche gerieren (sog. Mitarbeiterexzess). Nach aktueller Gesetzeslage bin ich im Fall eines Mitarbeiterexzesses für die entsprechende Verarbeitung personenbezogener Daten durch die beschäftigte Person nicht zuständig. Zuständig ist nach § 40 BDSG die jeweilige Datenschutzaufsichtsbehörde des Landes, da die betreffen-

de Person nicht die Voraussetzungen der in § 9 Abs. 1 BDSG genannten Stellen erfüllt. Damit einheitliche Lebenssachverhalte bei einer Aufsichtsbehörde gebündelt werden können, halte ich die dargestellte Erweiterung meiner Zuständigkeit, beispielsweise durch eine ergänzende Regelung in § 9 BDSG, für erforderlich.

→ Die laut Gesetzesbegründung aufgrund der Entscheidung des EuGH vom 7. Dezember 2023 in Sachen SCHUFA Holding[74] in § 37a BDSG-E aufgenommene Neuregelung zum Scoringverfahren gibt sowohl aus grundsätzlichen Erwägungen als auch aus einer Reihe von Einzelgesichtspunkten Anlass zu Kritik, so dass ich entsprechende Nachbesserungen angeregt habe. Hierzu gehören u. a. die Prüfung, ob diese Vorschrift mit den Anforderungen des Art. 23 DSGVO zur Einschränkung von Betroffenenrechten in Einklang steht, und die Aufnahme eines formalen Zertifizierungserfordernisses durch eine unabhängige Stelle für die dem Scoring zu Grunde zu legenden wissenschaftlich anerkannten mathematisch-statistischen Verfahren.

Infolge des vorzeitigen Endes der 20. Wahlperiode des Deutschen Bundestages fällt der Gesetzentwurf nunmehr der Diskontinuität anheim. Ich hoffe, dass der 21. Deutsche Bundestag das Vorhaben zügig wiederaufgreift und hierbei die von mir vorgebrachten Änderungsvorschläge berücksichtigt.

5.3.2 NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) soll die IT-Sicherheit in Deutschland gestärkt werden, indem zahlreichen Einrichtungen Cybersicherheitsmaßnahmen sowie Meldepflichten auferlegt werden. Angesichts der engen Verzahnung zur IT-Sicherheit betrifft dies auch den Datenschutz.

Die von der EU im Dezember 2022 verabschiedete Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS2-Richtlinie) stellt auf europäischer Ebene Regeln für sogenannte wichtige und wesentliche Einrichtungen auf und verpflichtet unter anderem zur Umsetzung von Cybersicherheitsmaßnahmen und Meldung erheblicher Sicherheitsvorfälle. Die EU-Mitgliedstaaten mussten die NIS2-Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen. Die deutsche Umsetzung konnte leider nicht in dieser Frist abgeschlossen werden.

Der Cyber- und Informationssicherheit kommt in der Digitalisierung eine große Bedeutung zu. Digitalisierung und Cybersicherheit sind dabei untrennbar mit dem Thema Datenschutz verbunden. Bedrohungen oder gar Verletzungen der IT-Sicherheit betreffen regelmäßig auch den Schutz personenbezogener Daten. Datenschutz lässt sich also nicht ohne funktionierende IT-Sicherheit realisieren. Daher ist eine enge Verzahnung beider Themen sinnvoll und notwendig. Das NIS2UmsuCG bietet damit eine Chance, Staat, Wirtschaft und Gesellschaft im digitalen Raum besser zu schützen.

Kern des NIS2UmsuCG ist die Neufassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG). Dem BSI fällt hier die zentrale Rolle zu, die vorgesehenen Maßnahmen zu kontrollieren, betroffene Stellen zu unterstützen und als die zentrale Stelle für Informationssicherheit auf nationaler Ebene zu fungieren. Zudem soll es Informationen zu Angriffen und Schwachstellen sammeln. Schwachstellen sind Sicherheitslücken, durch deren Ausnutzung sich Dritte unbefugt Zugang zu IKT-Produkten oder -Diensten verschaffen bzw. diese beeinflussen können. Sie stellen eine große Gefahr für die IT-Sicherheit und damit auch den Datenschutz dar. Aus diesem Grund hat mein Haus schon in der Vergangenheit darauf aufmerksam gemacht, dass im Rahmen der Neuregelung des BSIG die Chance genutzt werden sollte, den Weg von der Detektion einer Schwachstelle bis hin zu ihrer Schließung klar vorzuzeichnen und deren konsequente und sofortige Schließung vorzuschreiben.[75] Die Risiken einer offen gelassenen Schwachstelle überwiegen schlicht die Vorteile, die durch das Offenhalten entstehen könnten. Leider sah auch der Regierungsentwurf des NIS2UmsuCG keine Vorgaben dafür vor. In meiner öffentlichen Stellungnahme vom 4. November 2024[76] habe ich daher den federführenden Ausschuss für Inneres und Heimat des Bundestages gebeten, entsprechende Regelungen im Gesetz zu ergänzen.

Die durch das NIS2UmsuCG geplante Neufassung des BSIG sieht nicht nur neue Befugnisse und Datenver-

74 EuGH, Urteil vom 7. Dezember 2023, Az. C-634/21 – SCHUFA Holding (Scoring), abrufbar unter: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0634

75 Schreiben des BfDI vom 18. September 2023 an sechs Ministerien vom 03.07.2023, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Schwachstellen-schließen-Sicherheit-stärken.pdf

76 Stellungnahme der BfDI vom 4. November 2024, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/NIS2-UmsuCG-Bundestag

arbeitungen des BSI vor, sondern weiterhin einige Einschränkungen der datenschutzrechtlichen Betroffenenrechte. Ich habe daher weiter angeregt, diese seit Jahren bestehenden Einschränkungen auf ihre Notwendigkeit für die Arbeit des BSI und ihre Verhältnismäßigkeit mit Blick auf die Rechte und Freiheiten der Betroffenen zu evaluieren.

Der Schutz der Informationssicherheit ist nicht nur Aufgabe einer Behörde. IT-Sicherheits- und Datenschutzaufsichtsbehörden müssen zusammenarbeiten, um ein möglichst hohes Maß an Sicherheit erreichen zu können. Die NIS2-Richtlinie sieht daher die Weiterleitung von relevanten Informationen der IT-Sicherheitsaufsichtsbehörden an die Datenschutzaufsichtsbehörden vor. Der Regierungsentwurf des NIS2UmsuCG setzte dies leider nur unzureichend und damit richtlinienwidrig um. In meiner o. g. Stellungnahme habe ich darauf hingewiesen und konkrete Verbesserungsvorschläge unterbreitet.

Leider konnte das NIS2UmsuCG durch die vorgezogene Neuwahl des Bundestages nicht mehr beschlossen werden. Das Gesetzgebungsvorhaben muss daher in der 21. Legislaturperiode neu gestartet werden. Ein neuer Entwurf sollte die positiven Impulse aus der öffentlich gewordenen Formulierungshilfe zum Gesetzentwurf im Innenausschuss des Bundestages beibehalten und zusätzlich die Verbesserungsvorschläge aufgreifen, die von Sachverständigen in der Ausschussanhörung und von mir in den schriftlichen Stellungnahmen gemacht wurden. So sollten aus der Formulierungshilfe die Regelungen zum Umgang des BSI und der Bundesverwaltung mit Schwachstellen ebenso in einen neuen Entwurf übernommen werden, wie die richtlinienkonformen Regelungen zur Weitergabe von Informationen des BSI an die Datenschutzaufsichtsbehörden. Zudem sollte die Abstimmung zwischen den NIS-2-Aufsichtsbehörden und den Datenschutzaufsichtsbehörden in Bußgeldangelegenheiten klar geregelt werden, um die Verhängung doppelter Bußgelder zu vermeiden. Wenn in einem neuen Gesetzgebungsanlauf weitergehende Befugnisse des BSI für Grundrechtseingriffe vorgesehen werden, müssen diese verhältnismäßig ausgestaltet werden. Der verfassungsrechtlich notwendige Ausgleich des Eingriffsgewichtes ist z. B. durch eine Einbindung unabhängiger Aufsichtsbehörden in die Befugnisausübung denkbar.

Ich werde mich auch in der neuen Legislaturperiode wieder konstruktiv in die Beratungen zum Gesetz einbringen und mich nach Verabschiedung des Gesetzes für eine Umsetzung einsetzen, die den Interessen sowohl der Cybersicherheit als auch des Datenschutzes angemessen Rechnung trägt.

5.3.3 OZG-Änderungsgesetz

Der Gesetzgeber hat das OZG-Änderungsgesetz, das sich bei Erscheinen meines vorherigen Tätigkeitsberichts noch in der parlamentarischen Beratung befand, zwischenzeitlich beschlossen. Gegenüber der Entwurfsfassung haben einige Änderungen Eingang in das Gesetz gefunden.

In meinem vorherigen Tätigkeitsbericht habe ich den Entwurf eines OZG-Änderungsgesetzes aus datenschutzrechtlicher Perspektive beleuchtet.[77] Inzwischen wurde das Gesetz verabschiedet und ist in Kraft getreten. Dabei hat der ursprüngliche Entwurf auf Empfehlung des Innenausschusses des Deutschen Bundestages sowie im Vermittlungsausschuss Änderungen erfahren. Folgende das OZG betreffende Änderungen sind besonders hervorzuheben.

Zentralisierung der Bürgerkonten zur BundID, künftig DeutschlandID

Im Entwurf war zunächst vorgesehen, dass die Länderkonten nach Ablauf einer festen Übergangsfrist von drei Jahren entfallen sollen und künftig durch den Bund mit der BundID nur noch ein zentrales Bürgerkonto bereitgestellt werden. Das verabschiedete Gesetz sieht nunmehr die Möglichkeit vor, dass ein Länderkonto automatisch in ein Bundeskonto überführt („migriert“) wird. Die Frist von drei Jahren beginnt erst, wenn die Voraussetzungen einer solchen automatisierten Migration geschaffen sind. Da sich mit einer Migration auch datenschutzrechtliche Fragen stellen werden, sollten die jeweiligen Aufsichtsbehörden eng eingebunden werden. Zugleich sieht das Gesetz vor, dass die BundID künftig zur „DeutschlandID“ fortentwickelt wird. Ob und welche inhaltlichen Änderungen damit konkret verbunden sein werden, bleibt abzuwarten.

Personalausweis als Identifizierungsmittel im Bürgerkonto

Das Gesetz sieht wie schon der Entwurf vor, dass sich Bürgerinnen und Bürger mit dem elektronischen Personalausweis, also auf hohem Vertrauensniveau, authentifizieren müssen, wenn eine Verwaltungsleistung eine Identifizierung und Authentifizierung erfordert (zu den Ausnahmen sogleich). Auf Empfehlung des Innen-

77 32. TB Nr. 8.1

ausschusses wurde eine Regelung ergänzt, wonach der Personalausweis dabei nur noch für die erstmalige Authentisierung genutzt werden muss. Danach sollen auch andere Authentisierungsmittel verwendet werden können, die durch das Bundesministerium des Innern und für Heimat (BMI) nach Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) für diese Zwecke befristet zugelassen werden. Ziel der Regelung ist es laut Begründung, bis zur Etablierung der EUDI-Wallet „niederschwellige Authentisierungsmöglichkeiten" zu schaffen. Ich setze mich dafür ein, dass diese Regelung nicht zu einer Absenkung des Sicherheitsniveaus führt.

Elster als Identifizierungsmittel im Bürgerkonto

Bis zum 30. Juni 2026 sollte für Verwaltungsleistungen, die höchstens das Vertrauensniveau „substantiell" erfordern, nach dem Gesetzentwurf eine Identifizierung mit Elster-Softwarezertifikaten möglich sein. Diese Frist hätte durch das BMI und das Bundesministerium der Finanzen (BMF) unbeschränkt verlängert werden können. Entgegen meiner Empfehlung ist die Fristenregelung im Gesetz entfallen. Das bedeutet, dass für Verwaltungsleistungen, die das Vertrauensniveau „substantiell" erfordern, stets auch eine Authentifizierung mit Elster-Softwarezertifikaten möglich ist. Die generelle Zulassung von Elster-Softwarezertifikaten für Verwaltungsleistungen auf dem Vertrauensniveau „substantiell" ist jedoch abzulehnen, da diese Zertifikate eine entsprechend zuverlässige Identifizierung nicht sicherstellen. Alternativ sollte deshalb erwogen werden, Elster-Softwarezertifikate so nachzubessern, dass sie stets das Vertrauensniveau „substantiell" erfüllen.

Elster als Identifizierungsmittel im Organisationskonto

Anders als das Bürgerkonto ist die Nutzung des Organisationskontos für Unternehmen im Sinne des Unternehmensbasisdatenregistergesetzes verpflichtend. Das war bereits im Gesetzentwurf vorgesehen. Nach der Entwurfsfassung sollten jedoch Elster-Softwarezertifikate als Identifizierungsmittel im Organisationskonto nur für eine Übergangsfrist von fünf Jahren zugelassen werden, wobei diese Frist durch das BMI und das BMF unbeschränkt hätte verlängert werden können. Entgegen meiner Empfehlung wurde auch diese Frist gestrichen, so dass im Organisationskonto Elster-Softwarezertifikate ebenfalls dauerhaft für die Authentifizierung verwendet werden können. Insoweit bestehen dieselben Bedenken wie im Fall des Bürgerkontos. Ich begrüße jedoch, dass der Gesetzgeber gleichzeitig festgelegt hat, dass eine Nutzung des Organisationskontos unterbleiben muss, wenn im Einzelfall ein „höheres" Vertrauensniveau – nach meinem Verständnis also das Vertrauensniveau „hoch" – gefordert ist.

5.3.4 Registerzensusgesetz

Im Mai 2024 hat das Bundesministerium des Innern und für Heimat (BMI) erneut einen Entwurf für ein Registerzensus-Ermächtigungsgesetz in die Ressortabstimmung gegeben. Auf dieser Basis soll nicht nur die Vorbereitung und Durchführung des kommenden Zensus 2031, sondern darüber hinaus die Erhebungen für alle künftigen Bevölkerungszählungen sowie sämtliche Datenübermittlungen aufgrund entsprechender Lieferpflichten nach jeweils geltendem EU-Recht legitimiert werden. Bis zum vorzeitigen Ende der Legislaturperiode konnte jedoch keine ressortweite Einigung über den Gesetzentwurf erzielt werden.

Der mit dem Gesetzentwurf verfolgte Ansatz, die über Bevölkerungszählungen zu gewinnenden und für Politik, Wirtschaft und Gesellschaft unverzichtbaren Informationen künftig umfassend aus bereits vorhandenen Registern zu ziehen, statt wie bisher aufwändig durch ergänzende Befragungen von Teilen der Bevölkerung zu erzielen, wird auch von mir ausdrücklich begrüßt. Die potentielle Fehleranfälligkeit von Befragungsverfahren unabhängig davon, ob sie über den Einsatz von Erhebungsbeauftragten oder online über ein entsprechendes Internetportal durchgeführt werden, ist auch im zurückliegenden Zensus 2022 bestätigt worden und wirkt sich in der Regel unmittelbar zulasten des Rechts auf informationelle Selbstbestimmung der Betroffenen aus.

Dennoch habe ich gegen den Gesetzentwurf erhebliche Bedenken erhoben. Meine Kritik richtet sich vor allem gegen den danach vorgesehenen Aufbau und dauerhaften Betrieb eines umfassenden bevölkerungsstatistischen Datenbestands in der Verantwortung des Statistischen Bundesamts. Mit dieser sehr umfangreichen Sammlung personenbeziehbarer Daten würden wesentliche Inhalte der Datenbestände sämtlicher Melderegister dieses Landes zentral an einer Stelle auf Bundesebene gespiegelt und fortwährend mindestens jährlich über entsprechende Datenzulieferungen der Meldeämter aktualisiert. Auch wenn ich nachvollziehen kann, dass ein Bestand an grundlegenden soziodemografischen Basisdaten zur Verwendung für eine Vielzahl von gesellschafts- und wirtschaftspolitischen Entscheidungen eine möglichst hohe Qualität und Belastbarkeit aufweisen sollte, muss diese gesetzgeberische Zielsetzung in einem ausgewogenen Verhältnis zu den dazu eingesetzten Mitteln stehen.

Allein der Aufbau und Unterhalt des angedachten bevölkerungsstatistischen Datenbestands würde Daten-

verarbeitungen in einer Größenordnung beinhalten, die – auch wenn sie hinter der Mauer der statistischen Geheimhaltung erfolgen – sowohl in der Streubreite als auch in ihrer Tiefe als besonders intensive Eingriffe in das Grundrecht auf informationelle Selbstbestimmung zu qualifizieren wären, da sie im Unterschied zu den bisherigen Bevölkerungszählungen weder zeitlich begrenzt stattfinden würden noch eine Anonymisierung der Daten in diesem Bestand vorgenommen werden soll. In Anbetracht dessen können schon die zur Erforderlichkeit eines solchen Datenbestands angeführten Argumente nicht überzeugen. Sie fußen im Wesentlichen auf Erwägungen zur Her- und Sicherstellung einer höchstmöglichen Datenqualität sowie dem Hinweis auf künftig zu erwartende Anforderungen nach EU-Recht. Die Beratungen über den konkreten Inhalt der aktuell vorbereiteten Rechtsänderungen auf EU-Ebene sind allerdings noch nicht abgeschlossen, sodass der Zeitpunkt des Inkrafttretens dieses künftigen EU-Rechts zurzeit ebenfalls noch nicht absehbar ist.

Auch eine sorgfältigere Abwägung des gewählten Modells mit möglichen alternativen Vorgehensweisen, mit denen zumindest weniger einschneidende Folgen für das Recht der Betroffenen auf informationelle Selbstbestimmung verbunden sein könnten, lässt der bisherige Gesetzentwurf vermissen. So bleibt offen, ob die im Rahmen der Gesetzgebung zur Registermodernisierung bereits angelegten Qualitätssicherungselemente nicht ebenfalls ausreichen könnten, die Datengewinnung beispielsweise über stichtagsbezogene Anforderungen der dezentral bei den Meldeämtern vorgehaltenen Datenbestände sicherzustellen, statt diese zusätzlich zentral und dauerhaft in einem eigenen bevölkerungsstatistischen Datenbestand zu speichern.

Dabei sind die ebenfalls aus qualitätssichernden Erwägungen vorgesehenen regelmäßigen Datenzulieferungen aus einer Vielzahl weiterer Datenbestände in Bundes- und Länderregistern nach dem angedachten Lebenszeichen-Ansatz, die zum Zweck eines Abgleichs mit den Melderegisterdaten den Einsatz eines eindeutigen Personenkennzeichens bedingen würden, noch nicht berücksichtigt. Auch insoweit erweist sich der Gesetzentwurf als problematisch, da die entsprechenden Regelungen die Verwendung der Identifikationsnummer nach dem Identifikationsnummerngesetz bzw. ersatz- und übergangsweise der Identifikationsnummer für steuerliche Zwecke nach der Abgabenordnung vorsehen, ohne gleichzeitig die nach Art. 87 DSGVO erforderlichen geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen im Gesetzentwurf festzulegen. Dazu zählen beispielsweise Schutzmechanismen wie die Einschaltung einer unabhängigen neutralen Vertrauensstelle bzw. eines Intermediärs zur ausschließlichen Verarbeitung der eindeutig personenidentifizierenden Merkmale (zwecks Herstellung eines unverwechselbaren Personenkennzeichens) und eine Anbindung an das Datencockpit nach Maßgabe des Online-Zugangsgesetzes.

Meine Bedenken und Anregungen haben in den verschiedenen Überarbeitungen des Gesetzentwurfs leider keine Berücksichtigung gefunden. Ich hoffe, dass im Rahmen einer möglichen neuen Gesetzgebungsinitiative der bisherige Regelungsansatz entweder noch einmal grundlegend überdacht oder jedenfalls so überarbeitet wird, dass unvermeidbare Eingriffe in das Grundrecht auf informationelle Selbstbestimmung durch gesetzliche Vorgaben für geeignete Schutzmaßnahmen angemessen kompensiert werden.

5.4 Wirtschaft und Finanzen

5.4.1 Telemedien heißen nun Digitale Dienste

Am 14. Mai 2024 trat das Digitale-Dienste-Gesetz (DDG) in Kraft, das den Digital Services Act (DSA) der EU auf nationaler Ebene umsetzt. Mit dem DDG wurde auch das bisherige Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) in Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) umbenannt. [78]

Inkrafttreten des TDDDG

Mit dem Inkrafttreten des DDG und der damit einhergehenden Umbenennung in TDDDG hat sich, außer dem Titel, inhaltlich wenig am bisherigen TTDSG geändert. Lediglich der Begriff der Telemedien wird durch die Änderung jetzt durch den Begriff der digitalen Dienste ersetzt.

Das TDDDG hat weiterhin zwei wesentliche Geltungsbereiche. Das Gesetz regelt nach § 1 Abs. 1 Nr. 1 bis Nr. 6 TDDDG das Fernmeldegeheimnis weiter aus und schafft besondere datenschutzrechtliche Bestimmungen für die Anbieter von Telekommunikationsdiensten und digitalen Diensten. Nach § 1 Abs. 1 Nr. 7 TDDDG enthält es

78 Art. 8 des Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze vom 6. Mai 2024 (BGBl. 2024 I Nr. 149).

zudem Reglungen für den Schutz der Privatsphäre bei Endeinrichtungen. Endeinrichtung ist nach § 2 Abs. 2 Nr. 6 TDDDG jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten, also mit dem Internet verbundene Geräte wie beispielsweise Smartphones und Laptops, aber auch vernetzte Geräte wie „smarte" Küchengeräte, Alarmsysteme oder Heizkörperthermostate. Im Hinblick auf durch öffentliche Stellen des Bundes angebotene digitale Dienste bin ich gemäß § 29 Abs. 2 und 3 TDDDG auch für die Durchsetzung des Schutzes der Integrität von Endeinrichtungen i. S. v. § 25 TDDDG vor unzulässigen Zugriffen oder Speicherungen zuständig.

Kontrollen und Erfahrungen

Auch 2024 hat mein Haus die digitalen Dienste mehrerer öffentlicher Stellen des Bundes kontrolliert. Gegenstand dieser Kontrollen waren hierbei primär Webseiten und Apps, sowohl von obersten Bundesbehörden als auch von Behörden aus dem nachgeordneten Bereich. Leider haben meine Mitarbeiterinnen und Mitarbeiter bei meinen Kontrollen, wie auch in den vorangegangenen Jahren, wiederkehrende Verstöße gegen Grundsätze des TDDDG und der DSGVO festgestellt. So wird beispielsweise den Informationspflichten des Art. 13 DSGVO durch Nutzung unvollständiger Datenschutzerklärungen nicht vollumfänglich nachgekommen. Auch werden die nach § 25 Abs. 1 TDDDG für Zugriffe und Speicherungen notwendigen Einwilligung i. S. v. Art. 4 Nr. 11 DSGVO beispielsweise für selbstgehostete Trackingdienste vielfach nicht wirksam eingeholt. Die hierfür genutzten Einwilligungsbanner (sog. Cookie-Banner) entsprechen regelmäßig im Hinblick auf die Informiertheit und die Freiwilligkeit nicht den Vorgaben der DSGVO. Dies überrascht umso mehr, als dass mittlerweile auch die deutschen Gerichte[79] klare Vorgaben zur Gestaltung von Einwilligungsbannern machen.

Zudem konnte mein Haus im Rahmen von Kontrollen mittels technischer Analysen feststellen, dass die Speicherdauer von grundsätzlich zulässigen Cookies im Hinblick auf den verfolgten Zweck unnötig lange angelegt ist. So muss beispielsweise ein sog. Session-Cookie, welches Informationen über die aktuelle Sitzung auf dem Endgerät von Nutzenden speichert, für die Erfüllung seines Zwecks nicht über diese Sitzung hinaus gespeichert werden. Gleichwohl hat mein Haus für derlei Cookies teils Speicherdauern von über 100 Tagen festgestellt.

Aufgefallen ist meinem Haus auch, dass in solchen Fällen, in denen öffentliche Stellen des Bundes für das Hosting ihrer Webseite die Leistung einer IT-Dienstleistungsbehörde in Anspruch nehmen, nicht immer die hierfür notwendigen Vereinbarungen i. S. d. Art. 28 DSGVO getroffen werden. Hiernach ist für das Hosting der eigenen Webseite durch Dritte regelmäßig ein Auftragsverarbeitungsvertrag mit diesen abzuschließen.

Beratung

Einen besonderen Schwerpunkt hat mein Haus bei der Wahrnehmung der Aufsicht auch vergangenes Jahr wieder auf den Bereich der ergebnisorientierten Beratung zur datenschutzkonformen Ausgestaltung digitaler Dienste gelegt. Hier ließen sich, unsere rechtzeitige Einbindung vorausgesetzt, belastbare und für alle Beteiligten zufriedenstellende Ergebnisse erzielen.

Durch Rundschreiben wie beispielsweise zum Thema „Einbindung von Videoinhalten auf Webseiten öffentlicher Stellen des Bundes" oder Internetbeiträgen wie beispielsweise zum Thema „Einsatz des Webseiten-Analysetools Matomo" informiert mein Haus die beaufsichtigten Stellen auch proaktiv über datenschutzrechtliche Wertungen meiner Behörde.

Dennoch nehme ich zu meinem Bedauern weiterhin bei einigen öffentlichen Stellen des Bundes eine gewisse Beratungsresistenz wahr. Bei teils beharrlicher Verweigerung, Verarbeitungsprozesse auf eine datenschutzkonforme Art und Weise umzustellen, hat meine Behörde auch vergangenes Jahr vereinzelt von dem Recht Gebrauch gemacht, öffentliche Stellen des Bundes gemäß Art. 58 Abs. 2 DSGVO zur Vornahme konkreter Handlungen anzuweisen. Trotzdem möchte ich auch 2025 vorrangig auf Dialog und Beratung setzen, um den Anspruch einer effizienten und digitalen öffentlichen Verwaltung auch weiterhin in Einklang mit der Wahrung von Rechten der Bürgerinnen und Bürger aus der DSGVO zu bringen.

5.4.2 Der Digital Service Act und das Digitale Dienste Gesetz

Mit dem Digital Service Act (DSA) gelten seit dem 17. Februar 2024 EU-weit neue Regelungen zur Datennutzung für Tracking und Profiling im Rahmen von Online-Werbung. Mit der nationalen Umsetzung im Digitale-Dienste-Gesetz (DDG) erhielt mein Haus seit dem 14. Mai 2024 neue Aufgaben, die für eine wirksame Durchsetzung dieser Regelungen sorgen.

79 Beispielhaft folgende Entscheidungen: OLG Köln, 19. Januar 2024 – 6 U 80/23 oder LG München I, 29. November 2022 – 33 O 14776/19.

Die Regelungen des DSA 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.

Mit Inkrafttreten des DDG, dem deutschen Durchführungsgesetz zum DSA, wurde eine nationale Koordinierungsstelle für Digitale Dienste eingerichtet, welche die Aufsicht über die Anbieter digitaler Dienste und die Koordination von Beschwerden nach DSA übernimmt. Diese Aufgabe fällt in Deutschland der Bundesnetzagentur (BNetzA) zu.

Gemäß § 12 Abs. 3 DDG ist mein Haus die zuständige Behörde für die Durchsetzung der in Art. 26 Abs. 3 und Art. 28 Abs. 2 DSA enthaltenen Werbeverbote auf deutschen Online-Plattformen: Erstens das Verbot, profilbasierte Werbung gegenüber Minderjährigen auszuspielen (Art. 28 Abs. 2 DSA) sowie zweitens das Verbot, Werbung auch gegenüber Erwachsenen auszuspielen, wenn für die Profilbildung besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO verwendet wurden (Art. 26 Abs. 3 DSA).

DSA und DDG eröffnen zum einen die Möglichkeit für Bürgerinnen und Bürger zur Beschwerde wegen Verstößen gegen Art. 26 Abs. 3 oder Art. 28 Abs. 2 DSA bei der BNetzA als zentraler Beschwerdestelle i. S. v. § 20 DDG, deren inhaltliche Prüfung dann meinem Haus obliegt. Zum anderen gehen meine Mitarbeitenden im Rahmen unserer Ressourcen auch proaktiv auf deutsche Online-Plattformen zu, um sie bei der Einhaltung der Art. 26 Abs. 3 oder Art. 28 Abs. 2 DSA unterstützend zu beraten und so das Risiko für die Verletzung der Rechte von Bürgerinnen und Bürgern frühzeitig zu minimieren.

Die neuen Regelungen des DSA und des DDG für den Datenschutz, insbesondere im Bereich Profiling, sind aus meiner Sicht geeignet, zu einem sichereren Online-Umfeld für alle Nutzenden beizutragen. Meine Aufgaben sind daher für die Durchsetzung dieser Regelungen von zentraler Bedeutung.

Querverweis:

7.3.7 Altersprüfung in Digitalen Diensten

5.4.3 Automatisiertes und vernetztes Fahren ohne umfassende Videoerfassung öffentlicher Räume

Automatisiertes und vernetztes Fahren im Straßenverkehr benötigt ein umfassendes und genaues Bild der Fahrzeugumgebung, um die richtigen Fahrentscheidungen treffen zu können. Wie ist das mit dem Datenschutz vereinbar?

Ein automatisiert und vernetzt fahrendes Fahrzeug muss seine Umgebung sehen und hören, um sich situationsabhängig selbst steuern zu können. Die DSK hat unter meiner Federführung bereits 2023 mit einem Positionspapier deutlich gemacht, wie aus ihrer Sicht die Entwicklung zuverlässig verkehrssicherer Fahrzeuge gelingen kann, ohne dabei das Recht einer oder eines Dritten auf angemessenen Schutz der Privatheit zu verletzen. Für den Betrieb eines automatisiert und vernetzt fahrenden Fahrzeugs müssen Dritte davon ausgehen können, dass die während der Fahrt erfassten Video- und Audiodaten über die Umgebung in einem geschlossenen System verarbeitet werden. Nur in eindeutig bestimmten Ausnahmefällen in einem eng begrenzten Umfang, etwa zur Aufklärung eines Unfallhergangs oder unvorhergesehenen, möglicherweise verkehrsgefährdenden Fehlers des Fahrassistenten, dürfen nach §§ 63a bis 63f Straßenverkehrsgesetz Audio- und Videodaten für konkret bestimmte Zwecke übermittelt und verwendet werden.

Die Autohersteller und ihre Zulieferer beabsichtigen, mögliche allgemein im Betrieb der von ihnen hergestellten Fahrzeuge oder Komponenten auftretende Mängel der automatisierten und vernetzten Fahrfunktionen und hochentwickelten Fahrzeugassistenten erkennen und auf Basis von ereignisbasiert erhobenen Daten forensisch untersuchen zu können. Die daraus gewonnenen Erkenntnisse sollen für eine Mangelbehebung und allgemeine Weiterentwicklung der automatisierten und vernetzten Fahrfunktionen und anderen hochentwickelten Fahrzeugassistenten verwendet werden. Wenn dazu Audio- und Videodaten zum Zeitpunkt eines Ereignisses (Trigger) erforderlich sind, kann es nach Art. 6 Abs. 1 lit. f) DSGVO als Ergebnis einer Abwägung der berechtigten Interessen der Hersteller und ihrer Zulieferer zur Entwicklung und Fertigung verkehrssicherer Fahrzeuge und Komponenten gegen Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen erlaubt sein, Audio- und Videodaten über die Umgebung für die Zwecke der Mangelbehebung und Verbesserung zu verarbeiten. Ein besserer Schutz vulnerabler Verkehrsteilnehmenden im Straßenverkehr durch etwa einen Notbremsassistenten oder andere automatisierte und vernetzte Fahrfunktionen ist nur zu erreichen, wenn die technischen Systeme das voraussichtliche Verkehrsverhalten der vulnerablen Personen richtig einschätzen können. Dazu müssen zuweilen gerade die Daten verarbeitet werden, die einen besonderen Grundrechtsschutz genießen. Es muss zugleich gewährleistet sein,

dass Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen verhältnismäßig bleiben.

Soweit es allgemein, also über bloße Entwicklungsfahrten hinaus, um eine audiovisuelle Umgebungserfassung durch potentiell alle automatisiert und vernetzt fahrenden Fahrzeuge geht, setze ich mich weiterhin dafür ein, dass erfasste personenbezogene Daten nur unter konkret und eng zu fassenden Bedingungen aus Fahrzeugen an Dritte übertragen werden dürfen und durch geeignete fahrzeugtechnische Vorschriften der Schutz vor zweckfremder Verwendung der erfassten Daten gewährleistet ist. Die audiovisuellen Umgebungsdaten dienen in erster Linie der Fahrzeugsteuerung und müssen für diesen Zweck zu keinem Zeitpunkt das Fahrzeug verlassen. Vor diesem Hintergrund begrüße ich es sehr, dass die Hersteller und ihre Zulieferer über ihren europäischen Interessenverband ACEA meinen belgischen Kolleginnen und Kollegen einen Entwurf für Verhaltensregeln nach Art. 40 DSGVO für den Umgang insbesondere mit Audio- und Videodaten zur Entwicklung von hochentwickelten Fahrassistenten und automatisierten Fahrfunktionen vorgelegt haben. Gemeinsam mit meinen Kolleginnen und Kollegen in den Mitgliedstaaten der EU und in den Ländern stehe ich bereit, Lösungen zu finden, die Hersteller und Zulieferer die Innovation ihrer hochentwickelten Fahrassistenten und automatisierten und vernetzten Fahrfunktionen ermöglichen, ohne dadurch unangemessene Risiken für die Grundrechte und Grundfreiheiten zu schaffen. Die Erfassung einer großen Anzahl von sich in öffentlich zugänglichen Straßenräumen bewegenden Dritten (Passanten; Versammlungen usw.) bedarf ebenso wie die Übermittlung und weiteren Verarbeitung der Daten für die erforderliche Rechtssicherheit einer gesonderten und hinreichend konkreten gesetzlichen Regelung. Dies gilt umso mehr mit Blick auf Fahrzeuge, deren Hersteller den Schwerpunkt ihrer Datenverarbeitung in einem Drittstaat haben, in welchem das Recht auf Datenschutz nicht vergleichbar den EU-Standards angemessen geschützt wird und insoweit auch nicht unter etwaige Verhaltensregeln fielen. Die wichtige Erhöhung der Verkehrssicherheit von Fahrzeugen durch automatisiertes und vernetztes Fahren muss mit einem angemessenen Schutz der dabei verarbeiteten personenbezogenen Daten einhergehen.

5.4.4 Neue Gesetzgebung zur Bekämpfung von Finanzkriminalität

Im Koalitionsvertrag für die 20. Wahlperiode wurde vereinbart, die Bekämpfung der Finanzkriminalität zu verbessern. Das Finanzkriminalitätsbekämpfungsgesetz (FKBG) sollte hierbei ein zentraler Baustein werden. Ob und wann das darin vorgesehene neue Bundesamt zur Bekämpfung der Finanzkriminalität (BBF) nach dem vorzeitigen Koalitionsende noch errichtet wird, bleibt abzuwarten. Daneben wurde mit dem Vermögensverschleierungsbekämpfungsgesetz (VVBG) 2024 ein weiterer Teil des Projektes zumindest in die Ressortabstimmung gegeben. Mit der dortigen Pflicht zur Auskunft über das eigene Vermögen betritt der Gesetzgeber Neuland.

Wesentlicher Inhalt des FKBG war die Errichtung des BBF inkl. des Ermittlungszentrums Geldwäsche als eine neue Strafverfolgungsbehörde zur Verfolgung internationaler Geldwäsche mit Deutschlandbezug. Über das Gesetzgebungsverfahren habe ich bereits in meinem 31. Tätigkeitsbericht ausführlich berichtet.[80] Ursprünglich war vorgesehen, dass die neue Behörde im Jahr 2024 aufgebaut wird und 2025 ihre operative Tätigkeit aufnimmt. Mit dem vorzeitigen Ende der 20. Wahlperiode des Deutschen Bundestages ist der Fortgang des Gesetzgebungsverfahrens offen. Inwieweit meine bisherigen Stellungnahmen Berücksichtigung finden, ist ebenso ungewiss. Sollte an den Plänen zur Errichtung des BBF festgehalten werden, freue ich mich darauf, diesem bereits im Aufbau beratend zur Seite zu stehen und auf eine datenschutzfreundliche Ausgestaltung hinzuwirken.

Im April 2024 wurde ich zusätzlich in die Ressortabstimmung zum Entwurf des Vermögensverschleierungsbekämpfungsgesetzes mit einbezogen. Das Entwurfsstadium hat das Gesetz bis zum jetzigen Zeitpunkt nicht verlassen. Kern des geplanten Gesetzes war das sog. Vermögensermittlungsgesetz. In diesem sollte für Fälle mit besonderem Geldwäsche- oder Sanktionsrisiko eine neue Behörde geschaffen werden, das Ermittlungszentrum Vermögensverschleierung (EZV). Organisatorisch war eine Eingliederung in das BBF vorgesehen. Anknüpfungspunkt für das Tätigwerden sind Vermögensgegenstände; bei denen Anhaltspunkte bestehen, dass sie aus einer rechtswidrigen Tat stammen. Die Behörde sollte ermächtigt werden, mittels eines Verwaltungsverfahrens die Herkunft der für den Erwerb solcher Vermögenswerte aufgewendeten Mittel oder die wirtschaftlichen Berechtigungen an solchen Vermögenswerten aufzuklären. Neuerung war, dass die Ermittlungen erstmals vom Gegenstand ausgehen. Das administrative Ermittlungsverfahren sah dabei abgestufte Eingriffsbefugnisse vor. Diese begannen mit Registerabfragen und endeten mit einer Befugnis, von dem Eigentümer verdächtiger Ver-

80 31. TB Nr. 3.3.3

mögensgegenstände Auskünfte zu verlangen. Diese war als Obliegenheit ausgestaltet.

Ich hatte und habe neben der fehlenden Gesetzgebungszuständigkeit des Bundes auch weitere erhebliche datenschutzrechtliche Zweifel am Gesetzgebungsentwurf. So habe ich insbesondere das Fehlen von ereignisunabhängigen Aussonderungsprüffristen oder die Nichteinhaltung des Grundsatzes der hypothetischen Datenneuerhebung im Rahmen von zwischenbehördlichen Datenübermittlungen kritisiert.

Begrüßenswert ist, dass ich frühzeitig in die Ressortabstimmung eingebunden wurde. Ich habe den dortigen Austausch als sehr konstruktiv wahrgenommen und gehe davon aus, dass meine Anregungen Beachtung finden.

Ich bin daher zuversichtlich, dass die etablierten Gesprächsfäden wiederaufgenommen werden, sollten die Gesetzgebungsverfahren fortgeführt werden.

5.5 Arbeit und Soziales

5.5.1 Beschäftigtendatengesetz

In Umsetzung des Koalitionsvertrages für die 20. Legislaturperiode hat das Bundesministerium für Arbeit und Soziales (BMAS) in gemeinsamer Federführung mit dem Bundesministerium des Innern und für Heimat (BMI) den Entwurf eines Gesetzes zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt (Beschäftigtendatengesetz – BeschDG) vorgelegt. Infolge des vorzeitigen Endes der Legislatur scheitert allerdings auch der jüngste Vorstoß zur Regelung des Umgangs mit Beschäftigtendaten.

Die Initiative von BMAS und BMI begrüße ich sehr, entspricht sie doch langjährigen Forderungen und Erwartungen wie auch rechtlichen und tatsächlichen Erfordernissen. Auch die Datenschutzkonferenz (DSK) hatte schon 2014 die Schaffung eines Beschäftigtendatenschutzgesetzes gefordert.[81] In einer Entschließung vom April 2022 hatte die DSK zu verschiedenen Bereichen wie etwa dem Einsatz algorithmischer Systeme einschließlich Künstlicher Intelligenz (KI) oder Datenverarbeitung bei Bewerbungs- und Auswahlverfahren die Schaffung gesetzlicher Rahmenbedingungen empfohlen.

Viele der von der DSK bereits erwähnten Themenkomplexe finden sich im Entwurf eines Beschäftigtendatengesetzes grundsätzlich wieder. Ich bedaure, dass spezifische Regelungen zum Beschäftigtendatenschutz wegen des vorzeitigen Endes der 20. Legislaturperiode nicht mehr geschaffen werden konnten. Die nach wie vor überfällige Reform des deutschen Beschäftigtendatenschutzes darf insbesondere auch vor dem Hintergrund des Urteils des Europäischen Gerichtshofs (EuGH)[82] [83] vom 30. März 2023 nicht aus den Augen verloren werden. Der EuGH hatte darin unter anderem Anforderungen an nationale Vorschriften formuliert, die auf der Grundlage der Öffnungsklausel des Art. 88 Abs. 1 der DSGVO erlassen werden.

Ich hoffe, dass das Vorhaben der Schaffung spezifischer Gesetzesregelungen zum Beschäftigtendatenschutz in der kommenden Legislaturperiode erneut aufgegriffen wird. Gerne werde ich auch ein neues Gesetzgebungsverfahren konstruktiv beratend begleiten.

5.5.2 Kindergrundsicherung

Der 20. Deutsche Bundestag hat den Regierungsentwurf eines Gesetzes zur Einführung einer Kindergrundsicherung (BKG) nicht mehr verabschiedet. Aus der Perspektive des Datenschutzes bestanden keine grundlegenden Bedenken gegen das Gesetz. Sollte das Projekt in der 21. Legislaturperiode wiederaufgenommen werden, werde ich Regierung und Parlament auch weiterhin konstruktiv beraten, so dass die staatlichen Leistungen für Kinder einfach, unkompliziert, digital und datenschutzfreundlich gewährt werden können.

Das Gesetz zur Einführung einer Kindergrundsicherung[84] wurde in der 20. Wahlperiode des Deutschen Bundestages nicht mehr verabschiedet. Der Gesetzesentwurf sah vor, dass zur Bekämpfung von Kinderarmut die bisherigen finanziellen Förderungen für Kinder durch einen einkommensunabhängigen Kindergarantiebetrag für alle Kinder und Jugendliche (ehemals Kindergeld nach dem Bundeskindergeldgesetz) sowie einem einkommensabhängigen und altersgestaffelten Kinderzusatzbetrag (ehemals Kinderzuschlag) ersetzt werden. Zur Vereinfachung für Antragsteller sollten (teil)-automa-

81 25. TB Nr. 9.3.1

82 Urteil des EuGHs vom 30. März 2023 in der Rechtssache C-34/21, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0034

83 s. dazu auch Entschließung der DSK „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz!“, abrufbar unter: https://datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Beschaeftigtendatenschutz.pdf

84 BKG-Entwurf, BT-Drs. 20/9092, abrufbar unter: https://dserver.bundestag.de/btd/20/090/2009092.pdf

tisierte Datenabrufe aus verschiedenen Datenquellen, z. B. Steuerdaten, Sozialversicherungsdaten, Daten der Arbeitgeber, stattfinden. Mit dem „Kindergrundsicherungs-Check“ sollte standardisiert vorab geprüft werden, ob einem Kind der Kinderzusatzbetrag möglicherweise zusteht, ohne dass zuvor ein förmlicher Antrag auf Kinderzusatzbetrag gestellt wurde. Für den Check sollten Daten, die in Behörden, insbesondere Finanz- und Sozialbehörden, bereits in elektronischer Form vorliegen, zur Vorprüfung des Anspruchs auf den Kinderzusatzbetrag verwendet werden.

Bereits im vorherigen Tätigkeitsbericht hatte ich mich zum Entwurf des Gesetzes zur Einführung einer Kindergrundsicherung geäußert:[85] meiner Einschätzung nach bestehen – trotz Nachbesserungsbedarf in einzelnen Punkten – keine grundsätzlichen datenschutzrechtlichen Bedenken. Der (teil-) automatisierte Datenaustausch zwischen Behörden steht im Einklang mit dem im Rahmen der Verwaltungsdigitalisierung insgesamt verfolgten „Once-Only-Prinzip“. Dies verfolgt das Ziel, notwendige Angaben nur ein einziges Mal von der betroffenen Person durch Behörden zu erheben und dann für verschiedene Zwecke von Behörden weiter zu nutzen. Vor dem Hintergrund des besonderen Gewichts der Zielsetzung, Kinderarmut wirksam zu bekämpfen, und dem Nutzen für die Betroffenen selber, halte ich eine gesetzliche Abweichung vom verfassungsrechtlich verbürgten und im Sozialrecht ausdrücklich in § 67a Abs. 2 SGB X geltenden Ersterhebungsgrundsatz für datenschutzrechtlich vertretbar.

Die Zielsetzung, durch digitale und unbürokratische Verfahren den Bezug von staatlichen Leistungen für Familien zu erleichtern, begrüße und unterstütze ich. Sollte der Gesetzgeber das Vorhaben in vergleichbarer oder abgewandelter Form wieder aufgreifen, wären für eine datenschutzkonforme Gestaltung insbesondere die folgenden Aspekte zu berücksichtigen:

- **Durchführung des Kindergrundsicherungs-Checks nur mit ausdrücklicher Einwilligung**
  Von den vielen Millionen Berechtigten für den Kindergarantiebetrag wird nur ein kleinerer Teil Anspruch auf den Kinderzusatzbetrag haben. Vielen Bürgerinnen und Bürger kommen aufgrund ihres Einkommens dafür nicht in Betracht und wissen dies auch. Um eine massenhafte antraglose Verarbeitung der teilweise sehr sensiblen Daten dieser Personen im Rahmen des Kindergrundsicherungschecks zu vermeiden, empfehle ich, in der gesetzlichen Regelung die Einholung der Einwilligung der betroffenen Personen vorzusehen.
- **(Automatisierte) Datenerhebung im Rahmen des Antragsverfahrens bei Arbeitgebern**
  Beziehende von Sozialleistungen haben häufig Vorbehalte gegen die Offenbarung des Bezugs bedürftigkeitsabhängiger Leistungen gegenüber ihrem Arbeitgeber. Sie befürchten eine Stigmatisierung und könnten dadurch ggf. von der Beantragung dieser Leistungen abgehalten werden. Insofern sollten Betroffene auch die Möglichkeit haben, erforderliche Nachweise selbst beizubringen, wenn sie das möchten.
- **Gewährleistung erhöhter Schutzanforderungen bei Anwendung des „Once-Only-Prinzips“**, insbesondere Transparenz über das Datenschutzcockpit (§ 10 OZG)
- **Verarbeitung der Identifikationsnummer nach dem Identifikationsnummerngesetz (IDNrG) statt eine Verarbeitung der Steuer-Identifikationsnummer**
  Die Steuer-Identifikationsnummer ist zwar materiell identisch mit der Identifikationsnummer gemäß § 1 IDNrG; da jedoch ein rechtlich fingierter Unterschied zwischen beiden Zuordnungsmerkmalen besteht, gelten die erhöhten Schutzanforderungen an die Nutzung der Identifikationsnummer nicht unmittelbar. Zu den erhöhten Schutzanforderungen an die Nutzung der IDNr gehören u. a. eine sehr strenge Zweckbindung (§ 5 IDNrG), eine strukturelle Hemmung der Datenaustauschbarkeit (§ 7 Abs. 2 IDNrG) sowie die Transparentmachung über das Datenschutzcockpit (§ 9 IDNrG).

Querverweis:

7.2.1 Registermodernisierung

85 32. TB Nr. 8.11

6 Informationsfreiheit

6.1 Statistische Auswertungen zur Informationsfreiheit

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

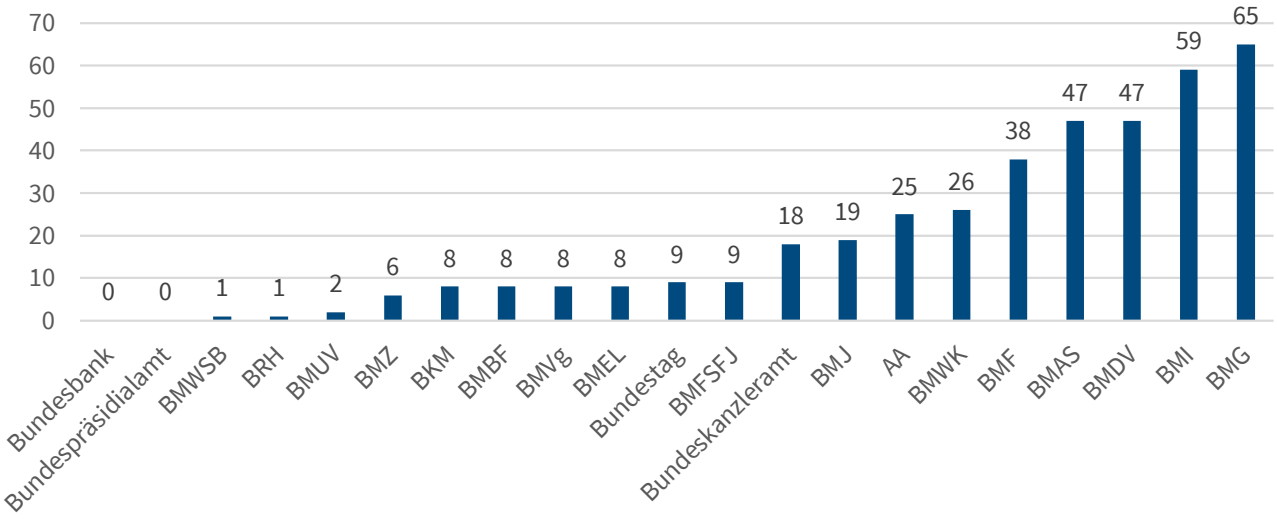
Mich erreichten im Berichtszeitraum insgesamt 595 Eingaben. Damit ist die Zahl der Eingaben im Vergleich zu den Vorjahren abermals gestiegen. In 404 Fällen riefen mich Petenten nach § 12 Abs. 1 IFG an und rügten eine Verletzung ihres Rechts auf Informationszugang nach dem IFG. Mit der Bitte um Vermittlung bei Anträgen nach dem UIG wandten sich antragstellende Personen in 26 Fällen an mich (§ 7a UIG). Im Vergleich zum Vorjahr stieg die Zahl der Vermittlungsbitten hinsichtlich der Anträge nach dem UIG. Die Zahlen bewegen sich aber auch 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 ihre Geschäftsbereiche verteilen sich die Eingaben wie aus der nachfolgenden Grafik ersichtlich. Die höchste Zahl der Eingaben betraf das BMG und seinen Geschäftsbereich. Wie in den Vorjahren ergibt sich dieses Ergebnis aus einem erhöhten Interesse an Fragen in Zusammenhang mit der vergangenen pandemischen Lage und der Entwicklung und Anwendung von Impfstoffen.

IFG-Anträge an meine Behörde

Im Berichtszeitraum gingen insgesamt 126 Anträge auf Informationszugang bei mir ein. Diese Anträge richteten sich sowohl auf den Zugang zu Akteninhalten im Rahmen von eigenen, an meine Behörde gerichteten Vermittlungsbitten nach deren Abschluss, als auch auf meine Stellungnahmen zu Gesetzesvorhaben. Im Vergleich zu den Vorjahren ist das Antragsaufkommen gleichbleibend.

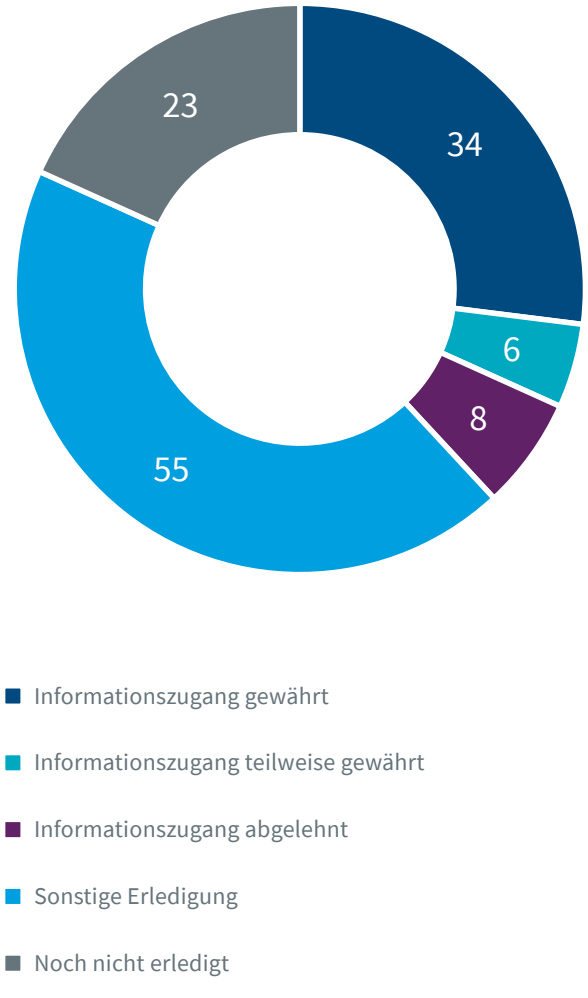
Anrufungen nach § 12 IFG im Berichtszeitraum nach Ressorts



Aus der Abbildung ergeben sich die Verteilung der (teilweisen) Zugangsgewährung, der Zugangsablehnung und der sonstigen Erledigung im Jahr 2024. 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 erbetenen Informationen in meinem Haus nicht vorliegen.

IFG-Anträge an meine Behörde im Berichtsjahr



6.2 Gremien

6.2.1 Konferenz der Informationsfreiheitsbeauftragten

Im Berichtsjahr hatte die Sächsische Datenschutz- und Transparenzbeauftragte den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten (IFK) inne. Die IFK widmete sich einer Vielzahl von Aspekten der Fortentwicklung staatlicher Transparenz in Bund und Ländern.

Die IFK ist ein Zusammenschluss der Beauftragten für Akteneinsicht, Informationsfreiheit und Transparenz des Bundes und der Länder mit dem Ziel, das Recht auf Informationszugang zu fördern und gemeinsam für seine Fortentwicklung einzutreten. Die IFK verständigt sich auf gemeinsame Positionen in Fragen der Informationsfreiheit. Dies geschieht insbesondere mit Entschließungen, Positionspapiere und Stellungnahmen. In ihrer 46. Sitzung am 5. Juni 2024 in Dresden, der 47. Sitzung am 27. November 2024 in Leipzig und auch dazwischen im Umlaufverfahren hat die IFK die nachfolgenden Entschließungen und Praxishandreichungen verabschiedet:

Bereits Ende April 2024 hat die IFK einen Leitfaden zum Aufbau und Betrieb staatlicher Transparenzportale herausgegeben. Die Praxishandreichung richtet sich an die Betreiber der Portale, an informationspflichtige Stellen sowie Nutzerinnen und Nutzer, die die Qualität einer Plattform prüfen möchten. Dazu gibt die IFK übersichtlich und kompakt Empfehlungen und Hinweise zur Gestaltung der Plattformen, benennt Anforderungen und zeigt konkrete Umsetzungsmöglichkeiten auf. Außerdem enthält der Leitfaden eine Checkliste, die die wesentlichen Kriterien zusammenfassend aufführt, beispielsweise zu den technischen Rahmenbedingungen, organisatorischen Festlegungen, der Barrierefreiheit und zum Verzicht auf Tracking.

Ende Juli 2024 hat die IFK Empfehlungen zur Erfüllung des Informationszugangsrechts veröffentlicht. Mit den Hinweisen richtet sich die IFK an öffentliche Stellen, die Informationsfreiheits-/Transparenz- und Umweltinformationsgesetzen unterliegen. Die Empfehlungen folgen dem Grundsatz »Informationsfreiheit by Design«. Im Kern geht es darum, dass informationspflichtige Stellen Daten und Dokumente zuverlässig, effizient und vollständig zur Verfügung stellen können. Um dieses Ziel zu erreichen, empfiehlt die IFK eine Reihe von organisatorischen und technischen Maßnahmen mit Fokus auf der elektronischen Aktenführung. Damit können öffentliche Stellen ihren Verwaltungsaufwand zur Bereitstellung amtlicher Informationen verringern und Verfahren beschleunigen.

In der Entschließung „Gut informiert im Superwahljahr 2024!“ hat die IFK darauf hingewiesen, dass besonders vor Wahlen die Gesetze über Transparenz und Informationsfreiheit für Wählerinnen und Wähler ein geeignetes Mittel sein können, um sich aus erster Hand Information zu verschaffen, die einen ungefilterten Eindruck über die tatsächliche Arbeit von Regierung und Verwaltung geben. Auch diese Informationen können eine valide und seriöse Grundlage für eine fundierte Meinungsbildung beziehungsweise öffentliche Diskussion sein, um später gut informiert und sachorientiert eine Wahlentscheidung zu treffen.

Die Entschließung „Gleicher Auftrag – gleicher Informationsanspruch gegenüber öffentlich-rechtlichen Rundfunkanstalten!“ befasst sich damit, dass das Ob und Wie des Informationsanspruchs vom Sitz der jeweiligen Rundfunkanstalt abhängt, obwohl alle öffentlich-rechtlichen Rundfunkanstalten im Kern den gleichen Auftrag haben. Bei Mehrländereinrichtungen scheitert ein wirksamer Informationszugangsanspruch häufig an dem Erfordernis, dass dieser staatsvertraglich geregelt sein muss und eine entsprechende Regelung fehlt. Der öffentlich-rechtliche Rundfunk ist Medium und Faktor öffentlicher Meinungsbildung. Die IFK fordert daher die Gesetzgeber auf, auch in diesem Bereich mit Schaffung bundesweit einheitlich hoher Standards für Transparenz zu sorgen. Eine Ausnahme gilt nur für die grundrechtlich geschützte journalistisch-redaktionelle Tätigkeit. Dies stärkt die Unabhängigkeit des öffentlich-rechtlichen Rundfunks.

Mit der Entschließung „Pflicht zur Informationsfreiheit und Transparenz auch für Kommunen in Hessen und Sachsen!“ fordert die IFK die Landesgesetzgeber in Sachsen und Hessen auf, ihren Bürgerinnen und Bürgern verbindliche Informationszugangsansprüche auch gegenüber den Kommunen zu gewähren. Bislang ist diese Entscheidung dort den einzelnen Kommunen überlassen, die sich freiwillig zur Transparenz verpflichten können. Im Gegensatz zu Hessen und Sachsen gelten die Transparenz- bzw. Informationsfreiheitsgesetze in allen anderen Ländern auch für Kommunen. Damit sind die Kommunen in den meisten Ländern zur Informationserteilung nach Maßgabe des jeweiligen Landesgesetzes verpflichtet.

Anknüpfend an eine frühere Entschließung aus dem Jahr 2022[86] [87] fordert die IFK in der Entschließung „Ein modernes Transparenzgesetz für Niedersachsen jetzt!“ den niedersächsischen Landesgesetzgeber auf, die im Koalitionsvertrag für die 19. Wahlperiode des Niedersächsischen Landtages enthaltene Vereinbarung, ein progressives Transparenzgesetz schaffen zu wollen, zeitnah umzusetzen. Dazu hat die IFK Vorschläge gemacht, welche Regelungen ein solches Gesetz zwingend enthalten muss.

Im Jahr 2025 hat Thüringen den Vorsitz der IFK inne.

6.2.2 Internationale Konferenz der Informationsfreiheitsbeauftragten

Die ICIC ist ein internationales Forum, das sich mit Fragen der Informationsfreiheit und Transparenz in der Regierungsführung beschäftigt. Die 15. Internationale Konferenz der Informationsfreiheitsbeauftragten (ICIC) stand unter dem Thema „Die Ermächtigung des Einzelnen durch Informationszugang: Sicherstellung von Transparenz und Inklusion in einer vernetzten Welt“ und fand vom 3. bis 5. Juni 2024 in Tirana, Albanien statt.

Zu den Hauptaufgaben der ICIC gehören der Austausch von Best Practices, die Förderung von Informationsfreiheitsgesetzen und die Unterstützung von Beauftragten für Informationsfreiheit in verschiedenen Ländern. Die Mitglieder der ICIC setzen sich aus Informationsfreiheitsbeauftragten, Regierungsvertretern, zivilgesellschaftlichen Organisationen und anderen Interessengruppen zusammen, die sich für die Stärkung der Informationsrechte und die Verbesserung der Transparenz in der Verwaltung einsetzen. Die Konferenz bietet eine Plattform für Diskussionen und die Entwicklung gemeinsamer Strategien zur Förderung der Informationsfreiheit weltweit.

Die Konferenz organisiert regelmäßig Veranstaltungen, Fortbildungen und Workshops, um das Bewusstsein für Informationsfreiheit zu schärfen und den Austausch zwischen den Mitgliedern zu fördern.

Ein weiterer wichtiger Aspekt ist die Rolle der ICIC bei der Unterstützung von Ländern, die ihre Informationsfreiheitsgesetze verbessern oder implementieren möchten. Die Konferenz bietet auch eine Plattform für die Diskussion über Herausforderungen, die mit der Umsetzung von Informationsfreiheitsgesetzen verbunden sind, wie etwa Datenschutz, Zugang zu Informationen und die Balance zwischen Sicherheit und Transparenz.

In einer zunehmend digitalen Welt kommt der ICIC eine besondere Rolle zu. Der Zugang zu Informationen und

86 Alle Entschließungen der IFK sind abrufbar unter: www.bfdi.bund.de/ifk-entschließungen
87 31. TB Nr. 6.1

die Transparenz von Regierungen sind für die Stärkung der Demokratie und das Vertrauen der Bürgerinnen und Bürger von entscheidender Bedeutung.

Die Mission der ICIC besteht darin, die Prinzipien der Informationsfreiheit und Transparenz in der Regierungsführung weltweit zu fördern. Die Konferenz setzt sich dafür ein, den Zugang zu Informationen für Bürgerinnen und Bürger zu verbessern und die Verantwortlichkeit von Regierungen zu stärken.

Zu diesem Zweck engagiert sich die Konferenz für den Austausch von Best Practices und Erfahrungen zwischen den Mitgliedern, um die Umsetzung und Durchsetzung von Informationsfreiheitsgesetzen zu unterstützen. Die ICIC strebt auch an, die Zusammenarbeit zwischen verschiedenen Akteuren, einschließlich Regierungen, zivilgesellschaftlichen Organisationen und internationalen Institutionen, zu fördern, um eine Kultur der Offenheit und des Vertrauens zu schaffen.

Die ICIC 2024 in Albanien brachte eine Vielzahl von Akteuren zusammen, darunter Informationsfreiheitsbeauftragte, Regierungsvertreterinnen und -vertreter, NGOs, Wissenschaftlerinnen und Wissenschaftler und Aktivistinnen und Aktivisten.

An der Konferenz haben sich meine Mitarbeitenden mit mehreren Beiträgen beteiligt. Zum einen haben diese im Rahmen des Panels „Ein ausgewogenes Verhältnis zwischen ATI (Access to Information) und Datenschutzrechten im digitalen Bereich. Wie können wir die persönlichen Daten der Bürgerinnen und Bürger schützen und gleichzeitig Anstrengungen unternehmen, um digitale Informationsrechte zu gewährleisten?“ die aus meiner Sicht drängendsten Herausforderungen dargestellt.

Ich bin grundsätzlich der Auffassung, dass Datenschutz und das Recht auf Zugang zu Informationen in einen angemessenen Ausgleich gebracht werden können. Das gilt sowohl für den Zugang zu amtlichen Informationen als auch für den Zugang zu Umweltinformationen nichtöffentlicher Stellen.

Herausforderungen sehe ich bei der proaktiven Bereitstellung größerer und aktueller Informationsbestände durch ein Transparenzgesetz, wie es im Koalitionsvertrag der 20. Wahlperiode zusammen mit einem Rechtsanspruch auf Open-Data vereinbart war.

Die Idee hinter Open-Data ist der – automatisierte – umfassende Zugriff auf Daten in offenen Formaten, deren Aufbereitung und Rekontextualisierung. Hier liegt meines Erachtens eine der Herausforderungen der Digitalisierung im Spannungsfeld zwischen offenen Daten und Datenschutz.

Zum anderen habe ich auf Einladung des Europarats in dem von ihm geleiteten Panel dargestellt, welche Vorteile Deutschland von der Ratifizierung der Tromsø-Konvention hätte.

In den vergangenen Jahren habe ich mich auf nationaler und internationaler Ebene für die Ratifizierung der Konvention eingesetzt. Bereits anlässlich der 8. Internationalen Konferenz der Informationsfreiheitsbeauftragten in Berlin 2013 hatten die teilnehmenden Beauftragten in ihrer „Berliner Erklärung“ die Ratifizierung der Tromsø-Konvention in so vielen Ländern wie möglich zu gefordert.

Auf nationaler Ebene rief die Konferenz der Informationsfreiheitsbeauftragten in Deutschland in den Jahren 2013 und 2021 ebenfalls zur Ratifizierung auf. Aus meiner Sicht würde Deutschland von einer Ratifizierung zumindest auf Bundesebene profitieren, da die Konvention über die derzeitige Rechtslage hinausgeht. Im internationalen Vergleich liegt Deutschland – beispielsweise in dem von dem Center for Law and Democracy erstellten Ranking der Rechtsgrundlagen für den Zugang zu Informationen – auf Platz 127 von 140.[88] Die Bundesregierung lehnte die Ratifizierung in der vergangenen Dekade mit dem Argument ab, dass das bestehende deutsche Informationsfreiheitsgesetz bereits einen ausreichenden Rahmen biete, um den Zugang zu Regierungsinformationen zu gewähren. Ich habe anhand von fünf wesentlichen Aspekten aufgezeigt, weshalb ich diese Auffassung nicht teile.[89]

Der Austausch mit den internationalen Informationsfreiheitsbeauftragten macht regelmäßig deutlich, wie wichtig es wäre, das 2005 verabschiedete IFG zu modernisieren. Ich empfehle, das Informationsfreiheitsgesetz zu einem Transparenzgesetz mit einem gesetzlich geregelten Transparenzregister weiterzuentwickeln. Mit diesen Anpassungen wäre das Informationsfreiheitsrecht des Bunds international betrachtet zumindest im Mittelfeld angesiedelt.

Schließlich haben meine Mitarbeitenden im Rahmen der geschlossenen Sitzung der Informationsfreiheitsbeauftragten am dritten Tag der Konferenz mit dem „Europa-Report“ den Überblick über die Aktivitäten der

88 Ranking des Center for Law and Democracy zum Infromationszugang, abrufbar unter: https://www.rti-rating.org/

89 Rede auf der ICIC 2024 in Tirana, Manuskript abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Reden_Gastbeitr%C3%A4ge/2024/ICIC-Troms%C3%B6-Convention.pdf

europäischen Kolleginnen und Kollegen in der ICIC aus dem vergangenen Jahr gegeben.

Gemeinsam mit meinen Kolleginnen und Kollegen haben wir eine öffentliche Erklärung verabschiedet. Diese trägt den Titel „Transparency and digital age: the information commissioner's role and citizen empowerment". [90]

In dieser Erklärung bekennen sie alle Mitglieder der ICIC zu neun Positionen, die den Zugang zu öffentlichen Informationen weltweit stärken sollen.

Ich empfehle die Zusammenlegung von Informationsfreiheitsgesetz und Umweltinformationsgesetz. Darüber hinaus empfehle ich die Weiterentwicklung zu einem Bundestransparenzgesetz mit proaktiven Veröffentlichungspflichten sowie Anordnungs- und Durchsetzungsbefugnisse für die Informationsfreiheitsbeauftragte, um im Konfliktfall handlungsfähig zu sein.

6.3 Erfahrungsaustausch

6.3.1 Zweiter Europäischer Case Handling Workshop zur Informationsfreiheit

Vom 6. bis 7. Mai 2024 fand der zweite Europäische Case Handling Workshop zur Informationsfreiheit in Madrid statt.

Nachdem ich 2023 erstmalig einen Europäischen Case Handling Workshop zur Informationsfreiheit im Europäischen Haus in Berlin veranstaltet hatte, konnte das Format im Jahr 2024 erfolgreich fortgesetzt werden. Vom 6. bis 7. Mai 2024 veranstaltete der spanische Rat für Transparenz und gute Regierungsführung in Madrid den zweiten Case Handling Workshop, an dem 30 Personen aus 13 europäischen Ländern und von der Europäischen Bürgerbeauftragten teilnahmen. Ziel des Workshops war es, eine Plattform für den europäischen Erfahrungsaustausch zu praktischen Anwendungsfragen des Informationsfreiheitsrechts zu schaffen. Der Austausch von bewährten Verfahrensweisen und Erkenntnissen aus der behördlichen Fallbearbeitung stellt aus meiner Sicht einen wichtigen Beitrag zur grenzübergreifenden Förderung von Transparenz dar.

Neben der Vorstellung verschiedener Fallgestaltungen aus der behördlichen Bearbeitungspraxis lag der thematische Fokus der Veranstaltung in diesem Jahr auf der proaktiven Veröffentlichung von Informationen auf Transparenzplattformen und dem Verhältnis von Informationsfreiheit zum Schutz personenbezogener Daten. Als Gastgeber für die Folgeveranstaltung im kommenden Jahr hat die Republik Kosovo Interesse geäußert. Aus meiner Sicht ist es wünschenswert, den Case Handling Workshop weiter zu entwickeln und als jährlich stattfindendes Format für den europaweiten Austausch auf Arbeitsebene zu etablieren. Mein Haus nimmt deshalb weiterhin die Aufgabe des Sekretariats wahr, um das Fortbestehen des Austauschs zu gewährleisten.

6.3.2 Erfahrungsaustausch der Bundesbehörden zur Informationsfreiheit

Sowohl der Erfahrungsaustausch mit den obersten Bundesbehörden als auch die neu hinzugekommene Veranstaltung mit verschiedenen Bundesoberbehörden und -anstalten in Bonn fanden im Berichtsjahr wieder an mehreren Terminen in Berlin und Bonn statt. Die Veranstaltungen stellen mittlerweile einen etablierten Bestandteil meines Beratungsangebots dar.

Beide Veranstaltungsreihen schaffen eine für alle Beteiligten wertvolle Möglichkeiten, sich über aktuelle Entwicklungen in der Rechtsprechung, deren konkrete Auswirkungen auf die praktische Arbeit und allgemeine Fragen der Bearbeitungspraxis auszutauschen. Über das große Interesse an diesem Beratungsangebot und die offene und engagierte Diskussion im Rahmen der beiden Veranstaltungen habe ich mich sehr gefreut.

Aufgrund der positiven Resonanz der Teilnehmenden beabsichtige ich, nicht nur diese beiden erfolgreichen Veranstaltungsformate fortzusetzen, sondern auch mein Angebot für weitere Behörden auszubauen.

Die beiden Austauschformate habe ich auch dazu genutzt, die beteiligten Behörden über meine Rolle in der Ombudstätigkeit sowie die Grundsätze, den Verfahrensablauf und die Grenzen des Vermittlungsverfahrens nach § 12 Abs. 1 IFG zu informieren. Ein besonderes Augenmerk lag dabei auf der Diskussion der Auswirkungen der Bestandskraft eines Bescheides nach dem IFG oder UIG auf das Vermittlungsverfahren. Dazu habe ich ausgeführt, dass auch eine etwaige Bestandskraft des Bescheides grundsätzlich nicht die im Verfahren nach § 12 Abs. 1 IFG maßgebliche Frage berührt, ob eine Verletzung von Rechten nach dem IFG oder UIG vorliegt. Ich habe darauf hingewiesen, dass zur Prüfung dieser

90 Gemeinsame Erklärung der ICIC 2024, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/ICIC/2024_06_05_ICIC-Public-Statement.pdf

Frage die Aufklärung des Sachverhalts notwendig ist und die Mitwirkung der informationspflichtigen Stelle damit weiterhin erforderlich bleibt. Ob und unter welchen Voraussetzungen ein rechtswidriger bestandskräftiger Bescheid dann geändert werden kann oder ob sonstige Maßnahmen von mir zu ergreifen sind, ist dann Gegenstand der weiteren Prüfung.

Ferner erfolgten ein Austausch und eine fachliche Diskussion zu dem Urteil des Bundesverwaltungsgerichts vom 20. März 2024, das sich zu Frage der Zulässigkeit anonymer bzw. pseudonymer Antragstellung äußerte.

6.4 Vermittlungsverfahren

6.4.1 Vertraulichkeit eines Fachgesprächs zwischen BVerfG und EGMR – zu den Grenzen des Vermittlungsverfahrens

Bei dem Vermittlungsverfahren mach § 12 Abs. 1 IFG handelt es sich um ein außergerichtliches Streitschlichtungsverfahren, bei dem in aller Regel einvernehmliche Lösungen angestrebt werden. Kann eine Rechtverletzung nach dem IFG nicht eindeutig festgestellt werden, bleibt eine abschließende Klärung der offengebliebenen Sach- und Rechtsfragen im Einzelfall dem förmlichen Rechtsbehelfsverfahren vorbehalten.

Ein Petent beantragte beim Bundesverfassungsgericht (BVerfG) verschiedene Unterlagen im Zusammenhang mit einem Fachgespräch zwischen Richterinnen und Richtern des BVerfG und einer Delegation des Europäischen Gerichtshofs für Menschenrechte (EGMR). Im Hinblick auf als antragsgegenständlich identifizierte Manuskripte, die in Vorbereitung der Veranstaltung an Dolmetscherinnen und Dolmetschern übermittelt worden waren, lehnte das BVerfG den Antrag ab. Zum einen stellten die Manuskripte als bloße Gedächtnisstütze zur Vorbereitung der Übersetzungstätigkeit keine amtlichen Informationen dar. Es handle sich vielmehr um Notizen im Sinne des § 2 Nr. 1 S. 2 IFG. Darüber hinaus sei der Informationszugang aufgrund der Vertraulichkeit der Fachgespräche ausgeschlossen. Dabei könne im Ergebnis offenbleiben, ob sich der Vertraulichkeitsschutz aus § 3 Nr. 3 lit. a) IFG (Vertraulichkeit internationaler Verhandlungen) oder § 3 Nr. 3 lit. b) IFG (Vertraulichkeit behördlicher Beratungen), einer entsprechenden Anwendung dieser Ausschlussgründe oder aus einer entsprechenden Anwendung des Grundsatzes des Kernbereichs exekutiver Eigenverantwortung ergebe. Abschließend handle es sich bei den Manuskripten um urheberrechtlich geschützte Werke, sodass dem Informationszugang gemäß § 6 S. 1 IFG der Schutz geistigen Eigentums entgegenstehe.

Der Petent vertrat in sämtlichen Punkten eine abweichende Rechtsauffassung und stellte diese ausführlich und für mich nachvollziehbar dar. Nach eingehender Prüfung der ausgetauschten Argumente teilte ich den Beteiligten mit, dass ich die rechtliche Auffassung des Petenten im Ergebnis für überzeugend halte. Gleichwohl ließen die im Vermittlungsverfahren aufgeworfenen Rechtsfragen, etwa bezüglich des Schutzes von besonderen öffentlichen Belangen, aufgrund ihrer Komplexität unterschiedliche Rechtsauffassungen zu.

Trotz meiner Vermittlungsbemühungen hielt das BVerfG abschließend an seiner rechtlichen Einschätzung fest. Unter Berücksichtigung der Grenzen des Verfahrens nach § 12 Abs. 1 IFG sah ich deshalb keine Möglichkeit, die Vermittlung zielführend fortzusetzen.

Bei dem Vermittlungsverfahren handelt es sich um ein außergerichtliches Streitschlichtungsverfahren. Mangels eigener Anordnungs- oder Durchsetzungsbefugnisse – wie sie beispielsweise im Bereich des Datenschutzes vorgesehen sind – ist das Verfahren vornehmlich auf einvernehmliche Lösungen ausgerichtet. Kann eine Rechtsverletzung nicht eindeutig festgestellt werden, weil die Vorgehensweise der um Informationszugang angegangenen Stelle aus tatsächlichen oder rechtlichen Gründen jedenfalls nicht unvertretbar erscheint, kann ein Vermittlungsverfahren in aller Regel nicht sinnvoll und zielführend fortgeführt werden. Jedenfalls in Fallkonstellationen, in denen das grundsätzliche „Ob“ der Anspruchsverpflichtung streitig ist, kommt eine einvernehmliche Lösung im Sinne eines gegenseitigen Nachgebens nicht in Betracht. Eine abschließende Beantwortung fortbestehender Rechtsfragen bleibt in diesen Fällen dem förmlichen Rechtsbehelfsverfahren, insbesondere der Prüfung im verwaltungsgerichtlichen Verfahren, vorbehalten.

Der Sachverhalt ist nun Gegenstand eines verwaltungsgerichtlichen Verfahrens.

6.4.2 Grenzen der behördlichen Informationsbeschaffungspflicht

Die Aufgabenwahrnehmung einer politischen Stiftung im Bereich der ideellen Begabtenförderung stellt keine Betrauung eines Privatrechtssubjekts mit der Erfüllung einer öffentlich-rechtlichen Aufgabe im Sinne des § 1 Abs. 1 S. 3 IFG dar. Allein die Zuwendung staatlicher Fördermittel führt nicht dazu, dass sich eine Behörde als Zuwendungsgeber die Begabtenförderung als gemeinwohlerhebliche Aufgabe zu eigen macht und sich der politischen Stiftung zur Erfüllung dieser Aufgabe bedient.

Ein Petent hatte gegenüber dem Bundesministerium für Bildung und Forschung (BMBF) auf Grundlage des IFG Zugang zu Informationen im Zusammenhang mit der Tätigkeit der Konrad-Adenauer-Stiftung (KAS) als Begabtenförderungswerk beantragt. Gegenstand der Anfrage waren unter anderem Auskünfte zu ideellen Förderprogrammen der KAS im Bereich der Begabtenförderung.

Die KAS ist als politische Stiftung in der Rechtsform eines Vereins eines von 13 Begabtenförderungswerken in Deutschland. Die Begabtenförderungswerke erhalten für ihre Handlungsfelder verschiedene Fördermittel des Bundes, soweit die haushaltsrechtlichen und spezifischen Fördervoraussetzungen und im Fall der politischen Stiftungen die Voraussetzungen des Gesetzes zur Finanzierung politischer Stiftungen aus dem Bundeshaushalt (Stiftungsfinanzierungsgesetz – StiftFinG) erfüllt sind. Das BMBF stellt den Begabtenförderungswerken hierbei Zuwendungen für die materielle und ideelle Förderung begabter Studierender und Promovierender im Inland zur Verfügung.

Das BMBF lehnte den Antrag ab und führte zur Begründung im Wesentlichen aus, dass die begehrten Informationen dort nicht vorliegen, oder erst zu einem späteren Zeitpunkt erhoben würden. Es bestehe auch keine Pflicht zu einer Informationsbeschaffung gemäß § 1 Abs. 1 S. 3 IFG i. V. m. § 7 Abs. 1 S. 2 IFG, da die Begabtenförderungswerke ihre eigenen satzungsgemäßen Aufgaben eigenständig wahrnehmen und nicht öffentliche-rechtliche Aufgaben des BMBF.

Der Petent wandte sich an mich und vertrat die Auffassung, die KAS nehme im Bereich der Begabtenförderung eine gemeinwohlerhebliche und deshalb öffentlich-rechtliche Aufgabe wahr. Das BMBF mache sich diese Aufgabe durch die Bereitstellung finanzieller Mittel zu eigen und bediene sich damit der KAS zur Erfüllung seiner öffentlich-rechtlichen Aufgaben.

Nach eingehender Prüfung der vorgebrachten Argumente war eine Verletzung von Rechten nach dem IFG für mich nicht feststellbar. Parteinahe Stiftungen politischer Parteien unterfallen als privatrechtlich verfasste Organisationen, ungeachtet einer Finanzierung aus öffentlichen Mitteln, grundsätzlich nicht der unmittelbaren Informationspflicht nach dem IFG. Gemäß § 1 Abs. 1 S. 3 IFG steht eine natürliche oder juristische Person des Privatrechts einer informationspflichtigen Behörde zwar gleich, soweit sich die Behörde dieser Person zur „Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient“. Anspruchsgegner ist gemäß § 7 Abs. 1 S. 2 IFG jedoch die sachlich zuständige Behörde, deren Aufgaben von dem Privatrechtssubjekt ausgeführt werden. In diesem Fall trifft die um Informationszugang angegangene Behörde überzeugender Weise eine Informationsbeschaffungspflicht. Anderenfalls liefe der Anspruch auf Informationszugang mangels Identität der formell anspruchsverpflichteten Behörde und des materiell informationspflichtigen Dritten ins Leere.

Im konkreten Fall lagen die tatbestandlichen Voraussetzungen des § 1 Abs. 1 S. 3 IFG nach meiner Einschätzung jedoch nicht vor. Zwar ist der Begriff der „öffentlich-rechtlichen Aufgabe“ im Sinne des § 1 Abs. 1 S. 3 IFG weit auszulegen. Ausreichend ist, dass es sich um die Wahrnehmung einer im öffentlichen Recht wurzelnden Verwaltungsaufgabe handelt. Eine Beschränkung auf den Bereich der Daseinsvorsorge kann aus dem Gesetz nicht abgeleitet werden. Vieles spricht deshalb auch nach meiner Einschätzung dafür, dass es sich bei der Begabtenförderung jedenfalls um eine gemeinwohlerhebliche Aufgabe im öffentlichen Interesse handelt.

Allein die Zuwendung staatlicher Fördermittel führt im konkreten Fall jedoch nicht dazu, dass sich das BMBF diese gemeinwohlerhebliche Aufgabe zu eigen macht („ihrer Aufgabe“) und sich zu ihrer Erfüllung der KAS „bedient“. Die KAS nimmt ihre Aufgaben als Begabtenförderungswerk unabhängig und autonom wahr. Insbesondere im ideellen Förderungsbereich kommt ihr eine Gestaltungsfreiheit zu. Gestützt wird die Annahme einer autonomen Aufgabenwahrnehmung auch durch die zuwendungsrechtliche Ausgestaltung der Finanzierung der Begabtenförderungswerke. Anders als etwa im Rahmen öffentlicher Aufträge oder anderer „klassischer Kooperationsformen“, die weiterhin eine gewisse Leitungs- und Kontrollverantwortung des Staates erkennen lassen, kommt der Behörde als Zuwendungsgeber regelmäßig ein rechtlicher, nicht aber ein fachlich-steuernder Einfluss zu. Zwar setzt eine staatliche Zuwendung nach haushaltsrechtlichen Regelungen und dem StiftFinG stets ein erhebliches Bundesinteresse an der Förderung voraus. Die Annahme, allein dies erfülle den Tatbestand des § 1 Abs. 1 S. 3 IFG, stellt nach meiner Einschätzung aber eine zu weitgehende Ausdehnung der Vorschrift dar. Es bedarf weiterer Anhaltspunkte, die die juristische Person des Privatrechts zu einem Kooperationspartner und damit quasi-staatlichen Träger öffentlicher Belange machen.

Grundsätzlich zugänglich bleiben die amtlichen Informationen, die sich auf den Zuwendungsvorgang als solchen beziehen. Dies ist jedoch kein Fall des § 1 Abs. 1 S. 3 IFG, sondern der behördlichen Anspruchsverpflichtung nach § 1 Abs. 1 S. 1 IFG.

6.4.3 Die Einstufung eines Dokuments erfasst nicht die gesamte Akte

Die Einstufung eines einzelnen Dokuments oder mehrerer Dokumente in einer Akte als Verschlusssache hat keine unmittelbaren Auswirkungen auf die sonstigen Aktenbestandteile.

Ein Petent hatte bei dem Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) gestützt auf das IFG Zugang zu dem vollständigen Akteninhalt des BMZ zu einem vom Weltfriedensdienst durchgeführten Projekt beantragt, insbesondere zu bestimmten konkret benannten Informationen. Das BMZ gewährte Informationszugang zu bestimmten allgemeinen Informationen, z. B. den rechtlichen Grundlagen der Tätigkeit des BMZ, und lehnte den Antrag im Übrigen ab. Alle in der betreffenden Akte befindlichen Dokumente seien als VS-NfD eingestuft, was dem Informationszugang entgegenstehe.

Der Petent wandte sich an mich und bezweifelte die Rechtmäßigkeit der Einstufung aller Dokumente in der Akte als Verschlusssache. Er sei davon überzeugt, dass die Akte des BMZ, auf die sich der Antrag bezog, nicht ausschließlich Inhalte bzw. Dokumente umfasste, die als VS-NfD eingestuft und auf jeder Seite entsprechend gekennzeichnet worden seien. Außerdem seien die materiellen Einstufungsgründe nicht ausreichend dargelegt.

Im Vermittlungsverfahren substantiierte das BMZ zunächst die materiellen Gründe, die die Einstufungsbedürftigkeit rechtfertigten. Die befürchteten Nachteile für die Interessen der Bundesrepublik Deutschland konnte ich nachvollziehen. Ich hatte jedoch weiterhin Zweifel, dass jedes Dokument in dem betroffenen Vorgang materiell einstufungsbedürftig war. Hierzu hielt das BMZ unter Hinweis auf § 20 Abs. 6 Verschlusssachenanweisung (VSA) an seiner Rechtsauffassung fest. Eine Verschlusssache sei in ihrer Gesamtheit nach dem höchsten Geheimhaltungsgrad zu kennzeichnen, wenn die Verschlusssache aus mehreren, unterschiedlich eingestuften Teilen bestehe.

Ich wies das BMZ darauf hin, dass dieses Verständnis weder der hiesigen Auslegung der VSA noch der aus Beratungs- und Kontrollbesuchen gewonnenen Erfahrungen zur Praxis in anderen Häusern entsprach. Der Begriff der Verschlusssache sei nicht aktenbezogen, sondern dokumentenbezogen zu verstehen. Selbst bei einem anderen Verständnis habe die in § 20 Abs. 6 VSA geregelte Kennzeichnungspflicht bei unterschiedlicher Einstufung verschiedener Teile einer Verschlusssache lediglich eine Warnfunktion. Sie begründe aber keine Einstufung der anderen Aktenteile. Mit anderen Worten folge die Kennzeichnung lediglich der (höchsten) Einstufung, sie habe aber keine konstituierende Einstufungswirkung. Einzelne abgrenzbare Teile der Akte könnten in der Konsequenz eben auch „nicht eingestuft“ sein. Ob sich eine materielle Einstufungsbedürftigkeit bisher nicht formell eingestufter Einzeldokumente aus einem engen Sachzusammenhang ergibt, der seinerseits Rückschlüsse auf schutzwürdige Tatsachen zulässt, müsse vielmehr im Einzelfall geprüft werden.

Das BMZ hat sich nach nochmaliger Prüfung diesen Ausführungen angeschlossen und alle Einzeldokumente auf ihre materielle Einstufungsbedürftigkeit überprüft. Soweit die Dokumente nicht einstufungsbedürftig waren, konnte der Informationszugang gewährt werden.

6.5 Beratungs- und Kontrollbesuche

6.5.1 Beratungs- und Kontrollbesuch beim Bundespolizeipräsidium

Mitte Mai 2024 führte ich einen Beratungs- und Kontrollbesuch bei dem Bundespolizeipräsidium (BPOLP) in Potsdam durch. Gegenstand des Besuchs war die Bearbeitung von Anträgen nach dem Informationsfreiheitsgesetz (IFG) und dem Umweltinformationsgesetz (UIG).

Die Überprüfung der Bearbeitungspraxis des BPOLP bei Anträgen nach dem IFG und UIG erfolgte auf Grundlage der Auswertung von etwa der Hälfte der Verfahrensakten aus den Jahren 2019 bis 2023. Als wesentliches Ergebnis des Beratungs- und Kontrollbesuchs ist festzustellen, dass die Anwendung des IFG und UIG weitestgehend bürger- und serviceorientiert erfolgt und die Verfahrensvorschriften sowie die materiell-rechtlichen Vorgaben dieser Gesetze im Wesentlichen beachtet werden.

Die Bearbeitung von Anträgen auf Informationszugang bei dem BPOLP und bei direktionsübergreifenden Anfragen wird unter Beteiligung der Fachreferate zentral von dem Referat 71 durchgeführt. Aufgrund dieser zentralen Bearbeitung wird eine konsistente und bis auf Ausnahmen widerspruchsfreie Bearbeitung der an das BPOLP gerichteten Anträge gewährleistet. Mit einer Organisationsverfügung zu der Verfahrensweise bei Anträgen nach dem IFG hat das BPOLP seine nachgeordneten Behörden, die ihm unterstehenden Bundespolizeidirektionen und Bundespolizeiakademie, angewiesen, alle dort eingehenden Anträge vorzulegen, um eine Koordinierung und einheitliche Bearbeitung in Fällen grundsätzlicher Bedeutung sicherzustellen. Da es sich bei den in § 57 Abs. 1 BPolG genannten Bundespolizeibehörden um jeweils eigenständige Behörden im Sinne von § 1 Abs. 4

VwVfG handelt, habe ich angeregt, diese Vorgehensweise vorab abzuklären.

In einigen Einzelfällen haben meine Mitarbeitenden eine fehlerhafte Abgrenzung einer nicht von dem Anspruch nach dem IFG umfassten Informationsbeschaffung von einer bloßen Informationsaufbereitung festgestellt. Zwar richtet sich der Informationszugangsanspruch nach dem IFG grundsätzlich nur auf die bei der informationspflichtigen Stelle vorhandenen Informationen. Dies schließt jedoch nicht aus, dass eine Pflicht zur Informationsaufbereitung besteht. Allerdings ist eine Neukontextualisierung, die zu einem zusätzlichen Informationsgehalt führt bzw. eine neue Information generiert, nach dem IFG nicht geschuldet. Der Informationszugangsanspruch umfasst aber die bloße Zusammenstellung oder einfache Addition gleichartiger Informationen. Diese Abgrenzung ist auch unabhängig von dem hierdurch verursachten Verwaltungsaufwand zu beurteilen.

Auch zu der Tenorierung von Bescheiden, dem Drittbeteiligungsverfahren und der Gebührenprognose haben meine Mitarbeitenden Hinweise und Anregungen gegeben.

6.5.2 Beratungs- und Kontrollbesuch im BMVg

Im März 2024 führte ich einen Beratungs- und Kontrollbesuch beim Bundesministerium der Verteidigung (BMVg) durch. Dort ist insgesamt eine offene und positive Grundhaltung gegenüber der Informationsfreiheit zu erkennen.

Aufgrund der großen Zahl an IFG-Anträgen haben meine Mitarbeitenden bei einem Beratungs- und Kontrollbesuch eine Stichprobe der Verfahren aus den Jahren 2019 bis 2023 überprüft.

Die Anwendung des IFG und UIG im BMVg erfolgt nach den Feststellungen meiner Mitarbeitenden bürger- und serviceorientiert und die Verfahrensvorschriften sowie die materiell-rechtlichen Vorgaben des IFG bzw. UIG werden im Wesentlichen beachtet.

Die Bearbeitung einschließlich der Beantwortung bzw. Bescheidung von IFG-Anträgen und die Beteiligung der Fachreferate erfolgt zentral bei einem Referat der Abteilung Recht und Organisation in Berlin. Die Bearbeitung von Anträgen nach dem UIG erfolgt aufgrund der größeren Sachnähe davon getrennt bei einem Referat der Abteilung Infrastruktur, Umweltschutz und Dienstleistungen in Bonn. Aufgrund der zentralisierten Bearbeitung wird eine konsistente und bis auf Ausnahmen widerspruchsfreie Bearbeitung der IFG- und UIG-Anträge gewährleistet. Die Fachreferate arbeiten weitestgehend zielgerichtet und kooperativ zu. Somit werden die Voraussetzungen für eine zügige Bearbeitung der IFG- und UIG-Anträge geschaffen. In dem Prüfungszeitraum kam es bei der Bearbeitung der Anträge phasenweise zu Fristüberschreitungen.

In der Tenorierung wie auch Begründungsdichte der Bescheide war bisweilen ein heterogenes Bild festzustellen. Die Durchführung der Drittbeteiligungsverfahren konnte nur teilweise überprüft werden, da diese dezentralisiert von den Fachreferaten durchgeführt worden sind und weitgehend nicht vollständig in den zur Verfügung gestellten Akten enthalten waren. Soweit die Drittbeteiligungsverfahren überprüft werden konnten, waren die entsprechenden Schreiben gelegentlich eher pauschal gehalten, in anderen Fällen war hingegen eine hohe Qualität zu erkennen. Zu dem festgestellten Verbesserungsbedarf bei der Tenorierung und Begründung der Bescheide sowie bei der Durchführung von Drittbeteiligungsverfahren habe ich verschiedene konkrete Hinweise und Anregungen gegeben.

7 Einzelthemen

7.1 Gesundheit

7.1.1 Authentifizierungsmöglichkeiten der gesetzlich Versicherten

Zu den Anforderungen an die Authentifizierung im Gesundheitswesen, diesbezüglichen Neuerungen und worauf Krankenkassen jetzt achten müssen.

Wenn Versicherte über die elektronische Patientenakte (ePA) auf ihre Gesundheitsdaten zugreifen möchten, müssen sie sich zunächst authentifizieren. Bei der Authentifizierung wird geprüft, ob diejenige Person, die zugreifen möchte, wirklich diejenige Person ist, die sie vorgibt zu sein. Die Pflicht zur Durchführung einer Authentifizierung ergibt sich aus Art. 32 DSGVO und trifft die Krankenkassen als Anbieter der ePA. Authentifizierungsverfahren werden abhängig von ihrer Sicherheit in drei Stufen eingeteilt, beginnend mit dem Vertrauensniveau „normal“, über „substantiell“ bis hin zu „hoch“. Gesundheitsdaten sind nach Art. 9 DSGVO als sensible Daten besonders schutzwürdig. Es spricht daher einiges dafür, das höchste Maß an Vertrauen in einen verfügbaren Authentifizierungsprozess für den Zugriff auf diese Daten vorauszusetzen.

Authentifizierungsverfahren, die ein hohes Vertrauensniveau gewährleisten, sind der elektronische Personalausweis (eID), die elektronische Gesundheitskarte (eGK) sowie die GesundheitsID (vom Gesetzgeber als „Digitale Identität“ bezeichnet), jeweils zusammen mit der zugehörigen persönlichen Identifikationsnummer (PIN). Trotz der vorhandenen sicheren Authentifizierungsverfahren werden nun zusätzlich auch weniger sichere Authentifizierungsverfahren eingeführt. Auf das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG), das das rechtliche Fundament dafür legt, bin ich in meinem 32. Tätigkeitsbericht bereits eingegangen.[91]

Aufbauend auf dem DigiG hat die Gesellschaft für Telematik (gematik) neue Spezifikationen erarbeitet, nach denen bei der GesundheitsID anstelle der PIN die Biometriefunktion des mobilen Endgeräts genutzt werden kann.[92] Nach Untersuchungen des Bundesamts für Sicherheit in der Informationstechnik im Jahr 2022 erreichten die Biometriefunktionen der am Markt erhältlichen mobilen Endgeräte nicht das Vertrauensniveau „hoch“, sondern bestenfalls das Vertrauensniveau „substantiell“, meist jedoch nur das Vertrauensniveau „normal“.[93] Die biometrische Authentifizierung mit Vertrauensniveau „normal“ lässt sich mit einfachsten Mitteln überwinden, etwa mit einem Foto der betroffenen Person oder einem von einem Glas abgenommenen Fingerabdruck. Die gematik hat diese neue Spezifikation trotz der von mir dargelegten datenschutzrechtlichen Herausforderungen verabschiedet.

Ob das Problem einer Authentifizierung mittels Face-ID oder Fingerprint (beiden Mechanismen weisen ein geringeres Schutzniveau auf als der PIN) dadurch gelöst werden kann, dass – wie im DigiG und den gematik-Spezifikationen vorgesehen – bei Versicherten eine Einwilligung in das weniger sichere Authentifizierungsverfahren eingeholt wird, ist streitig Das Sozialgericht Hamburg[94] und das OLG Düsseldorf[95] nehmen eine Abdingbarkeit des § 32 DSGVO, d. h. die Möglichkeit, mittels Einwilligung das Schutzniveau der Authentifizierung

91 32. TB Nr. 3.1.3

92 Siehe die gematik-Spezifikation gemSpec_IDP_Sek_V2.5.0 (Stand 16. August 2024), Anforderung A_23701, abrufbar unter https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_Sek/gemSpec_IDP_Sek_V2.5.0/

93 Siehe die BSI, Bewertung von Authentisierungslösungen gemäß TR-03107 in Version 1.1.1, Anwendungs- und Vorgehensbeschreibung, Version 1.06 vom 5. Oktober 2022, Gliederungspunkt 4.4.1, Seiten 34 f., abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1_Anforderungen.pdf?__blob=publicationFile&v=4

94 Urteil des SG Hamburg vom 30. Juni 2023, Az.: S 39 AS 517/23

95 Urteil des OLG Düsseldorf vom 28. Oktober 2021, Az.: 16 U 275/20

herabzusenken, an. Die wohl überwiegende Meinung in der Literatur lehnt eine vollständige Abdingbarkeit ab, nimmt aber zum Teil ebenfalls an, zumindest die konkreten Mittel oblägen der Disponibilität des Betroffenen[96] (statt vieler: Jandt in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 32 Rn. 39 m. w. Nachw.). Der Beschluss der 102. Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK) vom 24. November 2021 sieht Ausnahmen nur für eng umgrenzte und zu dokumentierende Einzelfälle vor.[97]

Bei unbesehener Umsetzung der gematik-Spezifikationen laufen die Krankenkassen Gefahr, gegen die DSGVO zu verstoßen. Die meiner Aufsicht unterliegenden Krankenkassen habe ich deshalb am 6. Mai 2024 entsprechend gewarnt. In der Warnung habe ich deutlich gemacht, dass Krankenkassen gegen Art. 32 DSGVO verstoßen könnten, wenn sie bei der ePA einen Zugriff auf Gesundheitsdaten zulassen, ohne dass eine Authentifizierung mit höchstmöglichem Vertrauensniveau stattgefunden hat oder ausnahmsweise ein zu dokumentierender Einzelfall nach dem genannten DSK-Beschluss vorliegt.

Weiter habe ich zur Sensibilisierung und Aufklärung der Öffentlichkeit auf meinem Internetauftritt einen Beitrag zu Authentifizierungsverfahren im digitalen Gesundheitswesen erstellt.[98] Darin gehe ich auf die häufigsten in diesem Zusammenhang gestellten Fragen ein und erläuterte, wieso aus Datenschutzsichtsicht bei Gesundheitsdaten eine biometrische Authentifizierung problematisch sein kann.

7.1.2 Entwicklung der medizinischen Registerlandschaft

Die Ausgestaltung medizinischer Register zeigte auch in diesem Berichtsjahr eine dynamische Entwicklung. Das Implantateregister (IRD) nahm im Juli 2024 seinen Vollbetrieb für Brustimplantate auf. Außerdem wird derzeit eine einheitliche Rechtsgrundlage für alle medizinische Register geschaffen, um zum einen eine Harmonisierung rechtlicher Vorgaben zu erreichen und zum anderen medizinische Forschung stark voranzutreiben.

Bereits im Jahr 2023 hatte das IRD den Probebetrieb mit ersten Echtdaten aufgenommen. Hierbei hatte ich das nötige Einvernehmen zum Pseudonymisierungsverfahren und zur Verschlüsselungstechnik erteilt und zu verschiedenen Einzelfragen beraten. Diese Konzepte sind nun auch die Grundlage für den Regelbetrieb. Ein besonderer Schwerpunkt lag in diesem Berichtsjahr darauf, wie man die Daten der gesetzlichen Krankenkassen, der privaten Krankenversicherung und der Träger freier Heilführsorge im IRD zusammenführen kann, ohne dass das Datenschutzrecht der Betroffenen verletzt wird. Nachdem das IRD nun zum 1. Juli 2024 seinen Vollbetrieb zunächst planmäßig für Brustimplantate aufgenommen hat, soll dieser zum 1. Januar 2025 auf Endoprothesen für Hüfte und Knie sowie auf Aortenklappen-Implantate erstreckt werden. Die Zweite Verordnung zur Änderung der Implantateregister-Betriebsverordnung vom 21. Oktober 2024 schaffte hierfür die erforderliche rechtliche Grundlage. Problematisch bleibt nach wie vor, dass die Registerstelle noch immer provisorisch bei einer Projektgruppe unmittelbar im Bundesministerium für Gesundheit (BMG) selbst angesiedelt ist. Somit bleibt die Empfehlung einer unabhängigen Registerstelle weiterhin bestehen.

Einen erfreulichen rechtlichen Fortschritt im Registerwesen bildet der Referentenentwurf des BMG für ein Gesetz zur Stärkung medizinischer Register und Verbesserung der Registerdatennutzung (Registerstärkungsgesetz) vom 9. Oktober 2024.

Das Registerstärkungsgesetz dient der Schaffung einer nachhaltigen, hochwertigen medizinischen Registerinfrastruktur. In Deutschland existieren derzeit ca. 400 medizinische Register. Nur sehr wenige dieser Register arbeiten auf der Basis spezieller gesetzlicher Grundlagen wie etwa die landesrechtlichen Krebsregister oder das Implantateregister. Die meisten medizinischen Register erheben daher personenbezogene Daten auf Basis der allgemeinen datenschutzrechtlichen Rechtsgrundlagen und bewegen sich dadurch in einem heterogenen Normengeflecht von EU-, Bundes- und Landesrecht. Zudem ist die Nutzbarkeit von Registern dadurch eingeschränkt, dass viele Nutzungszwecke eine repräsentative oder möglichst vollzählige Datenbasis voraussetzen, was derzeit nicht gewährleistet ist. Durch das Gesundheitsdatennutzungsgesetz und das Gesetz zur Beschleunigung der Digitalisierung im Gesundheitswesen wurden zur besseren Nutzung von Gesundheitsdaten auf nationaler Ebene bereits wichtige Schritte eingeleitet. Flankiert werden diese durch die Verordnung zum Europäischen Gesundheitsdatenraum. Der Entwurf eines Registerstärkungsge-

96 Statt vieler: Jandt in: Kühling/Buchner, DSGVO/BDSG, 4. Auflage 2024, Art. 32 Rn. 39 mit weiteren Nachweisen

97 Beschluss der 102. DSK vom 24. November 2021 zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/102DSK_Nichtanwendung-TOM.pdf?__blob=publicationFile&v=3.

98 Beitrag zu Authentifizierungsverfahren im digitalen Gesundheitswesen, abrufbar unter https://www.bfdi.bund.de/DE/Buerger/Inhalte/GesundheitSoziales/eHealth/Authentifizierungsverfahren_dig_Gesundheitswesen.html

setzes ergänzt durch einen einheitlichen Rechtsrahmen für sämtliche Register das Etablieren von rechtlichen und technischen Standards sowie das Vorantreiben von Forschung durch das Zusammenführen einer Vielzahl von Daten die bestehenden Rechtsgrundlagen.

Ich begrüße daher grundsätzlich die Schaffung einer einheitlichen rechtlichen Regelung, auch wenn noch an einigen Punkten datenschutzrechtliche Stellschrauben nachjustiert werden müssen. Dazu habe ich den Gesetzgeber noch einmal auf die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22./23. November 2023 zu den Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register hingewiesen [99]. Aufgrund der vorzeitigen Auflösung des 20. Deutschen Bundestages wurde dieses Gesetzgebungsverfahren leider nicht zum Abschluss gebracht. Ich rufe dazu auf, das Vorhaben in der 21. Wahlperiode erneut anzustoßen.

Die dynamische Entwicklung des Registerwesens im Gesundheitsbereich werde ich weiterhin konstruktiv begleiten. Dabei haben die Förderung der Forschung, die Qualitätssicherung der Arbeitsweisen der Registerstellen sowie der Schutz hoch sensibler personenbezogener Gesundheitsdaten hohe Priorität. Diese Ziele fördern sich gegenseitig. Die Zusammenarbeit mit den Register- und Vertrauensstellen sowie dem Gesetzgeber ist von diesem Ziel stets geprägt.

7.1.3 Ausgewählte Entscheidungen im Bereich Gesundheit

Einige meiner Entscheidungen nach Art. 58 Abs. 2 DSGVO betreffen Fragen von allgemeinem Interesse. In diesem Berichtsjahr befasste ich mich unter anderem mit den Anforderungen an den E-Mail-Versand von Gesundheitsdaten sowie der Verpflichtung, Software vorab zu testen.

E-Mail-Versand von Gesundheitsdaten

Weil eine öffentliche Stelle eine Buchungsbestätigung für Arzttermine, die den Namen der Ärzte enthielten, ohne Ende-zu-Ende-Verschlüsselung per E-Mail verschickt hat, hat mein Haus diese verwarnt.

Nach Art. 32 DSGVO haben Verantwortliche technisch-organisatorische Maßnahmen (TOM) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu gehört nach Art. 32 Abs. 1 lit. a) DSGVO auch die Verschlüsselung. Werden E-Mail-Nachrichten versendet, bei denen die unbefugte Offenbarung der enthaltenen personenbezogenen Daten ein hohes Risiko darstellt, bedarf es einer Ende-zu-Ende-Verschlüsselung. [100] Dies gilt insbesondere für Gesundheitsdaten i. S. v. Art. 4 Nr. 15 DSGVO. Diese sind besonders sensibel und schützenswert. Im Zusammenhang mit ihrer Verarbeitung können erhebliche Risiken auftreten. [101] Gesundheitsdaten liegen bereits dann vor, wenn aus den betreffenden Daten auf den Gesundheitszustand einer Person geschlossen werden kann. [102] Hierunter fällt auch die Information, dass eine Person einen Termin bei einem bestimmten Arzt gebucht hat. Hieraus kann gefolgert werden, dass bei der den Termin buchenden Person ein Behandlungsbedarf gegeben ist. Weiter kann durch Recherche des Arztes, auf welchem Fachgebiet dieser tätig ist, eingegrenzt werden, um was für eine Art von Krankheit es sich handeln kann. Eine unbefugte Offenbarung dieser Informationen kann für betroffene Personen zu Stigmatisierungen führen, etwa wenn bekannt wird, dass eine Person einen Termin bei einem Facharzt für Psychiatrie und Psychotherapie gebucht hat.

Mit der Entscheidung, eine Verwarnung auszusprechen, liegt mein Haus auf einer Linie mit der schwedischen Aufsichtsbehörde, die in einem vergleichbaren Fall, bei dem eine E-Mail mit Gesundheitsdaten ohne Ende-zu-Ende-Verschlüsselung versendet wurde, ebenfalls eine Verwarnung ausgesprochen hat. [103] In unserem Fall zeigte sich die verantwortliche Stelle einsichtig und hat ihre Prozesse zwischenzeitlich angepasst. Die Terminbestätigungen enthalten jetzt keine Angaben mehr dazu, bei wem der Termin gebucht wurde.

Verpflichtung, Software vorab zu testen

In einem weiteren Fall habe ich eine öffentliche Stelle verwarnt, weil diese eine neue Version ihrer Smartphone-App mit erstmals eingebautem Software Development Kit (SDK) einer Drittanbieterin über die App Stores bereitgestellt hat, ohne vorab durch Tests zu prüfen bzw.

---

99 Siehe hierzu die Entschließung der DSK vom 23. November 2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_medRegister.pdf

100 DSK-Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ vom 27. Mai 2021, Gliederungspunkt 4.2.2., abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf

101 Erwägungsgründe 51 und 75 DSGVO.

102 EuGH, Urteil vom 4. Oktober 2024, Az. C-21/23, Rn. 83, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62023CJ0021

103 Finale Entscheidung des Europäischen Datenschutzausschusses: EDPBI:SE:OSS:D:2023:652, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions/decision-no-652_en

überprüfen zu lassen, dass es nicht zu unbeabsichtigten Datenverarbeitungen kommt.

Nach Art. 32 DSGVO haben Verantwortliche TOMs zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu gehören nach Art. 32 Abs. 1 lit. b) DSGVO auch TOMs zur Sicherstellung der Vertraulichkeit der Systeme und Dienste. Risiken für die Vertraulichkeit bestehen besonders bei Software, die Daten über das Internet übertragen kann. Verantwortliche müssen deshalb durch TOMs sicherstellen, dass die Software entsprechend getestet wird, damit es nicht zu unbeabsichtigten Datenübertragungen kommt. Allgemeine Empfehlungen zu Software-Tests enthält das vom BSI herausgegebene IT-Grundschutz-Kompendium. Im Hinblick auf Software-Tests ist danach vorgesehen, dass diese nicht nur bei der erstmaligen Inbetriebnahme, sondern jedenfalls auch bei wesentlichen Änderungen der Software durchgeführt werden. Eine wesentliche Änderung ist der erstmalige Einbau eines SDKs einer Drittanbieterin. Einerseits können SDKs die Anwendungsentwicklung erleichtern, wenn auf fremden, bereits vorhandenen Programmcode zurückgegriffen werden kann. Andererseits kann dieser fremde Programmcode Gefahren bergen. So können sich darin ungewollte Funktionalitäten verbergen, mit denen die SDK-Herstellerin personenbezogene Daten an sich selbst überträgt.

In dem entschiedenen Fall wäre es Sache der Verantwortlichen gewesen, durch Tests zu überprüfen oder überprüfen zu lassen, dass es durch den SDK-Einbau zu keinen ungewollten Datenübertragungen kommt. Nachdem die Verantwortliche ihren diesbezüglichen Pflichten nicht nachgekommen ist, habe ich sie entsprechend verwarnt. Die Verantwortliche hat sich einsichtig gezeigt und wird dafür Sorge tragen, dass Apps künftig vor der Zurverfügungstellung an die Nutzenden getestet werden.

7.1.4 Modellvorhaben Genomsequenzierung

Das Modellvorhaben zur umfassenden Diagnostik und Therapiefindung mittels Genomsequenzierung bei seltenen und onkologischen Erkrankungen nach § 64e SGB V ist in diesem Berichtsjahr gestartet. Das nötige Einvernehmen für die Ausgestaltung der Einwilligungserklärung zur Nutzung der Patientendaten zu Forschungszwecken habe ich im August 2024 erteilt.

Die Genomsequenzierung stellt eine vielversprechende medizinische Methode zur Diagnostik und effektiven Therapiefindung insbesondere für seltene und onkologische Erkrankungen dar. Aus diesem Grund soll langfristig die Gendiagnostik als Regelversorgung für alle Patientinnen und Patienten zur Verfügung stehen. Im Rahmen eines Modellvorhabens wird die Durchführung dieser Diagnostik als Kassenleistung zunächst für den begrenzten Zeitraum von fünf Jahren erprobt. Es handelt sich für die infrage kommenden Versicherten um ein freiwilliges, von den Krankenkassen finanziertes Verfahren.

Da genetische Daten sehr sensible Daten im Sinne der DSGVO sind, muss der datenschutzrechtliche Rahmen dieses Modellvorhabens solide sein. Zur Durchführung der für das Modellvorhaben relevanten Genomsequenzierung stellt § 64e Abs. 15 SGB V klar, dass die Vorschriften des Gendiagnostikgesetzes (GenDG), insbesondere zu Aufklärung, Einwilligung und Mitteilung der Ergebnisse genetischer Untersuchungen und Analysen unberührt bleiben. Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) hat als zuständige Behörde eine Teilnahmeerklärung mit Informationen über die Genomsequenzierung sowie zur Einwilligung in die Teilnahme am Modellvorhaben für die Patientinnen und Patienten formuliert. Ich war in die Ausgestaltung der Teilnahme- und Einwilligungserklärungen sowie der Handreichung für das medizinische Personal eingebunden.

Für die weitere Nutzung der Patientendaten in der Forschung ist eine zusätzliche Einwilligung erforderlich. Die Ausgestaltung der Einwilligungserklärung muss gemäß § 64e Abs. 6 S. 5 SGB V mit meinem Einvernehmen erfolgen.

Das BfArM hat zu diesem Zweck die Verwendung der Mustereinwilligung der Medizin-Informatik-Initiative (MII-Broad-Consent)[104] in der Version 1.6d oder aktueller vorgesehen. Über die Zulässigkeit der Verwendung dieses Broad Consents im konkreten Fall des Modellvorhabens habe ich mich intensiv mit dem BfArM ausgetauscht. Insbesondere musste sichergestellt sein, dass die Nutzung des MII-Broad-Consents mit den maßgeblichen normativen Vorgaben vereinbar ist. Denn hier reguliert das Gesetz ein Antragsverfahren, das in der Kontrolle des BfArM liegt. Nur Nutzungsberechtigte, die dieses Antragsverfahren durchlaufen haben, sind zur Verarbeitung der Daten zum Zwecke der wissenschaftlichen Forschung befugt. Im Rahmen des Dialogs mit dem BfArM wurde deutlich, dass die Umsetzung dieses gesetzlich vorgegebenen Antragsverfahrens, die damit verbundene Zulassung der Datennutzung sowie

104 Siehe hierzu auch den Beschluss der DSK vom 15. April 2020, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20200427_Beschluss_MII.pdf

die Kontrolle durch das BfArM auch unter Verwendung des MII-Broad-Consents vorgesehen ist. Die Leistungserbringer – vor allem Unikliniken aus einer Reihe von Bundesländern – hinterlegen die erhobenen klinischen und genomischen Daten in einer Datenplattform, die vom BfArM als Plattformträger betrieben wird. Über ein Portal können antragstellende Forschungseinrichtungen Nutzungsanträge beim BfArM einreichen. Nach erfolgreicher Überprüfung der Anträge werden die Daten aus der Datenplattform und Analyse-Ergebnisse, die aufgrund der vernetzten Analyse aller Daten in der Datenplattform generiert werden, an die Nutzungsberechtigten für weitere Forschungszwecke zur Verfügung gestellt. Mit diesem Verfahren werden einerseits die in § 64e SGB V regulierten Anforderungen erfüllt und zugleich die aus Forschungsperspektive sehr wertvollen Genomdaten sowie die Analysedaten für die wissenschaftliche Forschung zugänglich gemacht.

7.2 Inneres und Justiz

7.2.1 Registermodernisierung

Bei der Registermodernisierung begannen die Beteiligten im Berichtsjahr verstärkt an der Umsetzung des Once-Only-Prinzips zu arbeiten. Dabei sind nicht nur neue technische, sondern zugleich datenschutzrechtliche Herausforderungen entstanden. Grundsätzliche Erwägungen zur Verbreitung der Identifikationsnummer und der Gewährung der Transparenz sind noch offen.

Auch 2024 spielte die Begleitung der Registermodernisierung eine große Rolle in meiner Tätigkeit. Die Vorzeichen sind dabei unverändert, wobei sie zunehmend auch in der Öffentlichkeit als eines der größten Digitalisierungsprojekte Deutschlands wahrgenommen wird. Die grundsätzliche datenschutzrechtliche Bewertung ist dabei weiterhin differenziert.[105] Zwar ist mit der Abkehr vom Direkterhebungsgrundsatz hin zum Once-Only-Prinzip ein erhöhter Eingriff in das Recht auf informationelle Selbstbestimmung verbunden, allerdings lässt sich dieser mit neuartigen Maßnahmen zu Gunsten von Transparenz, Kontrolle sowie einer Hemmung der Zusammenführbarkeit durchaus ausgleichen. Gleichzeitig stellt die Entscheidung, die Steuer-Identifikationsnummer (Steuer-ID) als allgemeine Identifikationsnummer (IDNr) zu verwenden, immer noch eine erhebliche verfassungsrechtliche Hürde dar, da ein einheitlicher, bereichsübergreifender Identifikator eine in jede Richtung wirksame Zusammenführbarkeitshemmung nicht zulässt. Doch auch unter diesen gemischten Vorzeichen haben meine Mitarbeitenden, zusammen mit Vertretern der Datenschutzkonferenz, wieder an vielen Stellen der Registermodernisierung mitgewirkt.

OZG-Änderungsgesetz

Am 23. Juli 2024 wurde das Gesetz zur Änderung des Onlinezugangsgesetzes (OZG-Änderungsgesetz) verkündet, welches schon im vorherigen Berichtszeitraum intensiv von mir begleitet wurde.[106] Für die Registermodernisierung ist dabei insbesondere die sog. Once-Only-Generalklausel des § 5 E-Government-Gesetz hervorzuheben. Diese Regelung erlaubt es allen öffentlichen Stellen, Nachweise und Daten direkt aus den Registern von Bund, Ländern sowie Kommunen abzurufen, soweit dies von Bürgerinnen und Bürgern im Rahmen einer OZG-Verwaltungsleistung gewünscht ist. Nach eingehender Beratung konnte erreicht werden, dass in Zukunft sämtliche Übermittlungen auf dieser Rechtsgrundlage, ob mit oder ohne IDNr, im Datenschutzcockpit (DSC) angezeigt werden. Gleiches gilt für solche der Registermodernisierungsbehörde (RegMoB). Die nun beschlossene Once-only-Generalklausel ist aufgrund ihres umfassenden, transparenzschaffenden Ansatzes in Bezug auf die Verwaltungsdigitalisierung eine weitsichtige und bürgerfreundliche Regelung, die ich daher ganz ausdrücklich begrüße. Für Übertragungen in andere EU-Mitgliedsstaaten auf Grundlage der Single-Digital-Gateway-VO verbleibt indes im geltenden Recht eine Transparenzlücke.

Während der IT-Planungsrat (IT-PLR) sich für einen Nachweisaustausch in Echtzeit (synchron) aussprach, entschied sich der Gesetzgeber dafür, im Bürgerkontakt auch zeitlich gestaffelte (asynchrone) Nachweisaustausche zulassen zu wollen. Dies führt leider dazu, dass die für die Transparenz sehr wichtige Vorschaufunktion beim Nachweisabruf nur noch eingeschränkt zur Verfügung steht. Für diese Fälle sollte noch eine ebenso niedrigschwellige Art der Nachschau definiert und geregelt werden.

Gesamtsteuerung Registermodernisierung

Allgemein

Auch im Jahr 2024 begleitete ich die Gesamtsteuerung Registermodernisierung (GS RegMo) bei der Umsetzung dieses großen Projekts. Dabei arbeitete ich insbesondere mit dem Lenkungskreis der Gesamtsteuerung sowie

105 32. TB Nr. 8.2, Seiten 99–101
106 32. TB Nr. 8.2, Seiten 102 f.

dem Programmbereich Recht (PB Recht) zusammen. All dies unter kontinuierlicher Mitwirkung der von mir geleiteten Kontaktgruppe Registermodernisierung der Datenschutzkonferenz (Kontaktgruppe).

Staatsvertrag NOOTS

Wieder spielten die Planungen zur Errichtung eines Nationalen Once-Only-Technical-Systems (NOOTS) eine gewichtige Rolle. Das NOOTS wird die zentrale technische Infrastruktur für den Austausch von Nachweisen zwischen verschiedenen öffentlichen Stellen bilden. Schwerpunkt in 2024 war dabei die Ausgestaltung einer tragfähigen Rechtsgrundlage für das NOOTS in Form eines geplanten Bund-Länder-Staatsvertrags. Diesbezüglich fand ab August 2024 ein intensiver Austausch zwischen dem PB Recht sowie dem IT-PLR und der Kontaktgruppe statt. Leider führten diese Beratungen nicht in allen Belangen zu einem datenschutzfreundlichen Ergebnis. So beschloss der IT-PLR im November 2024 einen Entwurf für den Staatsvertrag, der weder unmittelbar wirkende Zweckbegrenzungen für das NOOTS noch die Einrichtung einer gemeinsamen Anlaufstelle für Betroffene vorsieht. Stattdessen beschränkt sich der Entwurf darauf, zunächst nur Onlinedienste nach dem OZG sowie Register im Sinne des IDNrG zum Anschluss an das NOOTS zu verpflichten. Der Anschluss weiterer öffentlicher Stellen zu anderen Zwecken, die auch erst im weiteren Verlauf der Errichtung des NOOTS definiert werden sollen, bleibt ausdrücklich offen. Dabei ging es auch um eine mögliche Nutzung des NOOTS in der Eingriffsverwaltung. Eine derartige Ausweitung gefährdet die bisher gefundene Balance zwischen Risiken und Vorteilen der Verwaltungsdigitalisierung. Dem insofern für die Umsetzung des Once-Only-Prinzips notwendigen, umfassenden Datenaustauschsystem stünde im Rahmen der Eingriffsverwaltung ohne Weiteres kein ausreichender datenschutzrechtlicher Ausgleich gegenüber.

Bereits die Einrichtung des NOOTS als bereichsübergreifendes, niedrigschwelliges Austauschsystem über personenbezogene Daten zwischen verschiedenen Stellen des Staats ist ein Eingriff in die Grundrechte des Einzelnen, der eines wirksamen Ausgleichs bedarf.[107] Ohne Direkterhebung beim Bürger fällt technischen Mitteln zur Transparenz und Kontrolle, gepaart mit strukturellen Zusammenführungshemmnissen, diese wichtige Ausgleichsfunktion im Rahmen der Registermodernisierung zu. Dieses Ausgleichsregime ist allerdings spezifisch auf die antragsbasierte Leistungsverwaltung ausgerichtet und nicht auf eine etwaige Eingriffsverwaltung, bei der der Staat von sich aus aktiv wird. Wenn der Staat von sich aus Datenübermittlungen veranlasst, ist eine effektive Transparenz und Kontrolle durch den Bürger unmöglich oder bestenfalls nur nachgelagert denkbar. Der vertiefte Eingriff alleine durch die Errichtung dieses umfassenden Austauschsystems bliebe so ohne Ausgleich. Besonders intensiv wirkt dieses weite Anwendungsfeld mit Blick auf die Arbeit von Polizei- und Sicherheitsbehörden. Das Fehlen eines klaren Ausschlusstatbestands im Staatsvertrag, wie er z. B. in § 5 IDNrG vorgesehen ist, wird an dieser Stelle verschärfte Anforderungen auf die Gestaltung der technischen und organisatorischen Maßnahmen im NOOTS zur Folge haben, wobei noch nicht abschließend beschieden ist, ob alleine darüber eine datenschutzgerechte Gestaltung möglich sein wird. Die Gesetzgeber in Bund und Ländern sollten diesen Ausschlusstatbestand ausdrücklich regeln.

Zuletzt erschwert das Fehlen einer gemeinsamen Anlaufstelle für Betroffene eine wirksame Umsetzung der Betroffenenrechte gemäß Art. 12 Abs. 1 DSGVO, wonach diese durch den Verantwortlichen verständlich, leicht zugänglich und klar zu erfolgen hat. Dies ist bei den kleinteilig aufgefächerten Regelungen zur Verantwortlichkeit im Rahmen von OZG-Leistungen nur noch bedingt der Fall: So nimmt der Onlinedienst den Antrag in eigener Verantwortlichkeit entgegen. Wenn für den Antrag bestimmte Nachweise benötigt werden, stellen die am NOOTS angeschlossenen Register diese zur Verfügung, allerdings ebenfalls in eigener Verantwortlichkeit. Das NOOTS selbst wird die jeweiligen Übermittlungen als Verantwortlicher durchführen und erst im letzten Schritt tritt dann noch die eigentlich zuständige Fachbehörde hinzu. Selbst wenn diese Zerfaserung eine unvermeidbare Folge des arbeitsteiligen Zusammenwirkens mehrerer öffentlicher Stellen an der Verwaltungsdigitalisierung ist, ist es für den Betroffenen nicht mehr ohne Weiteres nachvollziehbar, wo die Grenzen zwischen den einzelnen Teilschritten verlaufen und an wen er sich dementsprechend wenden muss. An dieser Stelle sollten die Gesetzgeber von Bund und Ländern ebenfalls noch einmal nachbessern, ggf. auch im Rahmen einer vermutlich ohnehin notwendigen Anpassung des IDNrG (siehe im nachfolgenden Abschnitt).

Konzept der Sicheren Anschlussknoten/ Konsultation NOOTS

Für bereichsübergreifende Übermittlungen unter Nutzung der IDNr ist in § 7 Abs. 2 IDNrG eine zusätzliche Sicherungsmaßnahme definiert, nach der Übermittlun-

107 32. TB Nr. 8.2, Seite 101

gen verschlüsselt über Vermittlungsstellen zu erfolgen haben. Diese müssen unabhängig von den öffentlichen Stellen sein, die miteinander kommunizieren wollen, und dürfen keine Kenntnis von den Inhalten der Nachrichten erhalten. In der Diskussion um die technische Umsetzung schlug der technisch orientierte Programmbereich NOOTS der GS RegMo eine Architektur vor, bei der die Übermittlung nicht mehr einen tatsächlichen Weg über eine Vermittlungsstelle nehmen soll, sondern die Vermittlungsstelle lediglich einen Zulässigkeitsnachweis ausstellt, der vor der Kommunikationsverbindung zwischen den öffentlichen Stellen geprüft wird (sog. Token-Lösung). Flankiert werden soll die Veränderung durch die Einführung sog. Sicherer Anschlussknoten (SAK). Die SAK sollen dabei eine durch das NOOTS bereitgestellte, verpflichtende technische Infrastruktur sein, die allerdings nicht zentral betrieben wird, sondern lokal bei jedem angeschlossenen Kommunikationsteilnehmer. Der lokale Betrieb hat dabei zur Folge, dass die jeweilige Stelle die Kommunikationsinhalte noch im SAK im Klartext einsehen kann. Ein Grund für diesen Architekturvorschlag war u. a. die bessere Skalierbarkeit und Offenheit für Weiterentwicklungen oder Wechsel der eingesetzten Transportprotokolle.

Der PB Recht und mein Haus kamen zunächst übereinstimmend zum Ergebnis, dass dieser Architekturvorschlag den Anforderungen des § 7 Abs. 2 IDNrG nicht gerecht wird, da die Übermittlungen dann nicht mehr über eine Vermittlungsstelle liefen. Es wäre so in jedem Fall eine Rechtsanpassung notwendig. Gleichzeitig ergaben meine Prüfungen, dass dieser alternative Ansatz durchaus das Potential hat, ein mindestens ebenso wirksames Zusammenführungshemmnis wie die aktuell definierten Vermittlungsstellen zu sein, wenn nicht sogar darüberhinausgehend. Eine dementsprechende Weiterentwicklung dieses Ansatzes könnte so ein wichtiger Beitrag werden, das Gesamtsystem der Registermodernisierung, welches immer noch am Makel einer einheitlichen IDNr leidet, erheblich datenschutzfreundlicher zu gestalten. Hierfür müssen allerdings einige Anforderungen durch die Kombination aus Token-Vermittlungsstelle und SAK erfüllt werden. Der dauerhafte sowie unmanipulierte Betrieb und Einsatz dieser Einrichtungen muss technisch sichergestellt sein und darf nicht von willentlichen Entscheidungen der angeschlossenen Behörden oder einzelner Mitarbeiter abhängen. Die SAK dürfen nicht selbst zu einer Erhöhung der Zusammenführbarkeit führen. Auf die dort im Klartext eingebrachten Nachrichten darf nur der zuständige Kommunikationsteilnehmer Zugriff haben. Selbst technische Dienstleister der öffentlichen Stelle sollten die Übermittlungsinhalte nicht einsehen können. Die bereits nach aktueller Rechtslage vorgesehene Prüfung der abstrakten Übermittlungsberechtigung muss sich auch auf die Kohärenz zwischen angegebenen und tatsächlichen Übermittlungszweck erstrecken sowie beim Übermittlungsanlass auch die tatsächliche Initiierung des Vorgangs durch den Bürger erfassen. Gerade mit Blick auf diese abstrakten Prüfungen bietet die Konstruktion des SAK mit seinem Zugriff auf die Klardaten große Chancen, die letztlich zu einer Verbesserung des Datenschutzniveaus und einer effektiven Minderung des verfassungsrechtlichen Eingriffs durch das Once-Only-Prinzip führen könnten. Genau dieser Zugriff birgt aber zugleich auch das Risiko einer noch gesteigerten Verbreitung der betreffenden personenbezogenen Daten.

Im Laufe des Jahres entwickelte die GS RegMo diesen architektonischen Ansatz weiter und stellte ihn im Rahmen einer größeren Konsultation zum NOOTS vor, an der mein Haus ebenfalls beteiligt wurde. Die Beratungen hierzu werden 2025 fortgesetzt. Trotz der bisherigen Unklarheiten erkenne ich aber weiterhin eine große Chance in dem neuen Ansatz. Insbesondere auch deshalb, weil die bisherigen Architekturplanungen eine stete Einbindung der Vermittlungsstelle vorsehen, selbst dann, wenn die gewünschte Übermittlung nicht bereichsübergreifend ist. Zu diesem Thema werde ich in Zukunft gerne weiterhin beratend zur Seite stehen.

Rechtsverordnung Verwaltungsbereiche

Bereits im vorigen Jahr berichtete ich über die laufende Erarbeitung einer Rechtsverordnung zur Festlegung der Verwaltungsbereiche im Sinne des § 7 Abs. 2 IDNrG.[108] Durch die bereits erwähnten, vorläufigen Entscheidungen zur Architektur des NOOTS und der Vermittlungsstelle könnte sich die Notwendigkeit der Rechtsverordnung allerdings möglicherweise erledigen. Denn bei einem flächendeckenden Einsatz der Vermittlungsstelle, bräuchte es keine Bereiche mehr. Das bereits geltende Recht müsste an diesen Ansatz angepasst werden.

Unterprojekte

Im aktuellen Berichtsjahr sind einige wichtige Unterprojekte der GS RegMo weiter fortgeschritten. Hierzu zählen u. a. die geplante Einführung der IDNr nebst Anschluss an das DSC bei der Bundesagentur für Arbeit, dem Kraftfahrtbundesamt, der Deutschen Gesetzlichen Unfallversicherung sowie der Deutschen Rentenversicherung. Diesbezüglich habe ich bereits erste Kontakte

108 32. TB Nr. 82, Seite 102

mit der entsprechenden Projektseite bei der RegMoB hergestellt und plane für 2025 eine intensivierte Zusammenarbeit.

Pilotierung NWR

Ein weiteres Thema, über das mein Haus bereits im vorigen Tätigkeitsbericht informierte , war die Pilotierung der Einspeicherung der IDNr und der Anschluss an das DSC beim Nationalen Waffenregister (NWR).[109] Das NWR wurde vor allem deswegen als Pilot ausgewählt, da es vom Bundesverwaltungsamt (BVA) betrieben wird, welches gleichzeitig auch als RegMoB fungiert. Ein datenschutzrechtlicher Schwerpunkt war dabei die Bewertung der sog. Ersteinspeicherung, also der erstmaligen Einführung der IDNr in das Register. Hierbei vertrat mein Haus, anders als BMI und BVA, die Ansicht, dass auch diese erstmalige Einführung der IDNr bereits im Datenschutzcockpit (DSC) anzuzeigen ist und nicht erst nachfolgende Übermittlungen. In diesem Zusammenhang sind die Auswirkungen des OZG-Änderungsgesetzes noch Gegenstand anhaltender Prüfungen, wobei der besonders transparenzfreundliche Ansatz der neuen Regelungen ebenfalls dafürspricht, auch die Ersteinspeicherung in das DSC einzubringen.

Unstrittig ist allerdings, dass nachfolgende Übermittlungen unter Nutzung der IDNr im DSC transparent zu machen sind. Diese Anforderung entwickelte sich Anfang 2024 zum Problem, da das DSC aufgrund verschiedener Umstände noch nicht einsatzfähig am Register angeschlossen war, aber gleichwohl ein weiterer Datenaustausch zwischen NWR und der Identifikationsnummerndatenbank beim Bundeszentralamt für Steuern (BZSt) stattfinden sollte. Deshalb sprach mein Haus im März 2024 eine formale Warnung an das BVA bezüglich dieser beabsichtigten Übermittlungen aus und wies darauf hin, dass sie erst erfolgen dürfen, sobald sie im DSC transparent gemacht werden können. Die Gründe für die Verzögerung waren zum einen das Fehlen einer belastbaren Rechtsverordnung für die Benennung der für das DSC verantwortlichen Stelle sowie zum anderen Sicherheitsbedenken seitens des NWR bezüglich der Ende-zu-Ende-Verschlüsselung des DSC und den daraus resultierenden Anforderungen für die eigene technische Infrastruktur. Leider konnte gerade das letztere Problem auch bis zum Ende des Berichtszeitraums nicht gelöst werden, so dass die Pilotierung beim NWR aktuell weiterhin auf Eis liegt. Aufgrund der besonderen Wichtigkeit der Transparenzgewährung über das DSC werde ich dieses Thema in Zukunft weiter intensiv bearbeiten.

Datenschutzcockpit

Auch die Begleitung des DSC wurde gemeinsam mit der Kontaktgruppe fortgesetzt. Ein Schwerpunkt war dabei u. a. die Finalisierung der Rechtsverordnung über die Bestimmung der für den Betrieb des DSC zuständigen Stelle. Entwickelt wurde das DSC hauptsächlich unter Federführung des Landes Bremen. Aus verfassungsrechtlichen Gesichtspunkten entschied sich der Verordnungsgeber im Juli 2024 für eine Benennung des BVA als zuständige Stelle. Dies führt dazu, dass ich seitdem das Projekt nicht nur beratend, sondern auch in der Rolle als Aufsichtsbehörde begleite. Mit dieser Festlegung waren eigentlich alle Voraussetzungen für den Beginn des Echtbetriebs des DSC erfüllt, denn technisch war es schon seit 2023 einsatzbereit.[110] Durch die dann aber zusätzlich aufgekommenen Sicherheitsbedenken bei der Implementierung der Ende-zu-Ende-Verschlüsselung des DSC (siehe oben) verzögerte sich die Inbetriebnahme mit dem NWR als angeschlossenem Register jedoch bis auf Weiteres. Letztlich entschieden sich BMI und BVA daher dafür, dass DSC Ende 2024 ganz ohne Register online gehen zu lassen.

Weiterhin wurde auch an der zukünftigen Entwicklung des DSC weitergearbeitet. Vorrangig ging es dabei um die Gestaltung der sog. Bestandsdatenauskunft, also einer Auskunft über die dauerhaft in einem Register gespeicherten Daten zu einer Person (das DSC greift ansonsten ausschließlich auf Daten zu, die bei konkreten Übermittlungen anfallen). Da es sich bei der Bestandsdatenauskunft bereits um geltendes Recht nach § 10 Abs. 2 OZG handelt, muss diese schnellstmöglich implementiert werden. Insbesondere vor dem Hintergrund, dass nun für 2025 gleich für mehrere Register die Einspeicherung der IDNr vorgesehen ist. Eine Nutzung der IDNr ohne Bestandsdatenauskunft wäre allerdings nach Auffassung meines Hauses rechtswidrig.

Durch den Bruch der Regierungskoalition und dem bislang nicht verabschiedeten Haushalt für das Jahr 2025 zeichnet sich noch weiterer, negativer Ausblick für das DSC ab. Nach den Erkenntnissen meines Hauses werden die vorläufigen Mittel, die dem DSC zur Verfügung stehen, weder für einen regulären Minimalbetrieb noch für die Entwicklung der Bestandsdatenauskunft ausreichen. Wie aber bereits bei der Pilotierung des NWR dargestellt (siehe oben), ist das DSC als zentrales Transparenzinst-

109 32. TB Nr. 8.2, Seiten 103 f.
110 32. TB Nr. 8.2, Seiten 103 f.

rument eine zwingende Voraussetzung für die rechtmäßige Verarbeitung der IDNr. Sollte diese Problematik von der nächsten Bundesregierung nicht rechtzeitig gelöst werden, drohen große Verzögerungen bei der Umsetzung der Registermodernisierung.

Austausch mit dem Bundeszentralamt für Steuern

Im März des Berichtsjahres fand ein Informationsaustausch mit dem BZSt statt. Als Betreiberin der Identifikationsnummerndatenbank spielt das BZSt eine wichtige Rolle für die Umsetzung der Registermodernisierung. Schwerpunkt des Austauschs war dabei insbesondere die Kommunikation mit der RegMoB. Zu den wichtigsten datenschutzrechtlichen Erkenntnissen gehörte dabei, dass die Anfragen der RegMoB grundsätzlich keine registerspezifischen Daten enthalten und sie generell auch nur bis zur abschließenden Bearbeitung beim BZSt gespeichert und danach vollständig gelöscht werden. Das Entstehen einer „Schattendatenbank" ist damit weitestgehend ausgeschlossen. Weitere Aspekte des Austauschs betrafen die Einführung der IDNr in die Melderegister (dort in Form einer Umwidmung der bereits gespeicherten Steuer-ID) sowie in die Personenstandsregister (mit voraussichtlich erheblichen Zuordnungsproblemen) und zuletzt die Aufstellung eines Qualitätssicherungsprozesses für den Fall, dass die Register auf anderem Wege dem BZSt widersprechende Daten erhalten. Gerade diese Themen werden in Zukunft Gegenstand weiterer Beratungen sein.

Ausblick

Neben den bereits erwähnten Themenfeldern, die eine fortgesetzte Begleitung meinerseits erfordern, erwarte ich für die nähere Zukunft weitere grundsätzliche Weichenstellungen zum Einsatz der IDNr. Wie bereits im vorigen Tätigkeitsbericht erwähnt, wäre die Schaffung von Parallelsystemen, die statt auf die IDNr auf die (identische) Steuer-ID setzen, ein schwerwiegendes verfassungsrechtliches Problem für die weitere Verwaltungsdigitalisierung.[111] Selbst wenn meine grundsätzlichen Bedenken zum Einsatz eines einheitlichen Identifikators weiterhin bestehen (s. o.), sollten Lösungen gefunden werden, die auf der bestehenden Systematik der IDNr und des NOOTS aufbauen, da dort – anders als für die Steuer-ID – zumindest einige wichtige Datenschutzmaßnahmen von Anfang an berücksichtigt wurden.

Ich empfehle der Bundesregierung und dem Gesetzgeber weiterhin, keine Parallelsysteme für den bereichsübergreifenden Datenaustausch und die Umsetzung des Once-Only-Prinzips zu schaffen. Stattdessen sollte mit Blick auf das bereits bestehende Fundament aus IDNrG, EGovG, OZG sowie dem NOOTS als zentraler Infrastruktur ein einheitlicher Ansatz verfolgt werden, bei dem für noch bestehende datenschutzrechtliche Probleme konstruktive Lösungen zu entwickeln sind.

Ich empfehle der Bundesregierung weiterhin, dem weiten Transparenzverständnis des Deutschen Bundestages im Rahmen der Verwaltungsdigitalisierung (siehe Ausschussdrucksache 20(4)258 vom 19. Juli 2023) Rechnung zu tragen und auch die erstmalige Einspeicherung der IDNr in ein Register gemäß § 2 Nr. 1 IDNrG im Datenschutzcockpit sichtbar zu machen. Zudem sollten frühzeitig die notwendigen Vorbereitungen getroffen werden, die (noch) mit der Steuer-ID versehenen Datenübermittlungen der Meldeämter transparent machen zu können, sobald diese in die IDNr umgewidmet wurde.

7.2.2 EuGH-Urteile zum Beschwerderecht

In mehreren Gerichtsentscheidungen hat der Europäische Gerichtshof (EuGH) den Umfang des Beschwerderechts betroffener Personen und die Pflichten der Datenschutzaufsichtsbehörden weiter konturiert.

Im Berichtsjahr hat sich der EuGH in mehreren Entscheidungen sowohl mit dem Beschwerderecht betroffener Personen als auch mit den Durchsetzungspflichten der Datenschutzaufsichtsbehörden befasst. Nach Art. 77 Abs. 1 DSGVO hat jede betroffene Person das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren, wenn sie der Ansicht ist, dass eine Verarbeitung, von der ihre personenbezogenen Daten betroffen sind, gegen die DSGVO verstößt. In seinen Entscheidungen hat der EuGH klargestellt, dass es sich bei dem Beschwerderecht nicht um ein bloßes Petitions- bzw. petitionsähnliches Recht handelt.[112] [113] Vielmehr stelle die Entscheidung über eine Beschwerde einen rechtsverbindlichen Beschluss dar, dessen Richtigkeit von Gerichten vollständig überprüft werden könne. Einige deutsche Gerichte hatten das zuvor anders entschieden und waren davon

111 32. TB Nr. 8.2

112 Urteil des EuGHs vom 7. Dezember 2023, C-26/22 und C-64/22, abrufbar unter: https://eur-lex.europa.eu/eli/C/2024/917/oj/eng

113 Urteil des EuGHs vom 26. September 2024, C-768/21, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0768&qid=1739617269549

ausgegangen, dass die Richtigkeit der Behördenentscheidung gerichtlich allenfalls auf Willkür überprüft werden könne. Dieser Auffassung ist der EuGH nicht gefolgt.

Zudem hat der EuGH entschieden, dass die Datenschutzaufsichtsbehörde im Falle eines Datenschutzverstoßes durch eine beaufsichtigte Stelle verpflichtet sei, in geeigneter Weise zu reagieren, um der festgestellten Unzulänglichkeit abzuhelfen. Hierzu verweist er auf die Durchsetzungsmaßnahmen nach Art. 58 Abs. 2 DSGVO. Insoweit sei die Datenschutzaufsichtsbehörde verpflichtet, eine oder mehrere Durchsetzungsmaßnahmen zu ergreifen, wenn diese geeignet, erforderlich und angemessen sind. Zugleich sei es aber nicht ausgeschlossen, dass es ausnahmsweise aufgrund besonderer Umstände des Einzelfalls gerechtfertigt sein könne, von Durchsetzungsmaßnahmen abzusehen. Grundsätzlich könne die Datenschutzaufsichtsbehörde das geeignete und erforderliche Mittel wählen. Dieses Ermessen können Gerichte nur auf Ermessensfehler prüfen, insbesondere ob die oben aufgezeigten Grenzen von der Datenschutzaufsichtsbehörde eingehalten wurden. Zugleich verneinte der EuGH einen subjektiven Anspruch von Beschwerdeführenden auf eine Geldbuße. Geldbußen werden ausschließlich im öffentlichen Interesse verhängt.

Ich begrüße die Entscheidungen des EuGHs ausdrücklich. Der bislang zwischen den deutschen Obergerichten bestehende Meinungsstreit über den Charakter der Beschwerde nach Art. 77 DSGVO ist damit geklärt. Die Entscheidungen werden der Bedeutung des Beschwerderechts gerecht und verdeutlichen die gesetzlichen Durchsetzungspflichten und höchstrichterlichen Erwartungen an eine effektive Datenschutzaufsicht. Gleichzeitig wahren sie die Verhältnismäßigkeit in besonderen Ausnahmefällen. Damit es aber möglichst gar nicht erst zu Datenschutzverstößen kommt, ist es umso wichtiger, dass mein Beratungsangebot angenommen wird und ich gerade bei staatlichen Projekten bereits zu einem frühen Zeitpunkt eingebunden werde.

7.2.3 Datenschutz im Deutschen Bundestag

Bereits seit Einführung der DSGVO stellte sich die Frage, ob diese auch auf die deutschen Parlamente – einschließlich den Deutschen Bundestag – Anwendung findet und welche unabhängige Stelle deren Anwendung überwacht. Nun hat der Europäische Gerichtshof (EuGH) entschieden.

Seit Jahrzehnten stellt sich die Frage, welche datenschutzrechtlichen Vorschriften auf Parlamente und deren jeweilige Mitglieder Anwendung finden, ob diese Anwendbarkeit auch den parlamentarischen Kernbereich seiner Arbeit umfasst und wer die Einhaltung dieser Vorschriften überwacht. Auch mit Einführung der DSGVO wurden die offenen Fragen nicht ausdrücklich geregelt. Weder wurden die Parlamente der Mitgliedstaaten in deren Anwendungsbereich erwähnt, noch wurde eine Regelung zur Wahrnehmung der korrespondierenden datenschutzrechtlichen Aufsicht vorgesehen. Insbesondere wurden die allgemeinen Aufsichtsbehörden insoweit nicht für unzuständig erklärt, wie Art. 55 Abs. 3 DSGVO dies für die vergleichbare Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen regelt.

Mein Haus hat stets die Anwendbarkeit der DSGVO im parlamentarischen Kernbereich angenommen und die insoweit erforderliche Datenschutzaufsicht gelebt. An mich gerichtete Anfragen und Beschwerden zum Deutschen Bundestag wurden und werden ausnahmslos und mit besonderem Fokus bearbeitet. Die Bandbreite der betroffenen Datenverarbeitungen reicht dabei von Anfragen und Petitionen an das Parlament und seine Mitglieder, über den Auftritt der Abgeordneten im Internet und in sozialen Netzwerken bis hin zu deren Tätigkeit als Arbeitgeberin oder Arbeitgeber. Leider war insoweit lange unklar, wie weit meine Aufsichtsbefugnisse reichen. Wegen der besonderen Stellung des Deutschen Bundestages und seiner unmittelbar gewählten Mitglieder habe ich mich auf meine Beratungsaufgabe gegenüber dem Parlament konzentriert. Ungeachtet dessen ist es in den vergangenen Jahren fast ausnahmslos gelungen, die an mich herangetragenen Datenschutzverletzungen aufzuklären und Vorsorge zu treffen, dass diese nach Möglichkeit zukünftig unterbleiben. Hierdurch konnten die Hinweise vieler Bürgerinnen und Bürger umgesetzt und der Datenschutz im parlamentarischen Bereich insgesamt verbessert werden. Zudem stand mein Haus über die Jahre hinweg stets im Austausch mit dem Parlament, um dieses bei der Klärung der offenen Fragen, insbesondere betreffend die Datenschutzaufsicht zu unterstützen.

Der EuGH hat nun Klarheit geschaffen. [114] Ich begrüße sehr, dass das höchste europäische Gerichts bestätigt hat, dass die DSGVO grundsätzlich im parlamentarischen Bereich unmittelbare Anwendung findet.

---

114 Urteil des EuGHs vom 16. Januar 2024, C-33/22, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62022CJ0033&qid=1739617197928

Bei datenschutzaufsichtsrechtlichen Entscheidungen müssen meines Erachtens parlamentarische Anforderungen gebührend gewürdigt werden, um die legislative Kernfunktion des demokratisch unmittelbar legitimierten Parlamentes unberührt zu lassen. Mit einem klaren Schwerpunkt auf Information und Beratung kann mein Haus auf die Einhaltung datenschutzrechtlicher Vorgaben von Anfang an und angemessen hinwirken.

7.2.4 Sicherheitslücken gefährden den Schutz personenbezogener Daten

Sicherheitslücken und schlecht gewartete Systeme stellen eine erhebliche Gefahr für den Schutz personenbezogener Daten dar. Um diese Gefahr zu minimieren ist es notwendig, dass Sicherheitslücken schnellstmöglich von Verantwortlichen durch Aktualisierungen geschlossen werden und Erkenntnisse über Sicherheitslücken unmittelbar genutzt werden, um diese zu schließen.

In diesem Berichtsjahr stellen Sicherheitslücken weiterhin eine schwerwiegende Bedrohung für personenbezogene Daten dar. Sicherheitslücken werden schneller ausgenutzt als Aktualisierungen eingespielt werden oder Hersteller Aktualisierungen bereitstellen. Sowohl die langen Reaktionszeiten von Herstellern nach der Meldung von Lücken, als auch die mangelnde Qualität von bereitgestellten Aktualisierungen sind in diesem Berichtszeitraum besonders aufgefallen. So wurden in diesem Berichtsjahr potenzielle Datenschutzvorfälle im Sinne des Art. 33 DSGVO gemeldet, die auf einer bekannten Sicherheitslücke beruhten, vor der das BSI bereits gewarnt hatte. Die verantwortliche Stelle hatte bereits eine entsprechende Aktualisierung eingespielt, die zwischenzeitlich allerdings wieder obsolet geworden war, weil der Hersteller nachbessern musste. Dennoch stellen veraltete und schlecht gewartete Systeme weiterhin ein großes Problem dar.

Jede Sicherheitslücke stellt zunächst ein potentielles Risiko für die Verletzung des Datenschutzrechts dar. Ob eine Sicherheitslücke ausgenutzt wurde und personenbezogene Daten betroffen waren, ist für Verantwortliche häufig schwer festzustellen und dauert teils sehr lange. Die lange Zeit, die für eine Aufklärung benötigt wird, ist problematisch, da sich Gegenmaßnahmen zur Eindämmung eines möglichen Missbrauchs personenbezogener Daten kaum noch sinnvoll treffen lassen. Ein Grund dafür ist, dass Angreifer Sicherheitslücken ggf. auch in Kombination mit kompromittierten Zugangsdaten ausnutzen, um Hintertüren zu installieren. Aktiv werden die Angreifer teils erst lange Zeit nach dieser Installation. Die Zeit, bis diese maliziösen Aktivitäten auffallen, kommt hinzu. In solchen Fällen ist aus den vorhandenen Daten oft nicht mehr festzustellen, ob und inwieweit zwischenzeitlich Aktivitäten stattgefunden haben und damit auch nicht, in welchem Umfang ggf. der Schutz personenbezogener Daten verletzt wurde.

Durch die immer größere Abhängigkeit von einzelnen Herstellern oder Software-as-a-Service-Lösungen wirken sich einzelne Sicherheitslücken oder Fehler auf viele Stellen aus. Seien es unbeabsichtigte Betriebsstörungen oder Sicherheitslücken. Insbesondere bei Sicherheitslücken in solchen weit verbreiteten Produkten ist ein großflächiges Angriffsgeschehen festzustellen. Im Berichtszeitraum sind mehrere Artikel-33-Meldungen eingegangen, die auf die gleiche Sicherheitslücke bei unterschiedlichen Verantwortlichen zurückgeht.

Unerlässlich für den Schutz personenbezogener Daten ist es, dass Sicherheitslücken sofort geschlossen werden. Dazu ist es notwendig, dass Sicherheitslücken unverzüglich an den Hersteller oder ggf. eine zentrale Stelle wie das BSI gemeldet werden. Verantwortliche müssen die Aktualisierungen unmittelbar einspielen. Als effektiv zeigen sich dabei die Warnmeldungen des BSI, aufgrund derer Verantwortliche ihre Systeme geprüft und entsprechende Ausnutzungen von Sicherheitslücken festgestellt haben, wie aus Artikel-33-Meldungen an mein Haus hervorgeht.

Darüber hinaus ist es wichtig, dass Verantwortliche technische und organisatorische Maßnahmen ergreifen, um die Möglichkeiten erfolgreicher Angreifer einzuschränken und zu begrenzen. Dazu zählt insbesondere die Datenminimierung bereits zum Erhebungszeitpunkt, eine frühestmögliche Löschung, aber auch Maßnahmen wie Pseudonymisierung und Anonymisierung. Um die Sicherheit der Verarbeitung zu gewährleisten, muss der Verantwortliche auch bei der Auswahl der genutzten Produkte sorgfältig vorgehen. Als ein Auswahlkriterium sollte auch der Umgang des Herstellers mit Sicherheitslücken herangezogen werden.

Ich empfehle dem Gesetzgeber, eine unverzügliche Meldepflicht für Sicherheitslücken mit dem Ziel der sofortigen Beseitigung an den Hersteller oder eine zentrale koordinierende Stelle gesetzlich zu verankern, um die IT-Sicherheit in Deutschland zu stärken.

7.2.5 Die europäische Brieftasche für die digitale Identität und ihre nationale Umsetzung in Deutschland

Die reformierte eIDAS-Verordnung erweitert die eID-Systeme der Mitgliedstaaten zur elektronische Identifizierung um elektronische Brieftaschen. Die in der Verordnung festgehaltenen Rechte für Bürgerinnen und Bürger müssen jetzt über Durchführungsrechts-

akte und technische Vorgaben wirksam umgesetzt werden. Nur so kann Vertrauen in diese Schlüsseltechnologie der Digitalisierung entstehen.

Im März 2024 wurden Änderungen an der EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS VO) verabschiedet. Die Mitgliedsstaaten sind demnach verpflichtet, Bürgerinnen und Bürgern eine Brieftasche für die digitale Identität zur Verfügung zu stellen (EUDI-Wallet). Bisher haben die Mitgliedstaaten nur eID-Systeme zur Verfügung gestellt. In Deutschland ist das die Onlineausweisfunktion des Personalausweises, des elektronischen Aufenthaltstitels und der eID-Karte für Bürgerinnen und Bürger aus EU-Mitgliedstaaten. [115] Wallets oder digitale Brieftaschen gehen einen Schritt weiter als reine eID-Systeme. Mit ihnen sollen auch Nachweise und Eigenschaften, die über Identitätsdaten hinausgehen, digital vorgehalten und für Dienstleistungen vorgelegt werden können. Dann sollen in einer App nicht nur der Ausweis, sondern auch beliebige andere Attribute wie z. B. die Fahrerlaubnis, Zugangsberechtigungen und Zeugnisse, aber auch Mitgliedschaften oder Konzerttickets abgelegt werden können. Diese Weiterentwicklung einer staatlich-regulierten sicheren digitalen Identität begrüße ich, da sie als „Schlüssel" für alle digitalisierten Lebensbereiche genutzt werden kann. Wichtig ist, dass die Rechte der Bürgerinnen und Bürger gewahrt bleiben.

EUDI-Wallet

Die eIDAS VO hat hier auch gute Ansätze: So ist die Nutzung der EUDI-Wallet freiwillig und zudem auch eine Nichtdiskriminierungsklausel vorhanden, die besagt, dass Bürgerinnen und Bürgern keine Nachteile beim Zugang zu öffentlichen und privaten Diensten entstehen dürfen, wenn sie sich gegen die EUDI-Wallet entscheiden (Art. 5a Abs. 15 S. 1 und 2 eIDAS VO). Wenn die Wallet genutzt wird, haben Bürgerinnen und Bürger grundsätzlich das Recht, ein Pseudonym zu nutzen. Eine Identifizierung darf nur dann gefordert werden, wenn eine rechtliche Verpflichtung das vorsieht (Art. 5, Art 5a Abs. 4 lit. b) und Art. 5b Abs. 9 S. 2 eIDAS VO). Auch ist vorgesehen, dass alle Datenverarbeitungen im Zusammenhang mit den personenbezogenen Daten in der Wallet unter alleiniger Kontrolle der Nutzenden stehen (Art. 5a Abs. 4 lit. a) eIDAS VO). Nach allgemeinem Verständnis dieser Regelung muss jede Anfrage einer Stelle an die Wallet durch die Walletnutzenden bestätigt werden. Vor der Bestätigung der Datenübermittlung ist es auch möglich, nur eine Teilmenge der erfragten Daten freizugeben (sog. „Selective Disclosure"). Zur Nachvollziehbarkeit muss die Wallet in einem gemeinsamen Dashboard eine Liste aller Stellen anzeigen, mit denen eine Verbindung aufgenommen wurde, welche Daten diese erhalten haben sowie eine einfache Möglichkeit, diese Stellen zum Löschen der Daten aufzufordern. Bei Verdacht auf unrechtmäßige Anfragen muss die Wallet eine einfache Meldung an die zuständigen Datenschutzbehörden ermöglichen (Art. 5a Abs. 4 lit. d) eIDSA VO). Nutzer müssen ihre Daten auf ihrem Endgerät speichern können und die Wallet muss das Recht auf Datenübertragbarkeit unterstützen (Art. 5a Abs. 4 lit. f) und g) eIDAS VO).

Neben diesen Rechten für die Bürgerinnen und Bürger sind auch Regelungen für die Stellen, die Daten aus der Wallet nutzen wollen, die sogenannten vertrauenden Stellen, vorhanden. Damit Bürgerinnen und Bürger sicher erkennen können, wer sie auffordert, Daten preiszugeben, müssen vertrauende Stellen sich registrieren. Diese Maßnahme schützt auch vor Angreifenden, die sich in die Kommunikation schalten, um Daten abzugreifen oder zu verändern. Vertrauende Stellen dürfen von Bürgerinnen und Bürgern nur die Daten anfordern, die sie im Registrierungsprozess angegeben haben (Art. 5b Abs. 1 bis 3 eIDAS VO).

Diese sinnvollen Regelungen werden jeweils in Durchführungsrechtsakten und technischen Vorgaben weiter ausgeführt. Insbesondere das Recht auf pseudonyme Nutzung wurde in Entwürfen zu technischen Richtlinien leider bislang nicht im gebotenen Maße beachtet. Ich setze mich dafür ein, dass die Rechte der Verordnung in wirksame technische Maßnahmen überführt werden. Das von der Kommission verkündete Ziel, dass alle Mitgliedstaaten 2026 eine Wallet bereitstellen, ist sehr ehrgeizig. Damit die Wallet das Vertrauen der Bürgerinnen und Bürger erhalten kann, muss gründlich und sorgfältig vorgegangen werden und die Wallet möglichst bei Erscheinen ein fertiges und vollständiges Produkt sein.

Deutsche EUDI-Wallet

Den Mitgliedstaaten bleibt Entscheidungsspielraum bei der Wahl der konkreten Technik der Wallet und bei der Frage des Betreibermodells: Die Mitgliedstaaten können die Wallet selber bereitstellen, in Auftrag geben oder eine unabhängige Lösung anerkennen (Art. 5a Abs. 2 eIDAS VO). In Deutschland hat das Bundesministerium des Inneren und für Heimat in einem Konsultationsprozess und über einen Prototypwettbewerb Erkenntnisse zur

115 Im Nachfolgenden beziehen sich Aussagen zum Onlineausweis immer auf alle drei technisch identisch ausgestatteten Dokumente.

Vorbereitung dieser Fragen gesammelt. Unabhängig von der Frage des Betriebsmodells wurde entschieden, bei der Architektur auf signierte Daten zu setzten, was im Vorfeld teilweise umstritten war. So ist die Echtheit bei signierten Daten garantiert, sodass sie einen höheren Wert haben könnten. Alternativ kann man die Echtheit der Daten auch feststellen, indem ein gesicherter Kommunikationskanal verwendet wird. Die Daten sind dabei nur für den einzelnen Identifikationsvorgang nachweisbar echt. Isoliert betrachtet ist letzteres Verfahren, wie es auch die Onlineausweisfunktion nutzt, insofern zu bevorzugen, als es einen gewissen Schutz vor Zweckänderungen/missbräuchlicher Verwendung bietet. Verantwortliche müssen aber, wenn man Art. 25 Abs. 1 DSGVO maßstäblich anlegt, eine Abwägung treffen, welche technischen und organisatorischen Maßnahmen umzusetzen sind, um ein dem Risiko angemessenes Schutzniveau zu erreichen. In der Entscheidung der Bundesregierung zur Architektur der EUDI-Wallet fiel die Abwägung nun für den Nachweis der Echtheit mittels Signatur aus.

Bei einer böswillig handelnden vertrauenden Stelle oder einem Datenleck kann ein hoher Schaden für Betroffene entstehen, wenn ihre Ausweisdaten missbraucht werden. Der potentielle Schaden für Betroffene ist allerdings sowohl bei signierten als auch unsignierten Daten hoch. Der Anreiz für den rechtswidrigen Verkauf von Daten oder illegale Datensammlungen könnte mutmaßlich allerdings höher sein. Die signierten Daten sind aber nicht wesentlich anders nutzbar: Es kann sich damit beispielsweise nicht erneut im EUDI-Wallet-System identifiziert werden.

Kern jeder Wallet ist das nationale Identifizierungsmittel, das die Ausweisdaten bereitstellt. In Deutschland existiert mit der Onlineausweisfunktion ein sicheres und datenschutzfreundliches System. Die Onlineausweisfunktion ist dezentral: Wenn Bürgerinnen und Bürger sich online ausweisen, gibt es eine direkte Verbindung zu der Stelle, gegenüber der sie sich ausweisen. Es müssen keine Daten von einer zentralen Stelle geladen werden. Die Onlineausweisfunktion ist kartengebunden. Bei jeder Interaktion muss der Ausweis bspw. an das Smartphone gehalten werden. Zwar gibt es schon seit langem Bestrebungen, den Ausweis sicher in Smartphones zu hinterlegen und das Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PAuswG) sieht dies in § 10a auch schon vor, allerdings sind Smartphones mit Chips, die das unterstützen, noch wenig verbreitet. Deshalb wird die deutsche Wallet wohl ein „Evolutionslösung“ genanntes System unterstützen. Dabei wird die fehlende Sicherheitsfunktion der Smartphonehardware durch einen zentralen Server kompensiert. Ich berate das fachlich zuständige Bundesamt für Sicherheit in der Informationstechnik mit Fokus auf Maßnahmen zur Reduzierung des Risikos von Nachvollziehbarkeit und Profilbildung an diesem zentralen Server. Hierbei setze ich mich dafür ein, dass die dezentrale Lösung bei einer entsprechenden Verbreitung sicherer Hardware der Smartphones umgesetzt wird.

7.2.6 Anonymisierung

Anonymisierung schafft Freiräume für Forschung, Wertschöpfung und Innovationen. Die Beratung zu Fragen der Anonymisierung ist mir deshalb ein besonders wichtiges Anliegen.

Das Wesen einer Anonymisierung besteht, vereinfacht gesagt, darin, den Personenbezug von Daten aufzuheben. Mit dem Einsatz von Anonymisierungstechniken soll demnach erreicht werden, dass die betroffenen Personen nicht mehr identifiziert werden können.
Die Vorteile dieser Technologien für Datenverarbeiter liegen auf der Hand. Für anonymisierte Daten gelten die datenschutzrechtlichen Anforderungen für Daten mit Personenbezug nicht mehr. Anonymisierung schafft so Freiräume für Forschung, Wertschöpfung und Innovationen. Damit ist sie ein wichtiges Instrument. Anwendungsfälle gibt es unzählige, in allen Bereichen unseres gesellschaftlichen und wirtschaftlichen Lebens, insbesondere dort, wo Daten aggregiert und statistische Zusammenhänge dargestellt werden sollen. Das Verfahren zur Anonymisierung ist allerdings oft nicht einfach. Denn es wird gleichzeitig versucht, eine größtmögliche Aussagekraft der Daten zu bewahren.

Die Komplexität einer solchen Aufgabe bringt einen hohen Beratungsbedarf mit sich. So habe ich im Berichtsjahr in mehreren Projekten Beratungen zu rechtlichen und technischen Fragen der Anonymisierung von personenbezogenen Daten durchgeführt. Darüber hinaus habe ich mich intensiv im Rahmen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und im Rahmen des Europäischen Datenschutzausschusses mit diesem Thema befasst mit dem Ziel einer Verständigung auf eine gemeinsame nationale und internationale Position.

7.2.7 Rechtsklarheit bei IFG-Anfragen über Frag-den-Staat

In seinem Urteil vom 20. März 2024 hat das Bundesverwaltungsgericht (BVerwG) Rechtsklarheit hinsichtlich der Zulässigkeit der standardmäßigen Erhebung der postalischen Anschrift bei Anträgen nach Informationsfreiheitsgesetz (IFG) geschaffen.

Mit Bescheid vom 11. Februar 2020 hatte ich gegenüber dem Bundesministerium des Innern und für Heimat (BMI) eine datenschutzaufsichtsbehördliche Verwarnung ausgesprochen. Hintergrund war, dass das BMI von einem IFG-Antragsteller pauschal die Angabe seiner Postadresse gefordert hatte. Ein Antragsteller hatte sich über die von der Open Knowledge Foundation Deutschland e. V. betriebenen Plattform Frag-den-Staat mit einem IFG-Antrag an das BMI gewandt. Die Plattform bietet Bürgerinnen und Bürgern ein niedrigschwelliges digitales Angebot zur Stellung von IFG-Anträgen gegenüber öffentlichen Stellen. Hierzu erstellt die Plattform eine E-Mail-Adresse, die regelmäßig aus dem Vor- und Nachnamen des Antragsstellers sowie einer Zahlenfolge besteht und über die ein IFG-Antrag elektronisch bei jeweiligen öffentlichen Stelle eingereicht wird. Dabei hat die Open Knowledge Foundation Deutschland e. V. Maßnahmen gegen eine missbräuchliche Verwendung ihrer Plattform getroffen.

Verwaltungsverfahren sind grundsätzlich nicht formgebunden, sondern einfach, zweckmäßig und zügig durchzuführen (§ 10 S. 2 VwVfG). Dabei muss der Bescheid in einem Verfahren nicht zwingend in Papierform ergehen und auch nicht zwangsläufig postalisch übermittelt werden (§ 37 VwVfG). Eine Ausnahme hiervon nach dem IFG, etwa wegen einer notwendigen Drittbeteiligung oder einer Gebührenerhebung, war im konkreten Fall nicht ersichtlich. Ein Bescheid kann also auch per E-Mail an die E-Mail-Adresse eines Antragsstellers bei Frag-den-Staat erfolgen. Dennoch hatte das BMI die weitere Bearbeitung von der Angabe der postalischen Adresse oder der Angabe der E-Mail-Adresse eines kommerziellen Providers abhängig gemacht. Der Antragsteller übermittelte dem BMI daraufhin sowohl seine postalische als auch eine weitere E-Mail-Adresse eines großen kommerziellen Providers. Dabei bat er das BMI aber darum, die Entscheidung möglichst an die angegebene E-Mail-Adresse zu verschicken. Entgegen der Bitte übermittelte das BMI seine Entscheidung an seine Postadresse. Darin wurde dem Antragsteller mitgeteilt, dass die begehrte Information nicht vorhanden sei. Meines Erachtens hätte dies ohne Weiteres an die E-Mail-Adresse des Antragstellers bei Frag-den-Staat übermittelt werden können. Die Anforderung und notgedrungen weitere Aufbewahrung der Anschrift für eine bloße Negativinformation erschien mir unnötig und als Verstoß gegen die Grundsätze der Datenminimierung und Erforderlichkeit.

Die Anfechtungsklage des BMI gegen meine Verwarnung war in der ersten Instanz zunächst erfolgreich. Demgegenüber gab das Oberverwaltungsgericht Nordrhein-Westfalen mir in zweiter Instanz recht und bewertete die Ermessensentscheidung des BMI zur postalischen Versendung als rechtsfehlerhaft. Das BVerwG schloss sich in der Revision nunmehr jedoch der Auffassung des BMI an.[116] Es vertritt die Auffassung, dass die datenschutzrechtliche Erforderlichkeit erst nach der Ermessensentscheidung der Behörde zu bewerten sei. Was datenschutzrechtlich erforderlich sei, richte sich danach, welche Bekanntgabeform die Behörde gewählt habe.

Die Entscheidung des BVerwG sorgt für die Bürgerinnen und Bürger sowie die Bundesverwaltung für mehr Rechtsklarheit und ist insoweit grundsätzlich begrüßenswert. Zugleich kann ich im konkreten Fall aber gerade auch die Perspektive des betroffenen Bürgers verstehen, der eine digitale Plattform nutzen will, aber dann doch seine Postadresse angeben muss, nur um am Ende per Brief darüber informiert zu werden, dass die von ihm begehrte Information gar nicht vorhanden ist. Einfach, zweckmäßig und zügig ist das aus meiner Sicht nicht – und kein gutes Beispiel für die Verwirklichung der Digitalisierungsziele der Bundesregierung. Ich hoffe, dass Behörden vermehrt auf eine bürgernahe und digitale Verwaltung setzen und die Möglichkeit einer digitalen Beantwortung von IFG-Anträgen verstärkt nutzen. Zudem werde ich mich weiterhin für ein niedrigschwelliges und modernes Transparenzrecht einsetzen.

7.2.8 Der neue Dienst „Mein Justizpostfach“

Der Dienst „Mein Justizpostfach“ ermöglicht es Bürgerinnen und Bürgern, Nachrichten und Dokumente rechtsverbindlich elektronisch an angeschlossene Gerichte, Behörden und andere Stellen zu übermitteln. Aus datenschutzrechtlicher Sicht sehe ich bei dem Dienst und der zugrundeliegenden Infrastruktur noch Verbesserungsmöglichkeiten.

Seit Oktober 2023 bietet das Bundesministerium des Innern und für Heimat (BMI) den Dienst „Mein Justizpostfach“ (MJP) an. Dabei handelt es sich um einen kostenlosen Postfachdienst in der BundID (künftig DeutschlandID), der eine Kommunikation mit angeschlossenen Stellen – zum Beispiel Gerichten, Behörden, Rechtsanwältinnen und Rechtsanwälten sowie Notarinnen und Notaren – über die EGVP-Infrastruktur (Elektronisches Gerichts- und Verwaltungspostfach) ermöglicht. Um den Dienst verwenden zu können, müssen sich Bürgerinnen und Bürger mit ihrem elektronischen Personalausweis authentifizieren. Dadurch wird sichergestellt, dass die Identität aller Postfachinhaber geprüft ist, so dass Doku-

116 Urteil des BVerwG vom 20. März 2024, 6 C 8.22, abrufbar unter: https://www.bverwg.de/de/200324U6C8.22.0

mente rechtsverbindlich auf elektronischem Weg an die jeweiligen Empfängerinnen und Empfänger übermittelt werden können.

Das MJP bietet damit einen echten Mehrwert für Bürgerinnen und Bürger, steht exemplarisch aber auch für die Herausforderungen solcher „verteilten Dienste". Damit sind Dienste gemeint, die von den Nutzenden als ein einheitliches Angebot wahrgenommen werden, obwohl sie sich technisch aus mehreren Komponenten zusammensetzen, die ihrerseits von verschiedenen Stellen betrieben werden. Bei dem MJP wird die Postfach-Komponente vom BMI betrieben, der Nachrichtenversand erfolgt aber mithilfe der EGVP-Infrastruktur und mithilfe von Komponenten, die von den Justizverwaltungen des Bundes und der Länder betrieben werden. In solchen Fällen müssen die Anbieter bzw. Betreiber sorgfältig prüfen, wer in welchem Umfang für die Verarbeitung personenbezogener Daten in dem Dienst allein oder gemeinsam verantwortlich ist. Den Nutzenden ist das in den Datenschutzhinweisen durch Benennung der Verantwortlichen und Angaben zu Datenempfängern transparent zu machen, damit sie wissen, welche Stellen die Daten in eigener Verantwortung verarbeiten und gegenüber welchen Stellen sie ihre Rechte ausüben können bzw. müssen. Für das MJP war das nicht ausreichend gewährleistet, als es unmittelbar nach Inbetriebnahme des Dienstes zu einer Datenpanne gekommen ist. Betroffene hatten sich daraufhin an mich gewandt, weil sie auf Grundlage der Datenschutzhinweise nicht erkennen konnten, welche weiteren Stellen für die Verarbeitung ihrer Daten verantwortlich seien, und daher – anders als das BMI – von einer Verarbeitung in alleiniger Verantwortlichkeit des BMI ausgegangen waren. Wie die Verantwortlichkeit beim MJP einzuordnen ist, prüfe ich derzeit.

Datenschutzrechtlichen Handlungsbedarf sehe ich außerdem in Hinblick auf die EGVP-Dienste, die das MJP nutzt, um die Adressierung und den Versand von Nachrichten zu ermöglichen. Die EGVP-Infrastruktur ist ursprünglich für den Nachrichtenversand allein zwischen Gerichten und Behörden entwickelt worden, sah also eine Teilnahme von Bürgerinnen und Bürgern nicht vor. Daher wurde das EGVP originär so konzipiert, dass jeder Postfachinhaber mit einem ausgewählten Datenkranz in ein Verzeichnis eingetragen wird. Diese Verzeichnisdaten können andere Postfachinhaber einsehen. Hieran hat sich durch die Öffnung des Dienstes für Bürgerinnen und Bürger nichts geändert, sodass gegenwärtig unter anderem Vor- und Nachnamen sowie die Anschriften von Bürgerinnen und Bürgern, die ein solches Postfach besitzen, teilweise für Inhaber anderer Postfächer sichtbar sind (also etwa für Gerichte, Behörden, Rechtsanwältinnen und Rechtsanwälte, Notarinnen und Notare). Jedoch sind die Eintragungen für andere Bürgerinnen und Bürger nicht einsehbar. Das gilt unabhängig davon, ob zwischen den Beteiligten eine Kommunikationsbeziehung besteht. Dies sollte mittelfristig geändert werden, sodass Verzeichnisdaten von Bürgerinnen und Bürgern nur noch einsehbar sind, wenn und solange zwischen den konkret Beteiligten eine Kommunikationsbeziehung besteht.

7.2.9 Frühzeitige Einbindung bei geplanter Neuregelung zur Verhütung von Strom- und Gasunterbrechungen

Wenn in Privathaushalten der Strom oder das Gas abgestellt wird, stellt dies die Betroffenen vor große Herausforderungen. Unter welchen Voraussetzungen Strom- und Gasunterbrechungen durch eine Einbindung von Sozialbehörden vermieden werden dürfen, ist in der vom Bundeskabinett beschlossenen Energiewirtschaftsgesetz-Novelle (EnWG) mit umfassender Beratung durch meine Behörde angemessen geregelt worden.

Die Bundesregierung hat am 13. November 2024 den vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) vorgelegten Entwurf eines umfassenden Gesetzes zur Änderung des Energiewirtschaftsrechts im Bereich der Endkundenmärkte, des Netzausbaus und der Netzregulierung beschlossen, die sog. EnWG-Novelle. Die betreffende Neuregelung wurde aufgrund der vorgezogenen Neuwahlen in der laufenden Legislatur nicht mehr verabschiedet.

Eine Teilregelung innerhalb der Novelle soll die Unterbrechung der Energieversorgung bei Haushaltskunden verhindern, die ihre Rechnungen trotz Mahnung nicht begleichen. Energielieferanten sind in diesen Fällen unter bestimmten Voraussetzungen berechtigt, die Energieversorgung vier Wochen nach vorheriger Androhung unterbrechen zu lassen. Die vom Kabinett beschlossene EnWG-Novelle enthält nun unter anderem eine Regelung, die eine Weitergabe von Daten säumiger Haushaltskunden an Sozialbehörden unter engen Voraussetzungen zulässt, um Strom- oder Gasabschaltungen zu vermeiden (§§ 41f und 41g EnWG Regierungsentwurf).

Bei der Erarbeitung dieser Neuregelung wurde meine Behörde bereits vor der regulären Abstimmung zwischen den Ressorts vom BMWK intensiv eingebunden. Denn die geplante Regelung bewegt sich im Spannungsfeld zwischen Datenschutz und dem Schutz der Betroffenen vor Strom- und Gasunterbrechungen. Im Ergebnis gelangten wir aufgrund dieses umfassenden konstruktiven Austauschs zu einer Regelung, die einen angemessenen Ausgleich zwischen den beiden Schutzgütern schafft. Der so entstandene Regierungsentwurf

enthält eine abgestufte Lösung: Zunächst wird Betroffenen ermöglicht, auf freiwilliger Basis in eine Weitergabe ihrer Daten an die örtlich zuständige Sozialbehörde einzuwilligen. Stattdessen ebenso möglich ist der Abschluss einer Ratenzahlungsvereinbarung oder der Vortrag einer besonderen Schutzbedürftigkeit zur Abwendung der Strom- oder Gasunterbrechung. Erst wenn keine dieser Möglichkeiten ergriffen wird und auch keine Begleichung der Rechnung stattfindet, können Energielieferanten bei kurz bevorstehender Strom- oder Gasunterbrechung mit dem Ziel, diese abzuwenden, unter bestimmten Voraussetzungen die örtlich zuständige Sozialbehörde informieren. Das BMWK hat sich damit entsprechend meiner Beratung gegen eine früh greifende gesetzliche Verpflichtung der Energielieferanten zur Einbindung der Sozialbehörden entschieden und den Umfang der Daten, welche zur Verhütung der Stromunterbrechung weitergeleitet werden dürfen, auf das Notwendige beschränkt.

7.2.10 Datenschutz bei der Bundestagswahl

Die Bundestagswahl 2025 fand auf Grundlage eines reformierten Wahlrechts statt. Die Überarbeitung der Bundeswahlordnung (BWO) erfolgte auch mit Blick auf den Datenschutz unter frühzeitiger Inanspruchnahme meiner Beratung.

Bedarf zur Änderung der BWO hatte sich nach der Reform des Bundeswahlgesetzes (BWG) 2023 ergeben. Bei der Überarbeitung der BWO wurde mein Haus durch das Bundesministerium des Innern und für Heimat (BMI) beteiligt. Neben verschiedenen nicht-datenschutzrechtlich motivierten Regelungszielen sollte die BWO insbesondere an die Vorgaben der DSGVO angepasst und der Schutz von Persönlichkeitsrechten z. B. bei Wahlbewerbungen verbessert werden. Hierbei war einem Urteil des Europäischen Gerichtshofs (EuGH) Rechnung zu tragen. Der EuGH hatte 2022 klargestellt, dass die Verarbeitung personenbezogener Daten bei Wahlen nicht vom Anwendungsbereich der DSGVO ausgenommen ist, welche somit grundsätzlich auch unmittelbar bei der Bundestagswahl gilt.[117] Die BWO spiegelte bisher nicht wider, dass sich die Betroffenenrechte direkt aus der DSGVO ergeben, wobei sie im Wahlrecht allerdings spezifisch ausgestaltet werden.

Die Neufassung der BWO zielt auf praktische Verbesserungen des Datenschutzes. Ein verbesserter Schutz von Persönlichkeitsrechten sowie vor potentiellen Gefährdungen ergibt sich für Personen, die sich um Mandate bewerben. So wird bei der Bekanntmachung der Kreiswahlvorschläge künftig statt der Anschrift nur der Wohnort der Bewerberinnen und Bewerber angegeben. Diese begrüßenswerte Maßnahme dient ihrem Schutz. Potentiellen Gefährdern wird es erschwert, die Wohnanschrift auszuspähen. Begrüßenswert ist der Ansatz der BWO, datenschutzrechtlich Verantwortlichen Muster zur Verfügung zu stellen, um betroffene Personen zu informieren. Denn dies kann als Hilfestellung für die Praxis dazu beitragen, ein einheitlich hohes Datenschutzniveau bei den Wahlen und deren Vorbereitung zu gewährleisten. Gegenüber dem BMI wurde eine Überprüfung der neu gefassten Muster insbesondere in Hinblick auf vollständige und verständliche Information angeregt.

Ich freue mich darüber, dass das BMI mein Haus frühzeitig in die Überlegungen zu den geplanten Änderungen eingezogen hat. Meine Mitarbeitenden hatten somit Gelegenheit verschiedene Hinweise zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten einbringen zu können. Ich wünsche mir, dass dieses Beispiel Schule macht und mein Angebot einer frühzeitigen datenschutzrechtlichen Beratung verstärkt wahrgenommen wird.

7.3 Wirtschaft und Finanzen

7.3.1 European Blockchain Sandbox

Reallabore erleichtern und beschleunigen den Transfer von Neuerungen in die Praxis. Sie bieten als Testräume für Innovation und Regulierung Potenziale, die gerade auch für den digitalen Wandel von Wirtschaft und Gesellschaft von Bedeutung sind.

Bereits seit Mitte 2023 nimmt mein Haus auf Einladung der Europäischen Kommission an einem Reallabor zum Thema Blockchain teil (European Blockchain Regulatory Sandbox).

Im Rahmen dieses Reallabors treffen ausgewählte Projekte aus dem Bereich Blockchain mit Aufsichtsbehörden zusammen, um in einem sicheren und vertraulichen Dialog regulatorische Aspekte innovativer Anwendungen von Blockchain und Distributed Ledger Technologien zu diskutieren. Ziel des Projekts ist es, einen Rahmen für Regulierungsbehörden, Aufsichtsbehörden und Blockchain-Innovatoren bereitzustellen, um in einen regulatorischen Dialog einzutreten und Hinder-

117 Urteil des EuGHs vom 20. Oktober 2022, C306/21, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0306&qid=1739620497817

nisse aus rechtlicher und regulatorischer Sicht in einem sicheren und vertraulichen Umfeld zu identifizieren.

- → Für die teilnehmenden Aufsichtsbehörden bietet das Reallabor eine Gelegenheit, Einblicke in neue Anwendungsfälle der Blockchain-Technologie zu bekommen und gleichzeitig den beteiligten Firmen ein besseres Verständnis der rechtlichen Anforderungen im Zusammenhang mit ihren Projekten zu vermitteln. Ich begrüße insbesondere, dass das Reallabor dazu beiträgt, dass Aspekte des Datenschutzes im Sinne des Grundsatzes „Data Protection by Design" in den Projekten bereits in einem frühen Stadium berücksichtigt werden.
- → Für die Beiträge im Rahmen der ersten „Kohorte" des Reallabors erhielt mein Haus im Sommer 2024 zusammen mit vier der anderen teilnehmenden Aufsichtsbehörden den „Most innovative Regulator Award", verliehen von einem Gremium unabhängiger Wissenschaftler verschiedener europäischer Universitäten. Ein Best Practices Report mit Ergebnissen aus der ersten „Kohorte" wurde auf den Webseiten der EU-Kommission veröffentlicht. [118]

Mein Haus nimmt auch an der aktuell laufenden zweiten „Kohorte" der Sandbox teil.

7.3.2 Messengerdienste

Messenger kommen heute in verschiedensten Variationen, Ausführungen und Systemintegrationen vor und sind eins der meist genutzten Kommunikationsmittel. Mir obliegt die datenschutzrechtliche Aufsicht über Messengerdienste von öffentlichen Stellen des Bundes sowie von Messengerdiensten, welche Telekommunikationsdienste sind. Neben Kontrollen zum rechtskonformen Einsatz dieser Dienste hat mein Haus sich mit neuen datenschutzrechtlichen Fragestellungen befasst, welche im Kontext von Interoperabilität entstehen, sowie eine öffentliche Konsultation zum Prüfkatalog Standardized Messenger Audit durchgeführt.

Kontrollen von Messengerdiensten der öffentlichen Stellen des Bundes (BwMessenger & Wire Bund)

Neben kommerziellen, zur privaten und geschäftlichen Kommunikation angebotenen Messengerdiensten bin ich für solche zuständig, die innerhalb der öffentlichen Verwaltung des Bundes eingesetzt werden. Im vorigen Jahr beschäftigten sich meine Mitarbeiterinnen und Mitarbeiter in zwei Kontrollen mit datenschutzrechtlichen Fragen rund um verwaltungsinterne Messengerdienste.

Die eine Kontrolle betraf den Dienst BwMessenger. Diesen entwickelte die Bundeswehr basierend auf dem Open-Source Protokoll Matrix. Er wird in Rechenzentren der Bundeswehr durch die BWI GmbH betrieben. Der Dienst steht Angehörigen der Bundeswehr für die dienstliche Kommunikation zur Verfügung. In meiner Kontrolle untersuchte ich insbesondere, auf welche Rechtsgrundlage die Bundeswehr die Datenverarbeitungen im Zusammenhang mit dem Betrieb des Messengerdienstes gegenüber den Angehörigen der Bundeswehr stützte.

Die Bundeswehr holte hierfür Einwilligungen u. a. ihrer Beschäftigten ein. Meine Mitarbeiterinnen und Mitarbeiter stellten zum einen fest, dass die Einwilligungen nicht wirksam eingeholt wurden. Im Anmeldeprozess wurde durch ein Kästchen eine Zustimmung zu den Nutzungsbedingungen und der Datenschutzerklärung abgefragt. Damit können betroffene Personen die Abgabe einer Einwilligung nicht hinreichend klar von dem Schließen eines Vertrages unterscheiden. Zum anderen stellte ich fest, dass die Einwilligungen auch aus Sicht des Beschäftigtendatenschutzes nicht wirksam waren. Denn bei der Frage der Freiwilligkeit muss die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände berücksichtigt werden, unter denen die Einwilligung erteilt worden ist. § 26 Abs. 2 S. 2 BDSG legt fest, dass eine freiwillige Einwilligung insbesondere dann vorliegen kann, wenn die oder der Beschäftigte infolge der Datenverarbeitung einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder Arbeitgeber und Beschäftigter gleichgerichtete Interessen verfolgen. Als Reaktion auf meine Feststellungen wird die Bundeswehr nunmehr ihre Prüfungen, Informationen und Dokumente beim Einsatz des BwMessengers darauf umstellen, dass die zur Erbringung des Dienstes stattfindenden Datenverarbeitungen zur Erfüllung ihrer öffentlichen Aufgaben und zu Zwecken der Erfüllung von Rechten und Pflichten des Beschäftigungsverhältnisses erforderlich sind.

Die zweite Kontrolle betraf den Dienst Wire Bund und die Frage, ob dieser Dienst einen Telekommunikationsdienst darstellt, wer ggf. Anbieter eines solchen ist sowie welche Stelle die datenschutzrechtliche Verantwortung trägt. Hierfür kontrollierte mein Haus, ob die bereitgestellten Dokumente des BMI und des ITZBund die Rollenverteilungen richtig darstellten. Meine Mitarbeiterinnen und Mitarbeiter stellten fest, dass es sich

118 Best Practices Report der Europäischen Kommission: https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Best+practices+report+2023+-+Part+B

bei Wire Bund in der aktuellen Ausgestaltung der rein verwaltungsinternen Nutzung nicht um einen Telekommunikationsdienst handelt. Datenschutzrechtlich Verantwortliche sind die jeweils den Dienst einsetzenden öffentlichen Stellen des Bundes. Das ITZBund tritt dabei als Auftragsverarbeiter auf.

In beiden Fällen konnte ich feststellen, dass die kontrollierten Stellen hier datenschutzrechtlich gut aufgestellt sind und sich kooperativ zeigten. Es wurde deutlich, dass starke Ambitionen bestehen, die Dienste datenschutzkonform auszugestalten.

Wie bei Besuchen meines Hauses üblich, gab ich im direkten Anschluss an die Kontrollen den Stellen im Rahmen eines offenen Austauschs die Möglichkeit, auch über die Kontrollgegenstände hinausgehende Fragen zu stellen. Dabei konnte ich auch erfahren, welche Themen und Fragestellungen die Akteure aktuell bewegen.

Abhilfemaßnahmen gegen zwei bekannte und vielgenutzte Dienste

Anlässlich von Beschwerden betroffener Personen leitete ich Verfahren gegen zwei bekannte und vielgenutzte Messengerdiensteanbieter ein, die keine Niederlassung in der EU haben. Für Verantwortliche ohne Niederlassung in der EU greift das One-Stop-Shop-Verfahren nicht[119].

Hintergrund der Beschwerden war in beiden Fällen, dass die Anbieter keinen Datenschutzbeauftragten i. S. v. Art. 37 DSGVO benannten und keine deutsche Datenschutzerklärung im Rahmen des Art. 13 DSGVO bereitstellten. Der eine Anbieter benannte zudem keine Vertretung in der EU gemäß Art. 27 DSGVO, der andere informierte nicht über die Kontaktdaten des Verantwortlichen in der Datenschutzerklärung.

Während einer der beiden Messengerdiensteanbieter auf die Anhörung reagierte und eine Datenschutzerklärung in deutscher Sprache und darin die Kontaktdaten des Verantwortlichen bereitstellte, hat mein Haus von dem anderen Anbieter keine Rückmeldung erhalten. Ein Bescheid gegen diesen Dienst ist mittlerweile rechtskräftig.

Hinsichtlich der offenen Punkte, insbesondere der fehlenden Benennung einer Vertretung in der EU und eines/einer Datenschutzbeauftragten, setzt sich mein Haus weiterhin dafür ein, einen rechtskonformen Zustand herzustellen. Dies gestaltet sich bei Diensten schwierig, die keinen Sitz in der EU haben und auf Schreiben meines Hauses nicht reagieren. Gleichwohl wird mein Haus auch in diesen Fällen die zur Verfügung stehenden Mittel einsetzen.

Insbesondere die Verstöße gegen Benennungspflichten von Ansprechpersonen wiegen meines Erachtens schwer, da betroffenen Personen von vornherein die Möglichkeit genommen ist, sich bei einem Verdacht auf Verstöße gegen die Vorgaben der DSGVO und sonstiger Datenschutzvorschriften an den Messengerdiensteanbieter und/oder den/die Datenschutzbeauftragte/n zu wenden, auch um etwa ihre Betroffenenrechte nach Kapitel 3 der DSGVO geltend zu machen. Dies gilt umso mehr, als dass es sich bei der elektronischen Kommunikation über Messengerdienste um einen besonders grundrechtssensiblen Bereich handelt. Nachrichteninhalte betreffen regelmäßig häusliche und private Aktivitäten. Auch Verkehrsdaten können ein umfangreiches Bild über private Sachverhalte der Anwenderinnen und Anwender von Messengerdiensten offenbaren.

Über den Fortgang der Verfahren werde ich zu gegebener Zeit weiter berichten.

Interoperabilität bei Messengerdiensten

Wie in anderen Bereichen digitaler Märkte, haben sich auch bei Messengerdiensten mit der Zeit große Dienstanbieter mit einem signifikanten Marktanteil gebildet. Zum Schutz des Wettbewerbs hat die Europäische Union mit dem Digital Markets Act (DMA) sogenannten Torwächtern spezielle Vorgaben auferlegt.

Eine dieser Vorgaben gegenüber Torwächtern, welche nummernunabhängige interpersonelle Kommunikationsdienste (NIICS) erbringen, stellt nach Art. 7 DMA die Pflicht zur Interoperabilität mit anderen Anbietern von NIICS dar. Nachdem ein Torwächter durch die EU Kommission benannt wurde, muss dieser zeitlich gestaffelt verschiedene Ausbaustufen von Interoperabilität mit anderen Marktteilnehmenden ermöglichen.

Beginnend mit der Möglichkeit, Text-, Bild und Sprachnachrichten zwischen zwei einzelnen Endnutzern auszutauschen, muss dies nach zwei Jahren auch für Gruppen ermöglicht werden. Vier Jahre nach der Benennung, müssen zuletzt Sprach- und Videoanrufe zwischen Gruppen implementiert sein. Darüber hinaus müssen diese Funktionen unter Beibehaltung des bestehenden Sicherheitsniveaus implementiert werden.

Neben großen Herausforderungen bei der technischen Umsetzung werden zudem komplexe Fragen aus Sicht des Datenschutzes aufgeworfen. Beispielsweise stellt

119 siehe hierzu https://www.bfdi.bund.de/DE/BfDI/Inhalte/Datenschutzpfad/DSGVO.html?nn=252102

die anbieterübergreifende Auffindbarkeit (User Discovery) zweier Nutzender von unterschiedlichen Diensten eine schwierige Frage dar. Nicht nur muss der Wille des Nutzenden berücksichtigt und datenschutzkonform abgebildet werden, sondern auch den Datenaustausch, um die Auffindbarkeit technisch zu ermöglichen, gilt es aus Sicht des Datenschutzes zu bewerten. Hierbei sind datenschutzrechtliche Anforderungen mit der technischen Notwendigkeit in Einklang zu bringen, ohne dabei die Praxistauglichkeit des Ansatzes zu verlieren.

Des Weiteren haben die Dienstanbieter zahlreiche Maßnahmen z. B. gegen technischen Missbrauch durch SPAM-Versand oder Bot-Accounts implementiert. Diese teilweise stark optimierten Mechanismen müssen nun auf die neuen Gegebenheiten durch die Interoperabilität angepasst werden. Hier gilt es zum Beispiel, etwaige Forderungen nach weiterem Datenaustausch zwischen den Diensten auf die technische Notwendigkeit und nicht zuletzt datenschutzrechtliche Zulässigkeit zu prüfen.

Da diese Fragestellungen nicht immer nur Datenschutz alleine, sondern auch weitere Themenfelder betreffen, habe ich viele in enger Zusammenarbeit mit anderen Behörden behandelt. Neben dem steten bilateralen Austausch mit dem BSI hierzu, ist das Thema Interoperabilität eines der Schwerpunktthemen des Digital Cluster Bonn. Insbesondere zusammen mit der BNetzA und dem BSI arbeite ich aktiv an gemeinsamen Standpunkten, auch um diese Position in den europäischen Datenschutzausschuss (EDSA) einzubringen.

Doch nicht nur in behördenübergreifender Zusammenarbeit habe ich mich mit diesen Fragestellungen befasst. Im zweiten Jour Fixe Datenschutz und Messengerdienste vom Mai 2024 war das Thema Interoperabilität Schwerpunkt. Zusammen mit den teilnehmenden Behörden und Anbietern von Messengerdiensten wurden insbesondere technische Fragestellungen diskutiert.

Hier zeigte sich, dass es noch ein weiter Weg sein kann, bis die Nutzenden über verschiedenen Messengerdienste hinweg miteinander kommunizieren können.

Öffentliche Konsultation zum Prüfmodell Standardized Messenger Audit – Frontend

Bei der Kontrolle und Überprüfung von Messengerdiensten möchte ich einen einheitlichen Standard anlegen. Um dies zu erreichen, haben meine Mitarbeitenden bereits 2023 die Entwicklung eines standardisierten Prüfkataloges für Frontendanwendungen im Rahmen des EDSA-Formates „Support Pool of Experts“ realisieren können.

Ein einheitlicher Prüfstandard mit ausreichend Flexibilität für individuelle Systeme ist sehr komplex und umfangreich. Um anderen nationalen und internationalen Aufsichtsbehörden, Anbietenden, Nutzenden und Entwicklerinnen und Entwicklern von Messengerdiensten die Möglichkeit zu geben, mein Haus auf mögliche Spezial- und Grenzfälle aufmerksam machen zu können, wurde der Katalog einer öffentlichen Konsultation unterzogen. Dabei war mir wichtig, sowohl Fachanwendende als auch die Zivilgesellschaft einzuladen, sich an der Ausgestaltung von Kriterien für datenschutzkonforme Messenger zu beteiligen.

Für die Teilnahme und zahlreichen Rückmeldungen bedanke ich mich sehr. Diese werden meine Mitarbeiterinnen und Mitarbeiter nun auswerten und die Ergebnisse auf meiner Website veröffentlichen. Sie werden neben den Erfahrungen aus der Praxis in die Überarbeitung und Fortentwicklung des Prüfkatalogs einfließen.

Querverweis:

9.7 Aus dem KI-Workshop des Digital Cluster Bonn

7.3.3 Positionspapier zur Pseudonymisierung von Stromzählerdaten

Mit der Einführung von sogenannten Smart Metern wird nicht mehr nur ein Jahresverbrauchswert ermittelt, sondern mindestens viertelstündlich ein Verbrauchswert erhoben. 36.500 Verbrauchswerte jährlich ermöglichen die Profilierung des Verbrauchsverhaltens und gebieten deshalb einen besonders sorgsamen Umgang.

Die Verwendung von Stromverbrauchsdaten wird mit dem Messstellenbetriebsgesetz (MsbG) datenschutzrechtlich umfassend geregelt. So dürfen nur solche Messsysteme eingesetzt werden, die den hohen Cybersicherheitsanforderungen der Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik genügen, und an die jeweils berechtigten Stellen auch nur Daten in einem Umfang gesendet werden, der für die Erfüllung ihrer jeweiligen Aufgabe erforderlich ist.

Mit der Novellierung des Gesetzes Anfang 2023 wurde festgelegt, dass die im Smart Meter viertelstündlich erhobenen Verbrauchswerte für Planungszwecke und für die Zwecke der Bilanzierung der Strommarktgeschäfte der Stromversorger pseudonymisiert täglich für den Vortag an die jeweils berechtigten Stellen zu versenden sind. Ich habe schon im Gesetzgebungsverfahren deutlich gemacht, dass für eine Pseudonymisierung, die wirksam eine Identifizierung der mit den jeweiligen Verbrauchsprofilen verbundenen Haushalte verhindert, die Daten bereits beim Versand zu pseudonymisieren sind. Das Verfahren zur Pseudonymisierung muss die Bundesnetz-

agentur im Benehmen mit meiner Behörde gemeinsam festlegen.

Im Rahmen der vorbereitenden Gespräche mit der Bundesnetzagentur (BNetzA) hat sich herausgestellt, dass mit einer schnellen Umsetzung aufgrund der Vielzahl der betroffenen Stadtwerke und Netzbetreiber nicht gerechnet werden kann. Mit meinem Positionspapier[120] für eine Festlegung der Bundesnetzagentur nach § 47 Abs. 2 Nr. 13 MsbG zur Pseudonymisierung nach § 52 Abs. 3 MsbG vom 28. Juni 2024 habe ich deutlich gemacht, unter welchen Voraussetzungen in der Übergangszeit die Viertelstundenwerte dennoch für die vorgesehenen Zwecke verwendet werden können. Die wichtigste Voraussetzung ist dabei die strikte organisatorische Trennung der Stellen für die Bilanzierung und Planung von den Stellen, die mit personenidentifizierenden Informationen etwa für eine Rechnungstellung umgehen müssen. Die Position wird von der BNetzA unterstützt.

Die BNetzA hat mir gegenüber dargelegt, dass es nach ihren Plänen durch eine Re-Organisation der Marktregeln zur viertelstündlichen Bilanzierung von Strommengen auf mittlere Sicht nur noch eine, zudem mit der Verarbeitung anschlussbezogener Daten nicht befasste Stelle geben soll. Diese soll dann ihrerseits die anderen Stellen mit akkumulierten und damit nicht mehr anschlussbezogenen Verbrauchszeitreihen zur Erfüllung ihrer Aufgaben versorgen. Dieses Vorhaben begrüße ich sehr, weil mit diesem Ansatz die derzeit gesetzlich festgelegte tägliche Verteilung der Viertelstundenwerte an die jeweils berechtigte Stelle hinfällig und das damit verbundene Risiko missbräuchlicher Datenverarbeitung verringert wird. Die betreffenden gesetzlichen Regelungen könnten mit der Umsetzung des Vorhabens der BNetzA wieder aufgehoben werden.

7.3.4 Untersuchungen von Android-Apps am Beispiel von Kinder-Smartwatches

Im Berichtsjahr wurden tiefergehende technische Erfahrungen zu geeigneten Untersuchungswerkzeugen und -methoden durch einzelne Untersuchungen von Android-Apps und IoT-Geräten gesammelt. Einige Open-Source-Untersuchungswerkzeuge konnten an die eigenen Bedürfnisse angepasst oder um funktionale Erweiterungen weiterentwickelt werden. Weitere Tools, z. B. für Dokumentation und Auswertung der Untersuchungsergebnisse, wurden konzipiert und implementiert.

Laborumgebung

Die Infrastruktur der Laborumgebung stellt dynamisch virtuelle Maschinen als Untersuchungsumgebungen bereit, die zur Untersuchung von IT-Anwendungen und -Hardware eingesetzt werden. Als Virtualisierungslösung kommt ein Open-Source Produkt zum Einsatz. Die virtuellen Maschinen haben freien, ungefilterten Zugang zum Internet; das kann für Untersuchungen wichtig sein, da die übrige IT der Bundesbehörden in den sog. Netzen des Bundes hängen und diese nur über unter Umständen gefilterte Proxys verlassen können. Ein Zugang zum Netz der Laborumgebung wird über eine VPN-Verbindung hergestellt; das Zugriffprotokoll erlaubt auch das Durchreichen lokal angeschlossener USB-Geräte wie etwa Android-Geräte zur Nutzung der ADB oder USB-WLAN-Sticks zur Verwendung als Hotspot an die virtuelle Maschine.

Meine Behörde betreibt seit dem Frühjahr 2023 ein IT-Labor, das derzeit in den Regelbetrieb überführt wird. In der Laborumgebung können die Mitarbeitenden meiner Behörde durch den Einsatz geeigneter Untersuchungswerkzeuge die Datenflüsse von Produkten – wie Apps, Anwendungen oder Geräten – untersuchen.

Mit den gewonnenen Erfahrungen aus den durchgeführten Untersuchungen im Berichtsjahr konnte ein allgemeiner Untersuchungsprozess definiert werden. Ziel ist es, den Prozess im nächsten Jahr weiter zu erproben und zu optimieren, so dass er bei Untersuchungen anderer IoT-Geräten leichter angewandt werden kann. Der Prozess gliedert sich in folgende Phasen:

1. Produktauswahl: Nach einer Marktsichtung erfolgt die Festlegung von Merkmalen und Kriterien zur Auswahl der Produkte, anschließend deren Beschaffung.

2. Prüfungsplanung: Die konzeptionelle Phase umfasst die Definition geeigneter Szenarien und Aktionen sowie eines Katalogs mit den zu untersuchenden Merkmalen und Kriterien für deren Bewertung.

120 Positionspapier vom 28. Juni 2024, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2024/Positionspapier-Pseudonymisierung-Z%C3%A4hlerstandg%C3%A4nge.pdf

3. Prüfungsvorgehen: Die operative Phase umfasst die Vorbereitung und Durchführung der technischen Untersuchung sowie die Dokumentation der Ergebnisse.
4. Auswertung: Bewertung der in Phase 2 festgelegten Merkmale anhand der Bewertungskriterien unter Berücksichtigung der dokumentierten Ergebnisse.
5. Analysebericht: Zielgruppenspezifische Zusammenfassen der Auswertung, z. B. zur Sensibilisierung und Aufklärung der Öffentlichkeit oder zur Erweiterung des bereits in der Datenschutz-Community vorhandenen Wissens zu Untersuchungswerkzeugen und -methoden.

Bei den Untersuchungen einiger der Apps zur Steuerung und Konfiguration von Kinder-Smartwatches ging es insbesondere darum, den technologischen Werkzeugkasten meiner Mitarbeiterinnen und Mitarbeiter zu erproben und weitere Ideen und Hilfsmittel zu entwickeln (Phasen 2 bis 4). Die dabei erarbeiteten, getesteten und bewährten Methoden wurden innerhalb des Wissensmanagements meiner Behörde als funktionierende Anleitungen für alle Mitarbeitenden zur Verfügung gestellt.

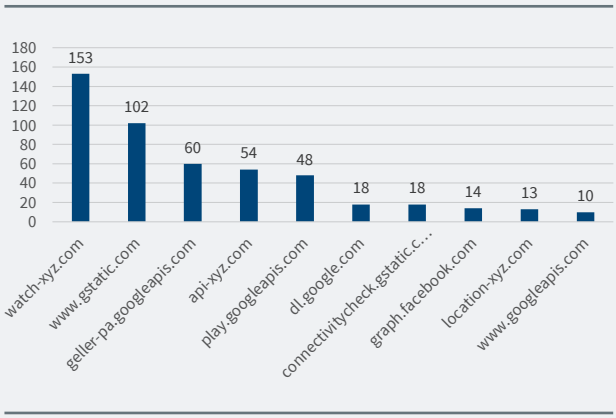
Es ging also nicht darum, einen umfassenden Marktüberblick zu gewinnen oder gar einem konkreten Verdacht auf Datenschutzverstöße bestimmter Smartwatch-Anbieter nachzugehen. Die Ergebnisse werden zur allgemeinen Information der Öffentlichkeit – in Erfüllung einer der Aufgaben der BfDI – verwendet [121].

Zur detaillierten Darstellung des Prozessvorgehens in Phase 2 verfassten die Mitarbeitenden meiner Behörde einen Artikel für die Zeitschrift „Datenschutz und Datensicherheit“. [122]

Untersuchungsergebnis zu dokumentierten Datenflüssen

Die Mitarbeitenden meiner Behörde entwickeln Tools zur Auswertung und Darstellung der Untersuchungsergebnisse, insbesondere der Datenübermittlung. Mit deren Hilfe ist es möglich, aus den dokumentierten Datenflüssen Merkmale, wie die Anzahl der aufgerufenen Endpunkte, die Anzahl der Verbindungen zu den einzelnen Endpunkten, die Größe der übermittelten Pakete usw. zu extrahieren und grafisch darzustellen.

Zur Illustration stellt folgende Abbildung die zehn Endpunkte mit den meisten Verbindungen und die Anzahl der Verbindungen pro Endpunkt dar. Die anbieterspezifischen Endpunkte wurden durch die Zeichenkette „xyz“ ersetzt. Der Datenfluss wurde für eine Kinder-Smartwatch beim Ausführen der Aktion „Chatten und verschicken eines Bildes von der App zur Smartwatch“ aufgenommen. Insgesamt wurden für diese Aktion 67 Endpunkte mit 610 Verbindungen und 4 Cookies identifiziert.



7.3.5 Anforderungen an sichere Videokonferenzdienste

Im vorigen Jahr gab es mehrere Medienberichte zu Sicherheitslücken rund um einen vielgenutzten Videokonferenzdienst. Mein Haus wirkte bei der Aufklärung des Sachverhaltes aus Datenschutzsicht mit und sensibilisierte durch die Veröffentlichung von Sicherheitshinweisen und konkreten Handlungsempfehlungen.

121 Angebot auf der BfDI-Webseite , „Smartwatches für Kinder“, abrufbar unter: https://www.bfdi.bund.de/DE/Buerger/Technische-Anwendungen/Smartwatch/Smartwatch_node.html

122 Der Artikel „Android-App-Untersuchung am Beispiel von Kinder-Smartwatches“ ist abrufbar unter: https://rdcu.be/d1sDC

Egal ob privat oder beruflich: Videokonferenzen sind zu einem wichtigen Werkzeug für Kommunikation und Zusammenarbeit geworden. Umso beunruhigender war es, als Mitte des Jahres über Sicherheitslücken bei einem großen Videokonferenzdienst berichtet wurde. Sicherheitslücken konnten ausgenutzt werden, um einen unberechtigten Zugriff auf Informationen von Besprechungen zu erlangen. Betroffen waren u. a. der Titel des Meetings, Startzeitpunkt und die geplante Dauer, sowie der Name der Person die das Meeting erstellt hatte. Teilweise sei auch eine telefonische Einwahl in Meeting-Räume ohne Eingabe eines Passwortes möglich gewesen. Die Sicherheitslücken wurden sowohl durch systemseitige Anpassungen als auch durch eine Anpassung der Empfehlungen für die betriebsseitigen Grundeinstellungen geschlossen.

Unsichere Videokonferenzdienste sind Einfallstore für Kriminelle – und damit auch eine Gefahr für den Datenschutz. Die Sicherheit einer Videokonferenz ist nicht ausschließlich vom genutzten Videokonferenztool abhängig, sondern auch davon, ob betriebsseitig angemessene Maßnahmen für die jeweilige Konstellation und Inhalt einer Videokonferenz ergriffen werden. Hierbei ist die Nutzung von Passwörtern für den Zutritt in Konferenzräume besonders hervorzuheben. Dies gilt besonders dann, wenn eine telefonische Einwahl ermöglicht wird. Sogenannte Wartelobbys zur Vorabprüfung der Berechtigung zur Teilnahme sind zu empfehlen.

Um den Schutz personenbezogener Daten bei der Verwendung von Videokonferenzen zu gewährleisten, müssen Anbieter die datenschutzrechtlichen und telekommunikationsrechtlichen Anforderungen sicherstellen. Ich habe hierzu die Handreichung „Datenschutzrechtliche Anforderungen an kommerzielle Anbieter von Videokonferenzdiensten“ erarbeitet. Diese ist als Hilfestellung an Anbieter kommerzieller Videokonferenzdienste gerichtet und liefert einen Überblick über wichtige rechtliche und technische Anforderungen. Die Handreichung ist auf meiner Homepage veröffentlicht und soll auch als Gradmesser für zukünftige Kontrollen dienen. [123]

7.3.6 Zusammenarbeit mit anderen Aufsichtsbehörden

Im Berichtsjahr organisierte meine Behörde zwei Treffen zum Informationsaustausch zwischen den IT-Laboren der deutschsprachigen Datenschutzaufsichtsbehörden. Die Treffen waren durch den kollegialen Austausch geprägt und dienten u. a. auch dem Kennenlernen der Verantwortlichen der IT-Labore.

Meine Behörde initiierte gemeinsam mit dem Landesbeauftragten für den Datenschutz Niedersachsen einen Informationsaustausch zwischen den IT-Laboren der deutschsprachigen Datenschutzaufsichtsbehörden. Die Einladung erfolgte über den Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. Im Berichtsjahr fanden zwei Treffen statt – eines am Standort meiner Behörde in Bonn und eines im Verbindungsbüro in Berlin. An beiden Treffen nahmen Mitarbeitende von elf Datenschutzaufsichtsbehörden der Länder, von vier kirchlichen Datenschutzaufsichtsbehörden, des Rundfunkdatenschutzbeauftragten, der Datenschutzstelle Fürstentum Liechtenstein, des Europäischen Datenschutzbeauftragten und meiner Behörde teil.

Zum Beginn wurden die Eckpunkte der Zusammenarbeit festgelegt. Neben dem freiwilligen und kollegialen Austausch sollten die Schwerpunkte der Treffen im Wesentlichen auf konkreten, praktischen Themen der IT-Labore liegen. Dabei sollten am Ende eines Treffens der Inhalt und die Themenverantwortlichen für das jeweils folgende Treffen sowie Termin und Ort bestimmt werden.

Beim ersten Treffen wurden zum einen unterschiedliche technische Ansätze und Tools zur technischen Prüfung von Android-Apps vorgestellt. Zum anderen wurden Prüferfahrungen ausgetauscht und zu einem Prüfprozess zusammengeführt. Dieses Thema wurde dann beim zweiten Termin fortgeführt und abgeschlossen.

Als Schwerpunkte für das zweite Treffen wurde die Prüfung von IoT-Geräten sowie der Aufbau und Betrieb einer Laborumgebung festgelegt. Die Mitarbeitenden meiner Behörde ergänzten das Programm um einen Show-Room, wo die Teilnehmenden die Gelegenheit bekamen, IoT-Geräte und Apps mit PiRogue-Minicomputern und der zugehörigen Tool-Suite zu prüfen. Inhaltlich stellten sie die eigene Untersuchungsmethodik – insbesondere einen Katalog mit zu untersuchenden Merkmalen und Bewertungskriterien – sowie die unterschiedlichen technischen Aufbauten zur operativen Durchführung einer Untersuchung vor.

Die Termine im Frühjahr in Bonn und im Herbst in Berlin waren durch den kollegialen Austausch geprägt und dienten auch dem Kennenlernen der Verantwortli-

123 BfDI-Handreichung „Datenschutzrechtliche Anforderungen an kommerzielle Anbieter von Videokonferenzdiensten“, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2024/Handreichung-DS-kommerzielle-Videokonferenz.html

chen der IT-Labore. Mit den beiden Treffen legte meine Behörde den Grundstein für den informativen Erfahrungsaustausch. Dieses Angebot wurde durch die Datenschutzaufsichtsbehörden sehr positiv aufgenommen und die Organisation für die nächsten beiden Treffen wurde bereits vereinbart.

7.3.7 Altersprüfung in digitalen Diensten

Die Diskussionen um den Einsatz von Methoden zur Altersprüfung in digitalen Diensten nehmen seit der Geltung des Digital Services Acts (DSA) und den Verhandlung über den Entwurf der sogenannten CSA-Verordnung[124] an Fahrt auf. Vor diesem Hintergrund habe ich mich in diesem Jahr intensiv mit der Frage der datenschutzrechtlichen Zulässigkeit von Methoden der Altersprüfung beschäftigt. Zudem habe ich die an den an der Umsetzung des DSA beteiligten deutschen Stellen im Mai 2024 zu einem gemeinsamen Workshop in mein Haus eingeladen und wir haben ein Punktepapier erarbeitet.

Ohne jeden Zweifel ist es wichtig, dass Minderjährige bei der Nutzung digitaler Dienste ausreichend vor Risiken wie Grooming, Mobbing oder der Konfrontation mit ungeeigneten Inhalten geschützt werden und der digitale Raum für sie ein möglichst sicherer Ort ist. Hierfür kommt eine Reihe von Maßnahmen in Betracht. Methoden der Altersprüfung sollten meines Erachtens nicht als Patentlösung gesehen werden.

Der Einsatz von Methoden der Altersprüfung geht regelmäßig mit Datenverarbeitungen einher und bedarf daher einer Rechtsgrundlage. Eine solche kann sich aus einer gesetzlichen Verpflichtung ergeben. Diese kommt allerdings nur für einige digitale Dienste in Betracht. Nämlich beim Zugang zu jugendgefährdenden Inhalten, Glückspielen oder dem Kauf von bestimmten Produkten wie Alkohol, Tabakwaren oder Waffen. Sogenannte Online-Plattformen sind nach dem DSA zu verhältnismäßigen Kinderschutzmaßnahmen verpflichtet. Der DSA enthält indessen keine allgemeine Verpflichtung zum Einsatz von Methoden der Altersprüfung, die mit der Verarbeitung zusätzlicher personenbezogener Daten einhergehen. Gegebenenfalls kann sich eine Pflicht für risikoreiche, von der Europäischen Kommission als solche eingestufte sehr große Online-Plattformen ergeben.

Außerhalb gesetzlicher Verpflichtungen müssen Diensteanbieter auf eine andere Rechtsgrundlage zurückgreifen und hierfür regelmäßig eine Abwägung vornehmen, wenn sie Methoden der Altersprüfung einsetzen wollen. Bei dieser Abwägung müssen sie das Kindeswohl vorrangig berücksichtigen, welches neben dem Schutz vor Risiken auch ein Recht auf Teilhabe und Befähigung in einem digitalen Umfeld sowie die Privatsphäre und informationelle Selbstbestimmung von Kindern umfasst.

Bei der Abwägung, ob eine Methode der Altersprüfung eingesetzt werden kann, muss auch die Effizienz in Anbetracht häufig niedrigschwelliger Umgehungsmöglichkeiten geprüft werden. Nicht selten sind andere Maßnahmen milder und sogar besser geeignet, einen wirksamen Schutz Minderjähriger zu erreichen, wie etwa Content Moderation oder Meldeverfahren. Insbesondere sind strenge standardmäßige datenschutzrechtliche und kindergerechte Voreinstellungen der Dienste wichtig. Dazu gehören insbesondere, dass etwa durch Algorithmen gesteuerte Mechanismen, die eine exzessive Nutzung fördern können, standardisiert unterbunden werden. Auch die mithilfe von Profilbildung der Nutzenden mögliche Personalisierung der Inhalte und Werbung sollte nicht standardisiert erfolgen, um Kinder zu schützen. Das Ausspielen von Werbung basierend auf einer Profilbildung Minderjähriger verbietet Art. 28 Abs. 2 DSA insgesamt. Ferner sollten die Profile nicht öffentlich einsehbar sein und eine Kontaktaufnahme Fremder unterbunden werden.

Im Rahmen der Abwägung muss auch in Betracht gezogen werden, ob Risikominimierungsmaßnahmen nur für Teilbereiche oder einzelne Funktionen, die tatsächlich ein Risiko für Kinder bergen, eingesetzt werden können.

Im Übrigen gelten die allgemeinen Regelungen der DSGVO. Methoden der Altersprüfung, die sensible Daten verarbeiten oder auf einer ausschließlich automatisierten Entscheidung beruhen und als absolute Zugangsschranke fungieren, sind regelmäßig unzulässig. Methoden der Altersprüfung sind ferner grundsätzlich unzulässig, wenn sie mit einer eindeutigen Identifizierung, Profilbildung, Tracking oder diensteübergreifender Verknüpfung der Daten einhergehen. Sie sollten so gestaltet sein, dass sie nur die Information weitergeben, ob Nutzende berechtigt sind, Zugang zu einem Dienst oder bestimmten Inhalten zu erhalten. Es soll nicht die Information weitergegeben werden, ob es sich um einen Minderjährigen handelt oder wie alt die Person ist. Darüber hinaus sollten detaillierte Informationen zu den Methoden und den mit ihnen einhergehenden Datenverarbeitungen bereitgestellt werden, insbeson-

124 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern.

dere um Nutzenden den Unterschied zwischen einer Altersprüfung und einer Identifizierung im Netz deutlich zu machen.

Insgesamt sollten meines Erachtens Methoden der Altersprüfung nur zurückhaltend eingesetzt werden, da sie mit erheblichen gesellschaftlichen Implikationen wie einer Gefährdung von Anonymität bzw. Pseudonymität im Internet und erheblichen Eingriffen in die Grundrechte insbesondere von Kindern und Jugendlichen einhergehen. Diensteanbieter sollten zunächst weniger invasive und womöglich effektivere Maßnahmen zum Schutz von Kindern ergreifen, wie die vorgenannten Maßnahmen datenschutzrechtlicher und kindergerechter Voreinstellungen oder Meldeverfahren.

Mindestens ebenso wichtig wie technische Maßnahmen digitaler Dienste sind gesellschaftlich-politische Maßnahmen, wie eine frühe Sensibilisierung und Aufklärung auch von Erziehungsberechtigten, um Kinder zu einer eigenverantwortlichen altersgerechten Nutzung digitaler Dienste zu befähigen.

Im Mai dieses Jahres lud ich die an der Umsetzung des DSA beteiligten Stellen Bundesnetzagentur, Bundesministerium für Familie, Senioren, Frauen und Jugend, Bundeszentrale für Kinder- und Jugendmedienschutz und der Landesanstalt für Medien Nordrhein-Westfalen zu einem gemeinsamen Workshop ein. In diesem erarbeiteten wir eine gemeinsame Positionierung zum Thema Altersprüfung in digitalen Diensten. Das Punktepapier ist auf meiner Webseite einsehbar. [125]

Querverweise:

4.2.1 Allgemeiner Bericht aus dem EDSA, 5.4.2 Der Digital Service Act und das Digitale Dienste Gesetz

7.3.8 „Chatkontrolle“ versus Grundrechte

Der EU-Verordnungsentwurf zum Auffinden von Material des sexuellen Online-Kindesmissbrauchs (Child sexual abuse material – CSAM) wurde durch den europäischen Gesetzgeber ein weiteres Jahr vorangetrieben. Während der Bericht des EU-Parlaments vom November 2023 die datenschutzpolitisch kritischsten Punkte adressiert, konnten sich die Mitgliedstaaten im Rat der EU auf keine gemeinsame Position einigen. Die bisher vorgeschlagenen Änderungen sind trotz zahlreicher Ideen aus datenschutzpolitischer Sicht weiterhin nicht tragfähig.

Bereits in meinen vorherigen beiden Tätigkeitsberichten hatte ich über die Pläne des Gesetzgebers der Europäischen Union (EU) zur Verabschiedung einer Verordnung zur Prävention und Bekämpfung des sexuellen Online-Kindesmissbrauchs (CSA-VO) berichtet und hierbei datenschutzrechtlich problematische Punkte kritisiert. Der Schutz von Kindern vor Missbrauch ist sowohl offline als auch online ein wichtiges Ziel und als Teil der Grundfesten einer demokratischen Gesellschaft überaus wichtig und unterstützenswert. Dennoch schießen die Pläne des europäischen Gesetzgebers weit über dieses Ziel hinaus und würden den Einstieg in eine anlasslose und flächendeckende Überwachung der privaten Kommunikation bedeuten. Praktisch sieht der im Mai 2022 vorgelegte Verordnungsentwurf der EU-Kommission vor, dass Anbietende von Messenger- und Hostingdiensten durch Aufbrechen von Ende-zu-Ende-Verschlüsselung oder durch Auslesen auf dem Endgerät (sog. Client-Side-Scanning) anlasslos verpflichtet werden, Inhalte ihres Dienstes zu durchsuchen. Ein Durchsuchen soll nach Kommissionsentwurf für Text- und Audionachrichten möglich sein. Gerade das Durchbrechen der Verschlüsselung unterwandert jedoch jede Form von vertraulicher Kommunikation und würde zu Sicherheitslücken führen, welche auch von Kriminellen genutzt werden könnten.

Auch wenn die Befürworter des Gesetzesentwurfs nicht müde werden zu argumentieren, dass der Verordnungsentwurf den Erlass von sog. Aufdeckungsanordnungen nur gegenüber einzelnen Diensteanbietern vorsieht, so hat eine solche Anordnung jedoch zur Folge, dass sämtliche Kommunikation des jeweiligen Dienstes durchleuchtet wird. Bei einem der größten und beliebtesten Messengerdienste beträfe dies allein in Deutschland potentiell etwa 60 Millionen Bürgerinnen und Bürger.

Angepasster Regelungsansatz

Obwohl sich der Innenausschuss des EU-Parlaments am 14. November 2023 auf eine vorläufige Position [126] (Bericht) geeinigt hat, konnte sich der Rat der EU bisher nicht auf eine entsprechende eigene Position (allgemeine Ausrichtung) einigen. Der Bericht des EU-Parlaments sieht einige grundrechtsschonende Positionen und aus meiner Sicht erhebliche Verbesserungen gegenüber dem

125 Punktepapier zur Altersverifikation, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2024/Punktepapier_gem-deut-Position-Altersverifikation.pdf

126 Zusammenfassung der Position des LIBE-Ausschusses zur CSAM-Verordnung, abrufbar unter: https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass-surveillance

Verordnungsentwurf der Kommission vor. Dies gilt insbesondere für die Änderung, Aufdeckungsanordnungen nur gezielt und gegenüber konkret verdächtigen Personen oder Gruppen einzusetzen. Auch wenn es hierbei im Detail noch Verbesserungspotential gibt[127], geht der Bericht in die richtige Richtung.

In den Verhandlungen im Rat der EU haben Präsidentschaften versucht, die teilweise weit auseinanderliegenden Positionen der Mitgliedsstaaten zu vereinen. Die von mir wiederholt vorgetragenen erheblichen datenschutzrechtlichen Bedenken bleiben bestehen.

Einer der Vorschläge durch die belgische Ratspräsidentschaft, die in der ersten Jahreshälfte 2024 den Vorsitz im Rat der EU innehatte, war die Einführung eines sog. Flagging Systems, um die weiterhin teils sehr hohen Fehlerquoten bei den geplanten Technologien, die zum Auffinden des CSA-Materials eingesetzt werden sollen, zu kompensieren. Anstelle Nutzende zusammen mit den gefundenen Inhalten unmittelbar an die zuständigen Strafverfolgungsbehörden zu melden, sollte zunächst ein Marker gesetzt werden und erst bei wiederholtem Anschlagen des Systems eine Meldung an die Behörden erfolgen. Dieses System adressiert jedoch nicht die Kernproblematik und stellt eine wenig effektive Symptombehandlung dar. Bei der Vielzahl der Nachrichten und der Fehlerquote von bis zu 12 Prozent[128] werden Meldungen von zu Unrecht verdächtigten Personen (sog. „False-Positives“) dadurch nicht nennenswert reduziert. Im schlimmsten Fall und bei einfacher Implementierung genügt ein schlichtes wiederholtes Senden eines böswilligen Inhaltes, um das System auszulösen. Ich werde mich weiterhin dafür einsetzen, dass der eigentliche Grundrechtsverstoß – das anlasslose und flächendeckende Scannen aller Nachrichtenhalte – auf ein grundrechtsschonendes Maß angepasst wird, etwa indem die Vorschläge des EU-Parlaments aufgegriffen werden.

Neben dem Flagging System wurde mit anderen Änderungsvorschlägen am Verordnungsentwurf versucht, die Schwere der drohenden Grundrechtseingriffe abzuschwächen. Ein Vorschlag sieht alternativ zum Client-Side-Scanning vor, dass die Nutzenden als Voraussetzung zur Nutzung eines Dienstes in die Überwachung ihrer Kommunikation einwilligen oder den Dienst nur sehr eingeschränkt nutzen können. Abgesehen davon, dass diese Idee die notwendigen Anforderungen an die Freiwilligkeit einer Einwilligung nicht einhalten dürfte, vermindert dieser Vorschlag auch nicht die Kernproblematik einer flächendeckenden und anlasslosen Massenüberwachung.

Nach Übernahme der EU-Ratspräsidentschaft in der zweiten Jahreshälfte 2024 hat Ungarn den anderen EU-Mitgliedstaaten weitere Ideen zum Verordnungsentwurf vorgelegt. Aufbauend auf dem letzten Entwurf der vorherigen Präsidentschaft sollte beispielsweise der Anwendungsbereich von Aufdeckungsanordnungen auf bekanntes CSAM beschränkt, die Risikokategorisierung der Dienstanbieter überarbeitet sowie einigen Dienstanbietern Mitwirkungspflichten zur Entwicklung von Scanningtechnologien auferlegt werden. Diese Einschränkung der Aufdeckungsanordnungen auf bekanntes CSAM und dadurch eine Verringerung der Gefahr von „false positives“ stellt aus Sicht des Datenschutzes zunächst eine positive Entwicklung dar. Jedoch würden Aufdeckungsanordnungen auch durch diesen Vorschlag immer noch nicht verdachtsabhängig und zielgerichtet gegenüber bestimmten Personen oder Personengruppen ergehen, sondern weiterhin stets für alle Nutzenden eines Dienstes gelten. Außerdem sah auch dieser Entwurf weiterhin das Durchbrechen von Ende-zu-Ende-Verschlüsselung und Client-Side-Scanning vor. Insofern sehe ich weiterhin erhebliche datenschutzrechtliche Probleme.

Das Scannen nach unbekanntem CSAM und der gezielten Kontaktaufnahme Erwachsener mit Minderjährigen in Missbrauchsabsicht (Grooming)[129] – und damit das Problem der hohen Fehlerquote der jeweiligen Technologien – sollen nach dem Vorschlag der ungarischen Präsidentschaft zudem nur ausgelagert und in eine übergangsweise CSAM-Interims-VO (Verordnung (EU) 2021/1232) überführt und deren zeitliche Geltung verlängert werden. Die Interims-VO soll Dienstanbietern ein Scannen ermöglichen, das Scannen jedoch nicht

127 Gemeinsame Stellungnahme von 1/2024 von EDSA und EDPS, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12024-legislative-developments-regarding-proposal_en sowie meine Pressemitteilung dazu, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2024/01_CSA-Verordnung.html

128 Europäische Kommission, Arbeitsunterlagen der Kommissionsdienststellen, Bericht über die Folgenabschätzung, Begleitunterlagen zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, SWD(2022) 209 final, Seite 283, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0209

129 Zur Definition von Grooming siehe auch Europäische Kommission, Arbeitsunterlagen der Kommissionsdienststellen, Bericht über die Folgenabschätzung, Begleitunterlagen zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, SWD(2022) 209 final, Seite 3, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0209

verpflichtend machen. Diese Verordnung stellt jedoch keine gültige Rechtsgrundlage zum CSAM-Scanning dar, was die Verordnung in ihrem Erwägungsgrund 10 auch selbst anführt. Dadurch wird die bisher schon bestehende Rechtsunsicherheit lediglich verlängert. Im Ergebnis hat es deshalb auch der ungarische Vorschlag zu keiner Einigung im Rat geschafft.

Ich freue mich sehr darüber, dass die Bundesregierung bislang an ihren roten Linien festgehalten hat und sich im Rat der EU für eine starke Anpassung des Verordnungsvorschlages einsetzte. So hat sich die Bundesregierung zum Beispiel im April 2023 kritisch gegen viele Punkte des Verordnungsentwurfs positioniert und ihre Zustimmung zum aktuellen Ratsentwurf von einer Änderung der wesentlichen Kritikpunkte abhängig gemacht. Im aktuellen Berichtsjahr hat die Bundesregierung an diesen Kritikpunkten weiterhin festgehalten und damit mit dazu beigetragen, dass ein grundrechtswidriger Verordnungsentwurf nicht verabschiedet wird. Nun kommt es darauf an, dass die Bundesregierung auch in der 21. Wahlperiode Kurs hält. Ich biete der Bundesregierung für einen grundrechtschonenden Weg zur Verwirklichung des von mir ausdrücklich unterstützen Ziels der Bekämpfung von Kinderpornographie der CSA-VO gerne weiter meine aktive Beratung an.

Ich empfehle dem Deutschen Bundestag, gegenüber der Bundesregierung und dem EU-Gesetzgeber auf eine erhebliche, grundrechtskonforme Überarbeitung des Verordnungsentwurfs zur Chatkontrolle im Sinne des EP-Berichts von November 2023 zu drängen, der eine durchgehende Ende-zu-Ende-Verschlüsselung gewährleistet, ein Auslesen von Nachrichten auf dem Endgerät (Client-Side-Scanning) ausschließt, die deutschen und europäischen (Kommunikations-)Grundrechte wahrt und ein flächendeckendes und anlassloses Auslesen privater Kommunikation verbietet oder anderenfalls darauf hinzuwirken, den Verordnungsentwurf insgesamt abzulehnen.

7.3.9 Zustellung in automatisierte Paketautomaten nach dem neuen Postgesetz

Mit dem neuen Postgesetz (PostG) sind erstmals genaue Vorgaben für Modalitäten der Zustellung von Briefen und Paketen in Kraft getreten, die für alle Postdienstleistungsunternehmen gelten. Empfänger von Postsendungen können Dienstleister so nun insbesondere bei der Zustellung von Paketen anweisen, die Sendungen etwa in anbieterneutrale automatisierte Stationen einzulegen. Gleichzeitig muss nach dem Gesetz der Zustellung in einer anbietereigenen Station widersprochen werden können, wenn dies von der betroffenen Person nicht gewünscht wird.

Am 19. Juli 2024 ist mit dem Postrechtsmodernisierungsgesetz ein vollständig überarbeitetes neues PostG in Kraft getreten. Damit traten neben dem bestehenden PostG auch die Post-Universaldienstleistungsverordnung (PUDLV), die Postdienstleistungsverordnung (PDLV) und das Postsicherstellungsgesetz außer Kraft. Diese Regelungen sind in großen Teilen mit in das neue PostG aufgenommen bzw. unverändert übertragen worden. So auch die für mich besonders relevanten zentralen Normen §§ 67–71 PostG, die datenschutzrechtliche Regelungen enthalten.

Neu eingeführt wurden mit §§ 12 und 13 PostG Vorschriften, die genau vorgeben, wie Brief- und Paketsendungen zugestellt werden sollen. Vorgaben hierzu gab es bisher lediglich für Universaldienstbetreiber oder marktbeherrschende Anbieter von Postdienstleistungen in PUDLV und PDLV. Nunmehr gelten diese Regelungen in deutlich erweiterter Form für alle Postdienstleistungsunternehmen.

So haben Empfänger von Paketen nach § 13 Abs. 2 Nr. 2 PostG u. a. das Recht, Postdienstleister anzuweisen, Pakete in eine anbieterneutrale automatisierte Station zu verbringen. Dem müssen Unternehmen nur dann nicht nachkommen, wenn eine Zustellung in einer solchen Station aus vom Anbieter zu vertretenden Gründen nicht erfolgen kann.

Gleichzeitig hat sich meine Behörde im Rahmen des Gesetzgebungsverfahrens dafür eingesetzt, dass Menschen, die automatisierte Paketstationen nicht nutzen wollen oder können, eine Paketzustellung in solche Stationen verhindern können. Zwar dürfen Postunternehmen Pakete nach dem neuen PostG grundsätzlich auch ohne Vereinbarung in eigene Stationen verbringen, wenn ein Empfänger an der Zustelladresse nicht angetroffen wurde und eine andere Form der Zustellung nicht erfolgen konnte. Nach § 13 Abs. 3 S. 3 PostG muss es jedoch möglich sein, einem solchen Paketempfang einmalig oder dauerhaft zu widersprechen, wenn diese Stationen nur mit einem technischen Gerät des Empfängers, z. B. dem eigenen Smartphone, genutzt werden können. Zusätzlich müssen betroffene Personen vom jeweiligen Anbieter über dieses Widerspruchsrecht nach § 13 Abs. 3 S. 4 PostG transparent informiert werden.

Es wäre aus meiner Sicht bürgerfreundlicher gewesen im PostG zu regeln, dass Pakete nur dann in automatisierten Paketstationen zugestellt werden, wenn die Empfangsperson dies wünscht. Das im parlamentarischen Verfahren eingefügte Widerspruchsrecht ermöglicht jedoch, dass Menschen, die kein Smartphone nutzen

können oder keine entsprechende App auf ihr Smartphone herunterladen wollen, auch weiterhin Pakete ohne Anwendung zusätzlicher technischer Hilfsmittel empfangen können.

7.3.10 50. Jour fixe Telekommunikation

Seit 25 Jahren lädt mein Haus zum Jour fixe Telekommunikation ein. Der Jour fixe dient dem Austausch mit der Telekommunikations-Branche zu aktuellen datenschutzrechtlichen Themen.

Ein schönes Jubiläum: Im Herbst 2024 fand der 50. Jour fixe Telekommunikation statt. Im halbjährlichen Rhythmus dient er dem Austausch mit der Telekommunikations-Branche zu aktuellen datenschutzrechtlichen Themen. Der Kreis der Teilnehmenden setzt sich insbesondere aus betrieblichen Datenschutzbeauftragten von Telekommunikations-Unternehmen und aus Vertreterinnen und Vertretern der Branchenverbände zusammen. Auch andere Bundesbehörden nehmen regelmäßig teil, etwa verschiedene Ministerien, die Bundesnetzagentur oder das Bundesamt für Sicherheit in der Informationstechnik.

Dialog und Austausch waren von Anfang an der Leitgedanke des Jour fixe. Bei Gesprächsformaten wie diesen gewinnen alle Seiten. Für mich ist er wichtig, weil er sich positiv auf meine Beratungs- und Kontrolltätigkeit wirkt. Denn die Auswirkungen meiner Aufsicht können hier unmittelbar diskutiert werden. Wie wirken geplante Rechtsvorhaben, wie können neue Vorgaben datenschutzkonform operationalisiert werden? Bei anstehenden Beratungs- und Kontrollbesuchen in den Unternehmen können meine Mitarbeiterinnen und Mitarbeiter dann direkt auf den Ergebnissen des Jour fixe aufbauen.

Dauerbrenner an Themen waren in den vergangenen Jahren u. a. die Vorratsdatenspeicherung und die Folgen des Schrems II-Urteils des Europäischen Gerichtshofs. Bürgerbeschwerden, die mich im Bereich Telekommunikation erreichen, drehen sich schwerpunktmäßig um die Ausübung von Betroffenenrechten, insbesondere um das Recht auf Datenauskunft. Auch dieses Thema stand daher wiederholt im Fokus des Jour fixe – und wird es sicher auch in Zukunft tun. Der Umfang und die Grenzen des Rechts auf Auskunft werden durch die Gerichte laufend konkretisiert. Deshalb sollen neue Urteile zeitnah mit der Branche erörtert werden. Dann können Anfragen der Kundinnen und Kunden von den Unternehmen rechtssicher beantwortet werden, sodass eine Beschwerde bei meiner Behörde im Idealfall gar nicht erst erforderlich ist.

Die mit der Branche und den teilnehmenden Behörden erarbeiteten Positionen werden oft in kompakter Form veröffentlicht. Diese Publikationen können die Datenverarbeitung in den Unternehmen dauerhaft prägen. Der Leitfaden meines Hauses zur datenschutzgerechten Speicherung von Verkehrsdaten[130] aus dem Jahr 2012 ist ein solches Beispiel. Ein weiteres ist meine „Position zu Auskunftsverlangen gegenüber Telekommunikationsdienstleistern“.[131]

Das Erfolgsmodell des Jour fixe Telekommunikation werde ich weiterführen. Das Feedback aus der Branche lässt erkennen, dass auch dort großes Interesse an einer Fortsetzung besteht.

7.3.11 Kein KI-Training bei Meta

Meta informierte Datenschutzbehörden im Sommer 2024, dass es Daten seiner Nutzenden für Zwecke des KI-Trainings verwenden möchte. Nach vielen kritischen Fragen durch mich und meine europäischen Kolleginnen und Kollegen hat Meta das angekündigte KI-Training bis auf weiteres ausgesetzt.

Meta kündigte im Juni 2024 an, künftig KI-Training mit Nutzendendaten aus seinen Diensten Facebook, Instagram und WhatsApp betreiben zu wollen. Die Auswertung der Nutzendendaten wollte Meta hierbei auf die Rechtsgrundlage des berechtigten Interesses (Art. 6 Abs. 1 lit. f) DSGVO) stützen. Es stellten sich hierbei viele kritische Fragen: Zum Beispiel, ob die Auswertung zu KI-Trainingszwecken von der Rechtsgrundlage des berechtigten Interesses gedeckt ist. Oder ob dritte Personen, die von Posts von Meta-Nutzenden betroffen sind, die zum KI-Training verarbeitet werden, transparent über die geplante Datenverarbeitung informiert wurden. Unklar blieb auch bis zuletzt, welche Daten Meta vom Messengerdienst WhatsApp für sein KI-Training verwenden wollte, insbesondere da Kommunikationsinhalte wegen der Ende-zu-Ende-Verschlüsselung nicht ausgelesen werden können.

Nachdem meine europäischen Kolleginnen und Kollegen aus dem Europäischen Datenschutzausschuss (EDSA) und ich der federführend zuständigen irischen Datenschutzaufsichtsbehörde (DPC) diverse kritische Fragen übermittelt hatten, die die DPC dann an Meta weiterleitete, entschied sich Meta, das geplante KI-Trai-

130 24. TB Nr. 6.7

131 BfDI-Position zu Auskunftsverlangen gegenüber Telekommuniaktionsdienstleistern, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Datenschutzpraxis/Auskunftsrecht_Telekommunikationsanbieter.html

ning bis auf weiteres zu pausieren. Eine ausführliche Antwort auf die von mir und meinen europäischen Kolleginnen und Kollegen gestellten Fragen durch Meta steht weiterhin aus.

7.3.12 Abomodelle bei großen Online-Plattformen

Ausgelöst durch ein Urteil des Europäischen Gerichtshofs (EuGH) haben die Diskussionen des Europäischen Datenschutzausschusses (EDSA) zu „Consent or Pay"-Modellen, mit denen datenschutzrechtliche Einwilligungen eingeholt werden sollen, erhebliche Aufmerksamkeit auf sich gezogen. Zum Einsatz solcher Modelle bei großen Online-Plattformen zu Zwecken verhaltensorientierter Werbung hat sich der EDSA im Berichtsjahr im Rahmen einer Stellungnahme geäußert.

Monatlich ein Entgelt zahlen oder das eigene Surfverhalten preisgeben – vor diese Wahl stellen immer mehr digitale Dienste ihre Nutzenden. Die Anbieter der Dienste wollen aufgrund der Einwilligung ihrer Nutzenden personalisierte Werbung anzeigen und so den Dienst finanzieren. In der Praxis stimmen die allermeisten Nutzenden auch einer umfangreichen Verarbeitung zu, wenn sie lediglich die Alternative haben, ein Abo abzuschließen.[132] Dabei führt das Tracking in vielen Fällen zu einer ganz erheblichen und umfangreichen Erfassung und Auswertung des Nutzerverhaltens im digitalen Raum, die nicht nur Folgen für die Grundrechte einzelner Nutzender, sondern auch für die gesamte Gesellschaft hat. So kann etwa die Personalisierung von Werbung und Inhalten durch Algorithmen zur Bildung sogenannter Filterblasen führen. Consent or Pay-Modelle bergen die Gefahr, dass Privatsphäre- und Datenschutz zu Gütern werden, die Personen vorenthalten sind, die es sich leisten können.

Der EuGH beschäftigte sich in seinem Urteil vom 4. Juli 2023 mit der Rechtmäßigkeit von Datenverarbeitungen zu Zwecken verhaltensorientierter Werbung. Der Gerichtshof bezweifelte, ob im vorgelegten Fall die Praxis unter eine andere Rechtsgrundlage als die Einwilligung fallen könnte. Im Zuge dessen äußerte der EuGH in einem obiter dictum (lat. „nebenbei Gesagtes"), Nutzende müssten „die Freiheit haben, im Zuge des Vertragsabschlusses die Einwilligung in bestimmte Datenverarbeitungsvorgänge, die für die Erfüllung des Vertrags nicht erforderlich sind, einzeln zu verweigern, ohne dazu gezwungen zu sein, auf die Nutzung des vom Betreiber des sozialen Online-Netzwerks angebotenen Dienstes vollständig zu verzichten, was bedingt, dass ihnen, gegebenenfalls gegen ein angemessenes Entgelt, eine gleichwertige Alternative angeboten wird, die nicht mit solchen Datenverarbeitungsvorgängen einhergeht".[133]

Vor dem Hintergrund dieses EuGH-Urteils ersuchten die niederländische und norwegische sowie die Hamburger Aufsichtsbehörde den EDSA um eine Stellungnahme nach Art. 64 Abs. 2 DSGVO zur Wirksamkeit datenschutzrechtlicher Einwilligungen bei großen Online-Plattformen unter „Consent or Pay"-Modellen. Dies sind Modelle, in denen Nutzende entweder in die Verarbeitung ihrer personenbezogenen Daten für Zwecke der verhaltensorientierten Werbung einwilligen oder ein Entgelt zahlen müssen, um den jeweiligen Dienst nutzen zu können.

Mit einem Antrag nach Art. 64 Abs. 2 DSGVO können Aufsichtsbehörden, der Vorsitz des EDSA oder die Kommission beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom EDSA geprüft wird. Der EDSA muss seine Stellungnahme dann innerhalb von acht Wochen abgeben, wobei diese Frist angesichts der Komplexität einer Angelegenheit um weitere sechs Wochen verlängert werden kann – wie in diesem Verfahren geschehen.

In seiner Stellungnahme[134] behandelt der EDSA die Wirksamkeit von Einwilligungen in Datenverarbeitungen zu Zwecken verhaltensorientierter Werbung bei „Consent or Pay"-Modellen großer Online-Plattformen. Der EDSA problematisiert die Freiwilligkeit der Einwilligung, insbesondere hinsichtlich der Nachteile bei einer Ablehnung (Zahlung eines Entgelts oder Nichtnutzung), Lock-in und Netzwerkeffekten, Machtungleichgewichten zwischen Anbietern und Nutzenden sowie der Konditionalität (d. h. der Frage, ob für den Zugang zu Waren oder Dienstleistungen eine Einwilligung erforderlich ist, obwohl die Verarbeitung für die Erfüllung des Vertrags nicht erforderlich ist). Ferner beschäftigt sich der EDSA mit der Frage, wann eine vom Anbieter bereitgestellte

132 siehe etwa die Eigenangaben von Spiegel Online, abrufbar unter https://devspiegel.medium.com/wie-unser-pur-angebot-f%C3%BCr-werbefreies-lesen-ankommt-f92abaa0640d oder von contentpasst, siehe Morel/Santos/Fredholm/Thunberg, Legitimate Interest is the New Consent – Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls, Seite 3, abrufbar unter: http://arxiv.org/pdf/2309.11625

133 Urteil des EuGHs vom 4. Juli 2023, C-252/21, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0252&qid=1739628145948

134 EDSA Stellungnahme 08/2024, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_de

(ggf. entgeltliche) Alternative ohne Einwilligung in die Datenverarbeitung gleichwertig ist, sowie mit weiteren Anforderungen der Einwilligung wie Granularität, Spezifität oder Informiertheit.

Der EDSA kommt zu dem Ergebnis, dass es großen Online-Plattformen in den meisten Fällen nicht möglich sein wird, die Anforderungen der DSGVO an eine wirksame Einwilligung zu erfüllen, wenn sie Nutzende nur vor die binäre Wahl stellen, entweder in die Verarbeitung personenbezogener Daten für Zwecke der verhaltensorientierten Werbung einzuwilligen oder ein Entgelt zu zahlen. Große Online-Plattformen sollten daher in Erwägung ziehen, eine weitere kostenlose Alternative ohne verhaltensorientierte Werbung anzubieten, z. B. in Form von Werbung, bei der weniger (oder keine) personenbezogene Daten verarbeitet werden.

Nach Abschluss der Stellungnahme wurde der Key Provisions Experts Subgroup des EDSA das Mandat erteilt, weitergehende Leitlinien zum Thema „Consent or Pay" auch bei dem Einsatz durch andere Verantwortliche als große Online-Plattformen und zu anderen Verarbeitungszwecken als verhaltensorientierter Werbung zu erarbeiten.

Die weiteren Diskussionen werden zeigen, ob und wie „Consent or Pay"-Modelle in anderen Zusammenhängen für wirksame Einwilligungen genutzt werden und ein Finanzierungsmodell für digitale Dienste sein können. Je mehr Dienste solche Modelle einführen, desto dringender wird die Frage, inwieweit Nutzende ihren Privatsphäre- und Datenschutz im Digitalen künftig nur gegen Entgelt gewährleisten können. Ich werde mich an diesen Diskussionen weiterhin aktiv beteiligen.

7.4 Sicherheit

7.4.1 Umsetzung des Smart-Borders-Programms der EU durch die Grenzkontrollbehörden

Die für 2024 geplante Inbetriebnahme der europäischen Grenzkontrollsysteme Entry-Exit-System (EES) und European Travel and Authorization System (ETIAS) musste kurzfristig erneut verschoben werden. Die Vorbereitungen bei den national zuständigen Behörden laufen, insbesondere bei der Bundespolizei. Ich habe den Implementierungsprozess im Berichtszeitraum weiter begleitet.

Mit ihrem Smart-Borders-Programm will die EU-Kommission den Kontrollprozess an den Außengrenzen zunehmend automatisieren und digitalisieren. Neben der Anpassung und Verknüpfung bereits bestehender Datenbanken ist auch die Einrichtung von zwei neuen Systemen vorgesehen. Mein Haus begleitet die geplanten Änderungen seit Jahren kritisch.[135]

Zwei dieser Systeme sollten ursprünglich 2024 an den Start gehen:

Mit dem EES soll das händische Stempeln der Reisepässe weitgehend entfallen, stattdessen wird künftig bei Einreise in den Schengen-Raum zu jedem betroffenen Drittstaatsangehörigen ein sog. EES-Dossier angelegt. Die gespeicherten Datensätze umfassen neben Stammdaten (Name, Geburtsdaten etc.) auch Fingerabdrücke und Lichtbilder der Person. Außerdem wird das Datum des Grenzübertritts erfasst und gleichzeitig automatisch der zulässige Aufenthaltszeitraum berechnet.

Das ETIAS betrifft von der Visumspflicht befreite Drittstaatsangehörige, die in Zukunft vor Reiseantritt in den Schengen-Raum einen Antrag auf Reisegenehmigung stellen müssen. Die Anträge werden im Zentralsystem automatisch mit anderen Datenbanken abgeglichen, im Trefferfall entscheidet die sog. nationale ETIAS-Stelle (in Deutschland das Bundespolizeipräsidium) über die Erteilung der Genehmigung.

Das EES sollte planmäßig nach den beiden sportlichen Großveranstaltungen im Sommer 2024 (Fußball-EM und Olympische Spiele) in der zweiten Jahreshälfte in Betrieb genommen werden, das ETIAS sollte ein halbes Jahr später folgen. Im September meldeten Deutschland, Frankreich und die Niederlande an die zuständige EU-Kommissarin, mangels ausreichender Testmöglichkeiten nicht für eine Inbetriebnahme der Systeme bereit zu sein, weshalb sich der Start nun weiter verzögert.

Die Bundespolizei ist mit der Implementierung der Systeme in die – heute schon teilweise automatisiert ablaufenden – Grenzkontrollprozesse befasst. Neben der Schaffung und Verknüpfung neuer Schnittstellen sowie der Integration in bereits bestehende Grenzkontrollanwendungen sind auch organisatorisch Anpassungen an Prozessen erforderlich, die Mitarbeitenden müssen sensibilisiert und im Umgang mit den Systemen geschult werden.

Auf mein Haus kommen als Aufsichtsbehörde neue Aufgaben zu, in den zugrundeliegenden EU-Verordnungen sind etwa regelmäßige Pflichtkontrollen im Umgang mit EES und ETIAS vorgesehen. Hinzu kommt eine Pflicht zur Veröffentlichung von Statistiken über den Eingang

135 27. TB Nr. 1.3

und die Bearbeitung von Anträgen zu Betroffenenrechten, die die zuständigen nationalen Stellen – das Bundesverwaltungsamt bzw. die Bundespolizei – an mich melden müssen.

Bereits 2023 haben meine Mitarbeitenden sich bei einem Informationsbesuch am Flughafen Düsseldorf einen Überblick über die Umsetzung der neuen europäischen Anforderungen verschafft. Hierbei konnten z. B. auch die für den EES-Registrierungsprozess vorgesehenen Self-Service-Terminals in Augenschein genommen werden.

2024 hat mich die Bundespolizei im Rahmen des Anhörungsverfahrens zu mehreren Errichtungsanordnungen nach § 36 Bundespolizeigesetz beteiligt, die die Implementierung der genannten Änderungen in die Grenzkontrollanwendungen der Bundespolizei betreffen. Hier konnte aus Datenschutzsicht noch der ein oder andere Punkt nachgeschärft werden, mein Haus wird die Entwicklungen in diesem Bereich weiter kritisch verfolgen, beratend begleiten und den Umgang mit den Systemen auch im Wege der neuen Pflichtkontrollen überprüfen.

7.4.2 OSINT-Beobachtungen im Internet

Bereits in meinem vorherigen Tätigkeitsbericht hatte ich unter der Überschrift „Internetrecherchen für die nationale Sicherheit – Auch hier gibt es Grenzen!" darüber berichtet, dass speziell Nachrichtendienste die Beobachtung des Internets als wichtiges Mittel ihrer Arbeit ansehen, aber auch hier das informationelle Selbstbestimmungsrecht zu beachten ist.[136] Dies gilt ebenso für Polizei- und Strafverfolgungsbehörden. Das Thema ist ein Dauerbrenner als Arbeitsmittel bei den Sicherheitsbehörden, aber auch in meiner Kontrolltätigkeit.

Für alle Sicherheitsbehörden stellt die sogenannte OSINT-Recherche (OSINT steht für „Open Source Intellligence"), also die Sammlung und Auswertung von öffentlich zugänglichen Daten im Internet, ein wichtiges Instrument dar. Faktisch sind viele Informationen, inklusive personenbezogener Daten, im Internet viel einfacher zu erlangen als in der Realwelt. Das hängt nicht nur mit Technikentwicklungen und deren Verbreitungsgrad zusammen, sondern mit dem Kommunikationsverhalten vieler Menschen. Im vermeintlichen Schutz einer anonymen Umgebung ist dies anders als im direkten Gespräch und es werden erstaunlich freizügig Inhalte mit Personen ausgetauscht, die man noch nie getroffen hat. Chats werden oft wie ein flüchtiges Gespräch genutzt, können aber noch viel später eingesehen werden und sind mitunter für einen weitaus größeren Kreis als angenommen einsehbar. Das gilt auch für Profile in sozialen Netzwerken, z. B. Fotos, Hinweise auf Hobbies, die berufliche Tätigkeit oder Familienangehörige. Was also im Sinne von OSINT frei zugänglich ist, ist mitunter nicht deckungsgleich mit beispielsweise Online-Ausgaben von Printmedien, die für eine breite Öffentlichkeit gedacht sind. Vielfach hat sich in Abgrenzung zu traditioneller Recherche in Publikationen daher der Begriff „Social Media Intelligence" (SOCMINT) im Fall sozialer Netzwerke etabliert, weil sich spiegelbildlich die Informationsgewinnung der Sicherheitsbehörden an diese Realität anpassen musste.

Angesichts der Vielfalt von Internetdiensten kann die Grenze, ab wann ein Eingriff in das Recht auf informationelle Selbstbestimmung so schwerwiegend wird, dass der Rückgriff auf die Generalklausel nicht mehr möglich ist und es einer spezialgesetzlichen Grundlage bedarf, nur für den jeweiligen Einzelfall beantwortet werden. Ob z. B. die Ermittlungsgeneralklausel der Strafprozessordnung, die der Staatsanwaltschaft „Ermittlungen jeder Art" erlaubt, im Einzelfall auch tatsächlich jede Art des Eingriffs in das Recht auf informationelle Selbstbestimmung rechtfertigt, darf bezweifelt werden. Ich berate deshalb sowohl im Gesetzgebungsprozess als auch in der Rechtsanwendung bei den von mir kontrollierten Stellen intensiv zu dieser Frage.

Polizei- und Strafverfolgungsbehörden des Bundes

Vor dem Hintergrund der schwierigen Abgrenzung der Eingriffsintensität haben sich meine Mitarbeitenden umfangreich über die verschiedenen Ermittlungsinstrumente beim Bundeskriminalamt informiert. Ferner konnte in Abstimmung mit der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen ein Informationsbesuch bei der Zentral- und Ansprechstelle Cybercrime der Staatsanwaltschaft Köln durchgeführt werden. In einem umfangreichen Austausch konnten alle Beteiligten tatsächliche und rechtliche Probleme zum Einsatz von OSINT-Recherchen bei der Strafverfolgung diskutieren. Diese Erkenntnisse fließen in meine Kontrolltätigkeit ein.

Nachrichtendienste des Bundes

Auf Einladung der Bundeswehruniversität München zum „OSINT-Forum 2024" hat meine Behörde einen Vortrag zu den datenschutzrechtlichen Anforderungen an OSINT im nachrichtendienstrechtlichen Kontext

136 32. TB Nr. 7.3

gehalten. Im konstruktiven Austausch mit ebenfalls eingeladenen Vertreterinnen und Vertreter von Behörden und Wirtschaftsunternehmen wurde deutlich, dass sich die konkreten OSINT-Datenverarbeitungen je nach Anwendung und Zweck massiv unterscheiden. Gleichwohl eint die unterschiedlich ausgestalteten OSINT-Datenverarbeitungen, dass es an klaren gesetzlichen Regelungen dahingehend fehlt, wann und zu welchem Zweck welche OSINT-Rechercheform zur Erkenntnisgewinnung und -verdichtung betrieben werden darf. Unklare rechtliche Vorgaben sorgen auf Anwenderseite für Rechtsunsicherheit und gefährden so die Einhaltung datenschutzrechtlicher Standards.

Im Berichtsjahr habe ich außerdem beim BND unterschiedliche Kontroll- und Beratungsbesuche durchgeführt, die auch an eine Beanstandung aus dem Jahr 2023 wegen einer Datenverarbeitung ohne ausreichende Rechtsgrundlage angeknüpft haben. Auch das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für den Militärischen Abschirmdienst haben mit der Aufklärung von öffentlichen Daten im Internet weiterhin einen wichtigen Schwerpunkt ihrer Arbeit. Ich diskutiere mit den Behörden dabei kritisch, ob sich bei der steten Weiterentwicklung und Diversifizierung von Internetdiensten in allen Fällen die Nachrichtendienste ausschließlich auf allgemeine Befugnisse zur Recherche öffentlicher Daten stützen können. Auf der praktischen Seite benötigen die Nachrichtendienste für ihre Tätigkeit anerkanntermaßen in diesem Umfeld adäquate technische Lösungen, um die Menge an unstrukturierten Daten zu beherrschen. Bei meiner Kontrolle und Beratung prüfe ich diese neu entstehenden Dateien insbesondere in deren Anwendung im Fall sozialer Netzwerke mit einem besonderen Augenmerk. So hatte ich bereits im vergangenen Tätigkeitsbericht über den geplanten Einsatz einer Datei beim BfV zur Recherche in sozialen Netzwerken berichtet. Diese Datei wurde aus verschiedenen Gründen im Ergebnis nicht eingeführt.

Internetrecherche von mitwirkenden Behörden in der Sicherheitsüberprüfung

Zudem führte ich beim BfV einen Kontroll- und Beratungsbesuch zur Internetrecherche des BfV als mitwirkende Behörde im Bereich der Sicherheitsüberprüfung durch. Die Internetrecherche ist ein wesentlicher Baustein der Sicherheitsüberprüfung, um sicherheitserhebliche Erkenntnisse aufzudecken. Das Sicherheitsüberprüfungsgesetz (SÜG) hat zwar eine Rechtsgrundlage zur Durchführung einer Internetrecherche. Es fehlen jedoch klare Definitionen zur Differenzierung zwischen öffentlichen und nichtöffentlichen Bereichen und auch zur Abgrenzung soziales Netzwerk von Individualkommunikation.

Aufgrund der gewachsenen Bedeutung des Internets auch für die Nachrichtendienste als mitwirkende Behörden soll die Möglichkeit der Internetrecherche im SÜG massiv ausgeweitet werden. Dies betrifft sowohl die Qualität als auch die Quantität der Recherche. Klare Definitionen sieht der ursprünglich geplante Gesetzesentwurf zur Änderung des SÜG leider nicht vor. Bei der Internetrecherche gemäß SÜG ist nicht zu verkennen, dass neben den personenbezogenen Daten der betroffenen und mitbetroffenen Personen stets eine große Anzahl von personenbezogenen Daten Dritter erhoben und verarbeitet werden, die keinen Bezug zu der entsprechenden Sicherheitsüberprüfung haben.

Querverweise:

5.2.1 Der Vorschlag zur Novelle des Sicherheitsüberprüfungsgesetzes, 8.1.5 Beratung und Kontrolle des BfV, 8.1.6 Beratung und Kontrolle des MAD

7.4.3 Novellierung des Fluggastdatengesetzes

Fast zwei Jahre nach Erlass des Grundsatzurteils des Europäischen Gerichtshofs (EuGH)[137] hat das Bundesministerium des Innern und für Heimat (BMI) im Juni 2024 die Ressortabstimmung für die Novellierung des Fluggastdatengesetzes (FlugDaG) eingeleitet.

Am 21. Juni 2022 hat der EuGH auf Vorlage des belgischen Verfassungsgerichtshofs ein Urteil erlassen, wonach die Richtlinie (EU) 2016/681 (PNR-Richtlinie) vom 27. April 2016 über die systematische Verarbeitung von Passenger Name Records/Fluggastdaten (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität zwar weiterhin gültig ist, aber sehr restriktiv ausgelegt werden muss. Diese Auslegung ist verbindlich für die Umsetzung der PNR-Richtlinie in allen Mitgliedstaaten und mithin auch der Maßstab für die Anwendung des FlugDaG, das in Deutschland der Umsetzung der Richtlinie dient. Die Fluggastdatenzentralstelle (PIU) ist in Deutschland beim Bundeskriminalamt eingerichtet.

Seit Verabschiedung der PNR-Richtlinie im Jahr 2016 weise ich regelmäßig auf problematische Fluggastdatenverarbeitung hin, so auch in den vorherigen Tätigkeits-

137 Urteil des EuGHs vom 21. Juni 2022, Az. C-817/19, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=oj:JOC_2022_340_R_0005

berichten.[138] Hervorheben möchte ich beispielweise die im FlugDaG vorgesehene Einbeziehung sämtlicher Intra-EU-Flüge und die mit einer Vorratsdatenspeicherung vergleichbare fünfjährige Speicherfrist für Fluggastdaten, welche der EuGH in seinem Grundsatzurteil ebenfalls aufgegriffen hat und die entsprechenden Vorschriften der Richtlinie nur bei enger Auslegung für europarechtskonform erachtet. Seit Erlass des Urteils habe ich deshalb die Dringlichkeit der Anpassung der Verwaltungspraxis bei der Verarbeitung von Fluggastdaten und die Novellierung des FlugDaG sowohl gegenüber dem BMI als auch im Europäischen Datenschutzausschuss (EDSA) deutlich gemacht. Das BMI hat im Juni 2024 die Ressortabstimmung zur Novellierung des FlugDaG eingeleitet.

Positiv hervorheben möchte ich, dass auf Verwaltungsebene bereits umfangreiche Anpassungen der Prozesse bei der Verarbeitung der Fluggastdaten durch die PIU als Folge des PNR-Urteils vorgenommen wurden. So werden z. B. Fluggastdaten bereits jetzt grundsätzlich nur noch sechs Monate statt fünf Jahre gespeichert und anschließend gelöscht. Auch wurden alle Altdatensätze durch die PIU gelöscht. Zudem werden nicht mehr pauschal die PNR-Daten aller Intra-EU-Flüge verarbeitet, sondern nur die von ausgewählten Flügen. Im europäischen Vergleich handelten das BMI und die PIU hier deutlich schneller als andere Mitgliedstaaten. Doch auch wenn in der Praxis bereits Anpassungen vorgenommen wurden, entbindet die Möglichkeit der richtlinienkonformen Auslegung nicht von den Grundsätzen der Bestimmtheit und Normenklarheit und damit von der Anpassung des FlugDaG selbst an die Vorgaben des EuGHs. Insoweit bleibt eine zügige Novellierung des FlugDaG im Lichte des EuGH-Urteils weiterhin geboten.

Im August 2024 habe ich der Bundesregierung in diesem Sachzusammenhang meinen zweiten Bericht zur sog. Musterkontrolle übersandt. Gemäß § 4 Abs. 3 S. 9 FlugDaG erstatte ich der Bundesregierung alle zwei Jahre Bericht über die Kontrolle der Erstellung und Anwendung der Muster für den Abgleich mit Fluggastdaten. Wesentliche Mängel bei der Datenverarbeitung habe ich im Berichtszeitraum nicht festgestellt. Ich habe aber erneut auf den Umfang der Grundrechtseingriffe durch die Verarbeitung der PNR-Daten hingewiesen. So wurden im Jahr 2023 rund 453 Millionen Passagierdatensätze von 125 Millionen Passagieren verarbeitet. Auch wenn die Speicherdauer in der Praxis nun nicht mehr stets fünf Jahre beträgt, werden die Daten für mindestens sechs Monate verdachtslos gespeichert. Demgegenüber steht die Generierung von 1.454 bis dahin unbekannten Verdächtigen. Dieses Ausmaß ist aufgrund von Verhältnismäßigkeitserwägungen – auch mit Blick auf weitere Grundrechtseingriffe – kritisch zu hinterfragen.

Gemeinsam mit meinen europäischen Kolleginnen und Kollegen im EDSA setze ich mich dafür ein, dass die nationalen PNR-Systeme überarbeitet und die rechtlichen Regelungen entsprechend angepasst werden. Bereits jetzt hat Deutschland durch die praktischen Anpassungen der PIU eine Vorreiterstellung in Europa eingenommen. Das überarbeitete FlugDaG könnte eine Vorbildfunktion übernehmen. Insofern empfehle ich dem Gesetzgeber, die Novellierung des FlugDaG unter Berücksichtigung der Vorgaben des EuGHs zügig abzuschließen.

Ich empfehle dem Gesetzgeber, die Novellierung des FlugDaG unter Berücksichtigung der Vorgaben des EuGHs zügig abzuschließen.

7.4.4 Polizei 20/20

Das gemeinsame Datenhaus der Polizeibehörden des Bundes und der Länder hat eine neue Entwicklungsstufe erreicht. Durch geplante Funktionalitäten sollen personenbezogene Daten in bestimmten Fällen übergreifend für andere Polizeibehörden sichtbar gemacht werden. Auf der politischen Ebene wäre es wünschenswert, für das Projekt weitere klare Rechtsgrundlagen zu ergänzen.

Über das Gesamtprogramm Polizei 20/20 (P 20) berichte ich regelmäßig, zuvor in meinem 32. Tätigkeitsbericht (Nr. 7.2). Auch in diesem Jahr kann ich positiv hervorheben, dass die Projektgruppe P 20 im Bundesministerium des Innern und für Heimat (BMI) die Datenschutzaufsichtsbehörden des Bundes und der Länder regelmäßig zu dem Gesamtprogramm und den Teilprojekten beteiligt und sich insgesamt ein konstruktiver Austausch verstetigt hat.

Entwicklung des Datenhauses:

Mitte des Jahres 2024 haben Mitarbeitende meines Hauses an Informationsveranstaltungen zu dem gemeinsamen Datenhaus der Polizeibehörden des Bundes und der Länder teilgenommen, zu denen das BMI eingeladen hatte. Das gemeinsame Datenhaus ist der Kern von P 20. In dem Datenhaus sollen künftig sämtliche personen-

138 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, 31. TB Nr. 7.1 und zuletzt 32. TB Nr. 7.1

bezogenen Daten aller Polizeibehörden mandantengetrennt gespeichert werden.

Das BMI stellte in den Terminen die Struktur des Datenhauses und die technische Architektur dar und erläuterte bestimmte Funktionalitäten. So wird beabsichtigt, die Mandantentrennung, also die technische Trennung zwischen den einzelnen Polizeibehörden, durch eine sog. Kontextualisierung zu durchbrechen. Konkret bedeutet dies, dass sich die Polizeibehörden untereinander in bestimmten Fällen Sichtfreigaben auf ihre jeweiligen Datenbestände einräumen können.

In der Weiterentwicklung des Datenhauses sehe ich interessante Ansätze, die es lohnt, weiter zu durchdenken. Grundsätzlich kann ein gemeinsames Datenhaus eine Chance für den Datenschutz sein. Zunächst muss jedoch geklärt werden, auf welchen rechtlichen Grundlagen das Datenhaus überhaupt betrieben und dessen Funktionen genutzt werden können. Besonders in der Funktionalität der Kontextualisierung sehe ich noch Klärungsbedarf. Ich sehe hier die Möglichkeit, dass Speicherschwellen nach dem Bundeskriminalamtgesetz (BKAG) unterlaufen werden können. Das BMI habe ich zu klärungsbedürftigen Punkten um eine Stellungnahme gebeten. Eine Antwort lag mir bis zum Redaktionsschluss noch nicht vor. Hier ist besonders darauf zu achten, dass der Grundsatz der Zweckbindung eingehalten wird. Insbesondere müssen die gesetzlichen und verfassungsrechtlichen Grenzen zur bevorratenden Speicherung zu Zwecken der Vorsorge eingehalten werden. Dazu hatte das Bundesverfassungsgericht im Herbst 2024 ein wichtiges Urteil gesprochen (Urteil vom 1. Oktober 2024, 1 BvR 1160/19) [139].

Es ist ein eigenes Modul vorgesehen, das die Grundsätze der hypothetischen Datenneuerhebung automatisiert berücksichtigen soll. Hierbei handelt es sich um Vorgaben des Bundesverfassungsgerichts. [140] [141] Diese sollen sicherstellen, dass Daten aus besonders eingriffsintensiven Ermittlungsmaßnahmen nur dann verwendet werden können, wenn dies für die Verfolgung hinreichend erheblicher Delikte notwendig ist. Die technische Umsetzung durch ein eigenes Modul sehe ich als Gewinn.

Mit Sorge sehe ich die Frage der Rechtsgrundlagen. Diese sind vorhanden, soweit das Datenhaus den polizeilichen Informationsverbund gemäß §§ 29 ff. des BKAG betrifft. Soweit aber die Polizeibehörden in Bund und Ländern darüberhinausgehend weitere Daten speichern wollen, kann dies nur auf der Grundlage eines Normengeflechts der Polizeigesetze in Bund und Ländern geschehen. Die Speicherung muss zudem in Kombination mit einer Vielzahl von Vereinbarungen zur Auftragsverarbeitung geregelt werden. Hier wäre es sowohl für den Datenschutz als auch für die Effizienz der polizeilichen Arbeit sinnvoll, klare gesetzliche Regelungen zu schaffen. Diese müssen aus verfassungsrechtlichen Gründen die technische mandantenfähige und an der Zweckbindung ausgerichtete Trennung der Daten vorsehen. Gleichzeitig kann eine zentrale Verantwortlichkeit für den technischen Betrieb geregelt werden. Dadurch würden die Polizeibehörden ein hohes Maß an Rechtssicherheit und Effizienz erhalten. Die aus Sicht des Datenschutzes notwendigen Anpassungen gehen in dieselbe Richtung wie das polizeiliche Interesse und inhaltlich sehe ich hier einen Konsens mit der Projektgruppe P 20.

Strategische Komponente des Polizeilichen Informations- und Analyseverbundes (PIAV-S)

PIAV-S soll den Polizeibehörden des Bundes und der Länder bundesweite strategische Auswertungen ermöglichen. Unter anderem sollen Drogenerstkonsumenten und Mehrfachkonsumenten erfasst und als „Echttäter“ gezählt werden. Seit 2019 besteht zwischen dem BMI und dem Bundeskriminalamt (BKA) einerseits und meinem Haus andererseits ein Dissens, ob mit PIAV-S personenbezogene Daten in Form von pseudonymisierten Daten verarbeitet oder ob die Daten anonymisisert werden. [142] Das BKA hat meinen Mitarbeitenden das System vorgestellt. Ich bin zu dem Ergebnis gekommen, dass die Daten pseudonymisiert verarbeitet werden. Grund hierfür ist, dass sich anonymisierte Daten grundsätzlich nicht dazu eignen, Echttäter zu zählen und diesen über die Zeit auftretende Ereignisse zuordnen zu können. In dieser Konsequenz bedarf es einer rechtlichen Grundlage, wenn personenbezogenen Daten weiterverarbeitet werden sollen. Ich halte die polizeiliche Generalklausel des § 16 Abs. 1 BKAG in bestimmte Fällen dafür als geeignete Rechtsgrundlage. Insbesondere dann, wenn die verarbeiteten Daten zugleich in dem bundesweiten Polizeilichen Informationsverbund (INPOL-Z) gespeichert werden und somit bestimmte Speicherschwellen des BKAG bereits erfüllen. Ist dies nicht der Fall, sind

139 Urteil des BVerfG vom 1. Oktober 2024, 1 BvR 1160/19, abrufbar unter: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2024/10/rs20241001_1bvr116019.html

140 Urteil des BVerfG vom 20. April 2016, 1 BvR 966/09 & 1 BvR 1140/09, abrufbar unter: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html

141 32. TB Nr. 7.2

142 32. TB Nr. 7.2

Auswertungen nur in einem begrenzten Umfang möglich. Hierfür sind unter anderem die Vorgaben aus der höchstrichterlichen Rechtsprechung zu beachten. Mit PIAV-S werden keine komplexen Auswertungen vorgenommen. Es handelt sich um Fallzahlenerhebungen mit einer starken Verschlüsselungsmethode. PIAV-S wird innerhalb des Programms P 20 nicht mehr weiterverfolgt. Das BKA betreibt PIAV-S in seiner Zentralstellenfunktion weiter.

PIAV-S-Politisch-Motivierte-Kriminalität (PIAV-S-PMK)

PIAV-S-PMK ist ein auf derselben Technik wie PIAV-S basierendes, aber anders ausgestaltetes Meldesystem für den Bereich des Staatsschutzes.[143] Mit dem System sollen die Landespolizeibehörden künftig personenbezogene Daten aus dem Phänomenbereich des Staatsschutzes elektronisch an das BKA liefern. Dadurch soll der Kriminalpolizeiliche Meldedienst weiterentwickelt werden. Ähnlich wie bei PIAV-S sehe ich die Anwendung gestützt auf die polizeiliche Generalklausel des § 16 Abs. 1 BKAG nur in einem begrenzten Umfang für zulässig. Umfangreiche Analysen können nicht auf die Generalklausel gestützt werden.

Für die datenschutzrechtliche Sicherheit und die Effizienz der Arbeit der Polizeibehörden empfehle ich, für das IT-Großprojekt Polizei 20/20 (P20) klare gesetzliche Regelungen zu schaffen.

7.4.5 Sicherheitsüberprüfungen in der Wirtschaft

Die in der Wirtschaft bestehenden datenschutzrechtlichen Defizite im Sicherheitsüberprüfungsbereich sind in vielen Fällen auf eine unnötige Unübersichtlichkeit der Regelungen und daraus resultierender Unsicherheiten bei der Rechtsanwendung zurückzuführen. Daher ist es mein Ziel, insbesondere durch konstruktive Beratung, einen kontinuierlichen fachlichen Austausch mit allen Beteiligten und aktive Öffentlichkeitsarbeit Mängeln vorzubeugen.

Im Bereich des Sicherheitsüberprüfungsgesetzes (SÜG) gehört es zu meinen Aufgaben, darüber zu wachen, dass auch bei den nichtöffentlichen Stellen, also bei Wirtschaftsunternehmen, die datenschutzrechtlichen Bestimmungen eingehalten werden (§ 36a Abs. 2 S. 1 SÜG). Dies betrifft eine Vielzahl von Unternehmen, die ihr Personal sicherheitsüberprüfen. Auch in diesem Berichtsjahr trafen sich deshalb meine Mitarbeitenden mit Vertretern von Wirtschaftsverbänden und Unternehmen und beantworteten eine Vielzahl von Beratungsanfragen bei und außerhalb von Kontrollen oder gaben proaktiv Empfehlungen ab.

Grundsätzlich sehe ich in der Privatwirtschaft eine große Bereitschaft zur umfassenden Umsetzung der Vorgaben des Datenschutzrechts in der Praxis. So werden meine Empfehlungen aus Beratungen und Kontrollen in der Regel vollständig und zügig umgesetzt. Verbände und Wirtschaftsunternehmen haben ein großes Interesse an einer rechtskonformen Datenverarbeitung, nicht zuletzt auch um Haftungsrisiken und behördliche Sanktionen auszuschließen.

Darüber hinaus habe ich Unterstützung sowohl von Vertretern der Wirtschaft als auch vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) erfahren, z. B. dankenswerterweise durch die arbeitsintensive Bereitstellung von Unterlagen, die ich zur Aufarbeitung von Dokumentationsmängeln der Unternehmen heranziehen konnte.

Zudem fanden meine Schulungsangebote bei der Bundesakademie für öffentliche Verwaltung, beim Sicherheitsseminar des BMWK sowie bei anderen Arbeitskreisen großen Anklang. Gleiches gilt auch für die auf meiner Homepage veröffentlichten Arbeitshilfen und Kontrollberichte[144]. Mit diesen Maßnahmen möchte ich das datenschutzrechtliche Wissen einem breiten Personenkreis zugänglich machen und sowohl Wirtschaftsunternehmen als auch sonstigen Akteuren im Sicherheitsüberprüfungsverfahren eine rechtssichere und effektive Datenverarbeitung ermöglichen.

Denn, wie in der Vergangenheit,[145] musste ich auch in diesem Berichtszeitraum immer wieder die Erfahrung machen, dass viele der von mir festgestellten datenschutzrechtlichen Defizite überwiegend auf Unsicherheiten bei der Rechtsanwendung sowohl auf Seiten der Wirtschaft als auch auf Seiten der öffentlichen Auftraggeber zurückzuführen sind. Vertreter der Wirtschaft, mit denen sich meine Mitarbeitenden regelmäßig treffen, bemängeln insbesondere die Unübersichtlichkeit und Komplexität der Regelungen im Sicherheitsüberprüfungsbereich sowie das fehlende Wissen der öffentlichen Auftraggeber über Abläufe des Geheimschutzes in der Wirtschaft.

143 32. TB Nr. 7.2

144 BfDI-Arbeitshilfen zum Sicherheitsüberprüfungsrecht, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Sicherheit/Praxis-Sicherheitsrecht/Praxis-Sicherheitsrecht-node.html

145 32. TB Nr. 9.1.6

Diese Umstände erschweren den Unternehmen nach Aussage der Wirtschaftsvertreter nicht nur die in Zeiten gestiegener Sicherheitsrisiken dringend notwendige rechtssichere Personalplanung, sondern wirken sich auch negativ auf den Umgang mit personenbezogenen Daten aus. Ich musste beispielsweise feststellen, dass öffentliche Auftraggeber in Verkennung der Rechtslage oder zur vermeintlichen Prozessvereinfachung Wirtschaftsunternehmen zu unzulässigen Datenverarbeitungen veranlassen. Zur Veranschaulichung verweise ich exemplarisch auf meine Arbeitshilfe nebst tabellarischer Übersicht[146] zur Datenverarbeitung durch Sicherheitsbevollmächtigte (SiBe), Sabotageschutzbeauftragte (SaBe) und sonstige Beauftragte nach § 25 SÜG, in dem u. a. die Differenzierungen nach dem Geheimschutz, dem Sabotageschutz und der sonstigen sicherheitsempfindlichen Tätigkeit sowie nach zuständigen Stellen und SiBe/SaBe-Bestellung erläutert werden.

Anlass für dieses Rundschreiben war, dass ich zuvor bei meinen Datenschutzkontrollen festgestellt hatte, dass hinsichtlich der Rolle und Befugnisse der Unternehmen bei Sicherheitsüberprüfungen erhebliche Unsicherheiten sowohl auf der Unternehmens- als auch auf der Behördenseite bestehen. Behörden baten SiBe und/oder SaBe in Unternehmen um eine weitreichende inhaltliche Mitwirkung an Sicherheitsüberprüfungen, auch wenn es hierfür keine Rechtsgrundlage gab. Dies führte zu Datenschutzverstößen auf beiden Seiten. So wurden beispielsweise in Unternehmen Sicherheitserklärungen eingesehen und geprüft sowie Sicherheitsakten geführt, obwohl die Voraussetzungen nach § 26 SÜG bzw. §§ 30 i. V. m. 18 SÜG nicht vorlagen.

Die in der 20. Wahlperiode beratene SÜG-Novellierung sollte in der neuen Wahlperiode erneut aufgegriffen werden. Damit bestünde eine Chance, die Systematik zu verbessern und die Regelungen klarer zu fassen. Gerne stehe ich hierzu weiter konstruktiv für Beratungen zur Verfügung.[147]

Deshalb werden die (proaktive) Beratung und der fachliche Austausch mit allen Akteuren im Sicherheitsüberprüfungsbereich – wie schon seit mehreren Jahren – auch in der Zukunft im Vordergrund meiner diesbezüglichen Tätigkeit stehen. Denn erfahrungsgemäß kann der Schutz der informationellen Selbstbestimmung gerade angesichts der Vielzahl der Unternehmen in meinem Zuständigkeitsbereich so am wirksamsten erreicht werden.[148]

Querverweise:

5.2.1 Der Vorschlag zur Novelle des Sicherheitsüberprüfungsgesetzes, 8.1.2 SÜG-Kontrollen belegen erhöhten Beratungsbedarf

7.4.6 BfDI erhält vollständigen FIU-Bericht

Mit Hilfe meiner datenschutzrechtlichen Abhilfebefugnisse, dem schriftlichen Austausch von Standpunkten und in persönlichen Gesprächen habe ich das Bundesministerium der Finanzen (BMF) überzeugt, mir lange vorenthaltene Informationen zu übersenden. So konnten die mir gegenüber bestehenden gesetzlichen Informationsverpflichtungen im gegenseitigen Einvernehmen erfüllt werden.

Im Frühjahr 2023 erlangten meine Mitarbeitenden Kenntnis davon, dass der Abschlussbericht zur Betrachtung der Bearbeitungsrückstände bei der Financial Intelligence Unit (FIU) im BMF vorlag. Daraufhin habe ich diesen zur Einsichtnahme beim BMF angefordert. Es erfolgte eine Übersendung des Berichts als Verschlusssache VS-Vertraulich mit teilweisen Schwärzungen von Textpassagen. Begründet wurde dies seitens des BMF damit, dass eine uneingeschränkte Übersendung tiefe Einblicke in die Arbeitsweise der FIU gewähren würde und eine Kenntnisnahme das Staatswohl der Bundesrepublik Deutschland gefährde. Selbst eine höhere Schutzklasseneinstufung könne die Gefahr nicht beseitigen. Darauf folgte ein Briefwechsel, in dem erneut die gegensätzlichen Standpunkte ausgetauscht wurden und ich die Übersendung einer vollständigen Fassung des Berichts verlangt habe. Letztendlich sah ich mich gezwungen, aufsichtsrechtliche Maßnahmen zu ergreifen und beanstandete die Nichtübersendung einer ungeschwärzten Fassung förmlich. § 16 Abs. 4 S. 1 Nr. 2 Bundesdatenschutzgesetz verpflichtet die beaufsichtigten Stellen, mir sämtliche für meine Aufgabenerledigung erforderlichen Informationen bereitzustellen. Ebenso ist die Berufung auf die Rechtsprechung des Bundeverfassungsgerichts zur Staatswohlgefährdung seitens BMF im konkreten Fall nicht möglich, da die Vorrausetzungen nicht vorliegen. Meine Behörde verfügt über effektive Vorkehrungen, um das Bekanntwerden von Dienstgeheimnissen zu

146 Übersicht zu §§ 24-31 SÜG, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Arbeitshilfen/Arbeitshilfen-S%C3%9CG/_Anlage-zu-S%C3%9CG-24-bis-31.html

147 32. TB Nr. 3.3.5

148 31. TB Nr. 12.4

verhindern. Leider führte diese datenschutzrechtliche Maßnahme zunächst nicht zum Umdenken beim BMF.

Anders bei der FIU. Es folgten konstruktive und lösungsorientierte Gespräche, die bestehende Bedenken ausräumen konnten. Im Ergebnis übersandte mir die FIU den vollständigen Bericht im Sommer 2024. Auch das BMF hatte keine weiteren Einwände. Die Gespräche haben aus meiner Sicht bestehende Vorbehalte abgebaut und zu mehr Vertrauen untereinander geführt. So ist es bereits in einem vergleichbaren Sachverhalt in diesem Jahr zu einer erfolgreichen und problemlosen Zusammenarbeit mit dem BMF gekommen. Ich bin daher zuversichtlich, dass auch gleichgelagerte Sachverhalte zukünftig gemeinsam mit BMF und FIU konstruktiv gelöst werden können.

7.4.7 Löscherfolge bei der FIU

Im Berichtszeitraum konnte ich wesentliche Verbesserungen bei der Löschung personenbezogener Daten durch die Financial Intelligence Unit (FIU) erreichen. Zum einen werden nun regelmäßige Löschungen im Informationspool durchgeführt. Zum anderen soll die einzelfallbezogene Löschung der Daten von Verpflichteten nach dem Geldwäschegesetz (GwG) ermöglicht werden. Abschließend konnten auch im Rahmen von Bürgerbeschwerden einzelfallbezogene Löschungen erreicht werden.

Einhaltung der Löschfristen im Informationspool

Schwerpunkt der Tätigkeit der FIU ist die Sammlung und Auswertung von Meldungen über verdächtigte Finanztransaktionen unterhalb des strafprozessualen Anfangsverdachtes. Diese Meldungen beinhalten eine große Anzahl personenbezogener Daten. Alleine im Jahr 2023 sind 322.590 Meldungen bei der FIU eingegangen. Die Meldungen speichert die FIU in ihrem sog. „Informationspool".

Nach § 37 Abs. 2 GwG ist die FIU verpflichtet, personenbezogene Daten zu löschen, wenn die Speicherung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Nach § 37 Abs. 4 GwG sind die Löschvoraussetzungen bei der Einzelfallbearbeitung oder nach festgesetzten Fristen zu prüfen.

Im Jahr 2021 wurde hierzu erstmals eine Kontrolle durchgeführt. In dieser wurde u. a. festgestellt, dass in der genutzten Fachanwendung kein technischer Mechanismus zur Umsetzung der Löschfristen implementiert war. Dies wurde gegenüber dem Bundesministerium der Finanzen förmlich nach § 16 Abs. 2 Bundesdatenschutzgesetz beanstandet.[149]

Seitdem habe ich das Verfahren zur Löschung personenbezogener Daten bei der FIU intensiv begleitet. Zwar hat die FIU nach meiner Beanstandung eine technische Lösung beauftragt. Diese war bisher aus verschiedenen Gründen aber nur kurzzeitig in Betrieb.

Im Oktober 2024 hat mir die FIU nun bestätigt, dass die Löschroutine wiederaufgenommen wurde. Seit dem 21. Oktober 2024 wird sie täglich ausgeführt. Damit hat die FIU die Forderung aus meinem Kontrollbericht nunmehr umgesetzt.

Löschung der Daten von Verpflichteten nach dem GwG

Verpflichtete nach dem GwG müssen sich im elektronischen Meldeportal der FIU, „goAML-Web", registrieren. Von dort werden die Daten automatisiert in die Fachanwendung der FIU übertragen. Fällt nun die Erforderlichkeit zur Verarbeitung weg – z. B. in Folge einer personellen Veränderung –, muss die FIU diese Daten löschen.

Im Rahmen einer Bürgerbeschwerde erlangte ich Kenntnis, dass es auch hierfür bisher keinen technischen Prozess gab. Dies habe ich ebenfalls förmlich gegenüber dem BMF beanstandet. Nach einem intensiven Austausch konnte die Löschung zunächst im Einzelfall umgesetzt werden. Ab Dezember 2024 hat mir die FIU eine standardisierte Löschfunktionalität zugesichert.

Löschung im Einzelfall

Wie eingangs ausgeführt, ist die FIU nach § 37 Abs. 4 GwG verpflichtet, auch bei der Einzelfallbearbeitung die Löschvoraussetzungen zu prüfen. Das Recht auf Löschung besteht nach § 37 Abs. 2 GwG unabhängig von festen Fristen immer dann, wenn eine Speicherung für die Aufgabenerfüllung der FIU nicht (mehr) erforderlich ist.

Dies bedeutet, dass personenbezogene Daten gelöscht werden müssen, wenn feststeht, dass die gegenständliche Verdachtsmeldung nicht mit einer strafbaren Handlung in Zusammenhang steht. Dem trat die FIU bisher entgegen und argumentierte, dass die Speicherung über den Zeitraum der festgelegten Löschfristen stets für ihre Aufgabenerfüllung erforderlich sei.

Auch hier konnten im Berichtszeitraum Verbesserungen erreicht werden. In einem Fall wurden die Daten gelöscht, nachdem die Verpflichtete in einer Nachmeldung die ursprüngliche Verdachtsmeldung korrigiert

149 30. TB Nr. 8.2.9

und damit zurückgezogen hatte. In einem anderen Fall beschritt der Beschwerdeführer zeitgleich den Verwaltungsrechtsweg und legte vor dem Verwaltungsgericht Köln erfolgreich dar, dass der Transaktion ein berufstypischer Vorgang zu Grunde lag. In beiden Fällen wurden die Daten letztlich vor Ablauf der regulären Frist gelöscht.

7.5 Arbeit und Soziales

7.5.1 Berechtigungsnachweis für Sozialtickets

Der Berechtigungsnachweis soll Empfängerinnen und Empfängern von Bürgergeld und anderen Sozialleistungen den vergünstigten Zugang zu Bildung, Sport und Kultur und insbesondere den Erwerb eines ermäßigten Tickets für den öffentlichen Nahverkehr ermöglichen. Einfache und digitale Lösungen auch für die Kundinnen und Kunden der Jobcenter sind möglich, der Sozialdatenschutz muss aber beachtet werden.

Im Berichtszeitraum habe ich mich intensiv mit dem Verfahren zur Ausstellung von Berechtigungsnachweisen für Sozialtickets im Land Berlin befasst, soweit Sozialdaten der in Berlin als gemeinsame Einrichtungen organisierten Jobcenter dafür verarbeitet werden sollen. Auf Bitte der Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung und in enger Abstimmung mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit sind meine Mitarbeiterinnen und Mitarbeiter in intensiven Beratungen bei der Bewertung verschiedener Vorschläge für digitale Verfahrensweisen unterstützend tätig geworden.

Ursprünglich wurden die zunächst sog. „Berlinpässe“ von den Bürgerämtern ausgestellt. Diese wurden dann durch Berechtigungsnachweise ersetzt, die direkt von den leistungsgewährenden Sozialbehörden ausgestellt werden. Diese Umstellung führte zu Verzögerungen in der Ausstellung der Berechtigungsnachweise, sodass Sozialleistungsempfängerinnen und -empfänger aktuell gezwungen sind, ihren Leistungsbescheid etwa bei einer Fahrscheinkontrolle vorzuzeigen.

Um Möglichkeiten auszuloten, die etwa mit einer Umgestaltung der Leistungsbescheide der Jobcenter verbunden sind, bin ich auch auf die Bundesagentur für Arbeit zugegangen. Eine datenschutzfreundliche und schnell umsetzbare Variante wäre es, QR-Codes auf die Leistungsbescheide der Beziehenden von SGB II-Leistungen zu drucken. Der Code könnte dann als digitaler Berechtigungsnachweis für ermäßigte Monatstickets dienen und beispielsweise am Fahrkartenautomaten eingescannt werden. Eine automatisierte Übermittlung von Sozialdaten von den Jobcentern an die Berliner Verkehrsbetriebe, für die grundsätzlich eine vorherige Einwilligung erforderlich ist, wäre damit entbehrlich.

Da das Thema der Gewährung eines „Sozialtickets“ auch in anderen Bundesländern virulent ist, würde ich eine bundeseinheitliche Vorgehensweise begrüßen.

7.5.2 Datenschutzpanne beim Rentenservice der Deutschen Post AG

Im November 2023 wurden beim Druck und Versand von ca. 25.000 Rentenausweisen durch den Renten Service der Deutschen Post AG die Zuordnung von personalisierten Willkommensschreiben an Neurentner und -rentnerinnen und dem zugehörigen Rentenausweis fehlerhaft vorgenommen. In der Folge dieser Falschzuordnung wurden sensible Sozialdaten, die dem Rentenausweis zu entnehmen sind, (Vorname, Nachname, Geburtsdatum und Rentenversicherungsnummer) gegenüber unberechtigten Dritten offenbart.

Im November und Dezember 2023 wurden bei mir zahlreiche datenschutzrechtliche Beschwerden gemäß Art. 77 DSGVO von betroffenen Personen eingereicht. Auch hat die Deutsche Post AG den Datenschutzverstoß gemäß Art. 33 DSGVO im November 2023 bei mir gemeldet. Nach umfassender Sachverhaltsaufklärung und rechtlicher Prüfung habe ich im Rahmen des von mir eröffneten datenschutzaufsichtsrechtlichen Verfahrens festgestellt, dass die Deutsche Post AG durch die unrechtmäßige Offenlegung der Daten gegen Art. 6 Abs. 1 DSGVO verstoßen hat. Außerdem waren die getroffenen technisch organisatorischen Maßnahmen nach Art. 32 DSGVO nicht geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, das dem in der massenhaften Verarbeitung sensibler personenbezogenen Daten immanenten hohen Risiko in angemessener Form begegnet. Aufgrund der festgestellten Verstöße habe ich die Deutsche Post AG im Berichtszeitraum gemäß Art. 58 Abs. 2 lit. b) DSGVO verwarnt.

Von einer Anweisung habe ich abgesehen, da die Deutsche Post AG umgehend auf meine Intervention reagiert und zusätzliche Maßnahmen implementiert hat, um zukünftig ein dem Risiko entsprechendes Schutzniveau zu gewährleisten. Außerdem wurden die Betroffenen postalisch von der verantwortlichen Stelle in Form eines Entschuldigungsschreibens informiert und gebeten, den Rentenausweis mittels eines vorfrankierten Rückumschlags wieder zurückzusenden.

8 Kontrollen und Beratungen

8.1 Beratungs- und Kontrollbesuche im Sicherheitsbereich

8.1.1 Kontrolle von Speicherungen im Vorgangsbearbeitungssystem der Bundespolizei

Eine Kontrolle von Speicherungen im Vorgangsbearbeitungssystem der Bundespolizei brachte keine erheblichen Verstöße zum Vorschein. Lediglich kleinere Mängel bei der Erfassung personenbezogener Daten wurden festgestellt, sodass ich von einer Beanstandung absehen konnte.

Die bereits im Frühsommer 2023 begonnene Kontrolle von Speicherungen personenbezogener Daten im Vorgangsbearbeitungssystem @rtus-Bund bei der Bundespolizeidirektion Berlin konnte im Berichtszeitraum abgeschlossen werden. Schwerpunkt der Kontrolle waren Vorgänge mit Bezügen zur politisch motivierten Kriminalität. Anhand der gesetzlichen Grundlagen sowie interner Erfassungsvorgaben der Bundespolizei prüften meine Mitarbeitenden insbesondere die korrekte Zuordnung von Personenrollen (Beschuldigte, Zeugen, Kontaktpersonen etc.) sowie die Berechnung von Löschfristen.

Im Ergebnis habe ich lediglich kleinere datenschutzrechtliche Mängel bei der Vorgangserfassung festgestellt, die nicht auf eine übergelagerte organisatorische Problematik hindeuteten, sondern auf Bearbeitungsfehler im Einzelfall zurückzuführen waren. Vielmehr konnte ich ein ausgeprägtes Problembewusstsein bei der Bundespolizei feststellen, die meinen Beratungs- und Kontrollbesuch mit hohem personellen Einsatz vorbereitet und unterstützend begleitet hat. Hierbei hat sich die Bundespolizei erkennbar um eine Aufarbeitung der entdeckten Fehlerfassungen bemüht und sich einer Beratung durch meine Mitarbeitenden gegenüber aufgeschlossen gezeigt. Festgestellte Verstöße wurden teilweise noch während des Kontrollbesuchs im Vorgangsbearbeitungssystem korrigiert.

Insgesamt konnte ich im Rahmen meines Ermessens von einer datenschutzrechtlichen Beanstandung absehen. Im Kontrollbericht habe ich einige Empfehlungen zur erneuten Sensibilisierung der Mitarbeitenden sowie möglichen Anpassungen an der Software beratend ausgesprochen, denen die Bundespolizei nachgekommen ist bzw. eine Prüfung zugesagt hat.

8.1.2 SÜG-Kontrollen belegen erhöhten Beratungsbedarf

Bei meinen in diesem Berichtsjahr durchgeführten Kontrollen nach dem Sicherheitsüberprüfungsgesetz (SÜG) konnte ich auf meine Beratung zurückzuführende positive Entwicklungen bei der Einhaltung datenschutzrechtlicher Bestimmungen in Sicherheitsüberprüfungsverfahren feststellen. Festgestellte datenschutzrechtliche Defizite können durch bessere personelle Ausstattung der kontrollierten Stellen, technische Unterstützung und mehr Aus- und Fortbildung abgestellt werden.

Im Berichtsjahr kontrollierte mein Haus bei 17 Stellen die Einhaltung der datenschutzrechtlichen Vorgaben des Sicherheitsüberprüfungsgesetzes (SÜG). Kontrolliert wurden sieben geheim- und sabotageschutzbetreute Unternehmen aus den Branchen der Rüstungsindustrie, Personalgestellung, IT/IT-Sicherheit, Telekommunikation und Objektsicherheit sowie zehn Bundesbehörden. Vier Kontrollen waren bei Redaktionsschluss noch nicht abgeschlossen. Drei bereits im Vorjahr begonnene Kontrollen konnten im Berichtszeitraum abgeschlossen werden.

In 13 Fällen habe ich Beanstandungen aufgrund datenschutzrechtlicher Verstöße ausgesprochen, wobei sieben auf den öffentlichen Bereich entfielen. Hinsichtlich der wiederholt festgestellten datenschutzrechtlichen Mängel oder Verstöße in Sicherheitsüberprüfungsverfahren nach dem SÜG kann ich im Wesentlichen auf die Tätigkeitsberichte der Vorjahre verweisen. Es gab jedoch auch einige neue Themen.

Neue Erkenntnisse aus den Kontrollbesuchen

Ein wiederkehrendes Thema war die Zusammenarbeit von Behörden und Unternehmen bei Sicherheitsüberprüfungen in der Wirtschaft. In einem Fall führte eine nichtöffentliche Stelle Sicherheitsakten ohne Rechtsgrundlage. In einem anderen Fall wiederum hatte eine öffentliche Stelle bei Sicherheitsüberprüfungsverfahren von Fremdpersonal die jeweiligen Fremdfirmen aktiv eingebunden und ohne Rechtsgrundlage Aufgaben der personellen Geheim- und Sabotageschutzüberprüfung an die Unternehmen übertragen, etwa das Einholen und Vorprüfen der Sicherheitserklärungen. Das führte hier im Ergebnis dazu, dass die Firma für die betroffenen Personen entgegen der Regelung in § 18 Abs. 1 SÜG Sicherheitsakten anlegte. Außerhalb des Anwendungsbereiches der §§ 24–31 SÜG, d. h. bei sicherheitsempfindlichen Tätigkeiten von Fremdpersonal in der Behörde, wirken die Unternehmen, auch wenn sie Beauftragte nach § 25 SÜG bestellt haben, jedoch nicht an Sicherheitsüberprüfungsverfahren mit und haben keine Befugnisse zur Datenverarbeitung nach dem SÜG. Nach den Vorgaben des SÜG arbeitet in diesen Fällen ausschließlich die jeweils zuständige Stelle. Da diese Praxis mir seitens der Wirtschaftsvertreter als „häufige Vorgehensweise“ geschildert wurde, habe ich ein Rundschreiben zur Datenverarbeitung durch Sicherheitsbevollmächtigte, Sabotageschutzbeauftragte und sonstige Beauftragte nach § 25 SÜG[150] verschickt.

In einem Fall veranlasste die personalverwaltende Stelle beim Geheimschutzbeauftragten regelmäßig Sicherheitsüberprüfungen für Ersatzkandidatinnen und Ersatzkandidaten aus Bewerbungsverfahren. Für diese Personen bestand zunächst keine direkte Einstellungsabsicht und somit erst recht keine konkrete Absicht, die Person mit einer sicherheitsempfindlichen Tätigkeit zu betrauen. Diese Verfahrenspraxis wurde auf meine Intervention hin mittlerweile abgestellt.

Obwohl mein Haus bereits im vergangenen Jahr beratend darauf hingewiesen hatte, dass es hierfür im SÜG keine Rechtsgrundlage gibt, stießen meine Mitarbeitenden bei zwei Kontrollen im Geschäftsbereich des BMVg auch in diesem Berichtsjahr zum wiederholten Male auf Listen über die Vernichtung oder die Abgabe von Sicherheitsakten an andere Dienststellen, die über einen Zeitraum von 10 Jahren zurückreichten. Diese Arbeitsweise wird durch eine interne Dienstvorschrift bindend vorgegeben. Die vom BMVg bereits zugesagte Überarbeitung dieser internen Weisungslage stand zum Kontrollzeitpunkt immer noch aus, so dass ich eine diesbezügliche Beanstandung aussprechen musste.

Aus einer Kontrolle ergab sich, dass das Personalverwaltungssystem „PVSPlus“ für den Organisationsbereich des personellen Geheim- und Sabotageschutz zwar grundsätzlich als Instrument für die Vorgangsverwaltung (Wiedervorlagemanagement und Fristenkontrolle) gemäß § 20 Abs. 1 SÜG genutzt werden kann. Die vorgefundene technische Ausgestaltung des Prozesses hat sich in dem konkret kontrollierten Fall jedoch als ungeeignet für ein zuverlässiges Fristenmanagement erwiesen, da nach Ausscheiden der betroffenen Person aus der Behörde für den Geheim- und Sabotageschutzbeauftragten nur ein sehr kurzes Zeitfenster für die weitere Bearbeitung des Vorgangs geöffnet blieb. Danach bestand faktisch keine Zugriffsmöglichkeit mehr auf eingetragene Fristen und Wiedervorlagen. Im Falle der kontrollierten Stelle führte das in zahlreichen Fällen dazu, dass Akten über die gesetzliche Vernichtungsfrist hinaus in der Aufbewahrung verblieben und eine unübersichtliche Ansammlung von nicht mehr löschbaren überholten Fristen und Wiedervorlagen eine zielführende Abarbeitung unnötig erschwerte.

In einem Fall kommunizierten Mitarbeitende über dienstliche Belange von sicherheitsüberprüftem Personal via Messenger-Dienst. Mein Haus forderte die verantwortliche Stelle auf, das Personal nochmals betreffend die Nutzung von Messenger-Diensten zu sensibilisieren und den Austausch von firmeninternen Informationen zu Sicherheitsüberprüfungen zu untersagen. Außerdem empfahlen meine Mitarbeitenden, die Einhaltung der Weisung durch hinreichende technische und organisatorische Maßnahmen zu kontrollieren.

In einem Fall war der Geheimschutzbeauftragte im Nebenamt bestellt und wendete nur einen geringen Anteil seiner Arbeitszeit für den Bereich Geheimschutz auf. Hinzu kam eine insgesamt unzureichende Besetzung dieses Aufgabenbereiches. Hierauf waren etliche datenschutzrechtliche Verstöße zurückzuführen. Ich forderte die Stelle auf, dafür Sorge zu tragen, dass die Tätigkeit des Geheim- und Sabotageschutzbeauftragten zukünftig hauptamtlich ausgeübt werden muss.

In einem Fall war keine Stellvertretung für den Sabotageschutzbeauftragten bestellt. Dies hat meine Kontrolltätigkeit beeinträchtigt. Vor allem steht aber zu befürchten, dass in einem solchen Szenario bei einem (längeren) Personalausfall des Sabotageschutzbeauftrag-

150 Rundschreiben vom 2. Mai 2024 zum Fünften Abschnitt des SÜG, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Sueg/Rundschreiben-f%C3%BCnfter-Abschnitt-S%C3%9CG

ten sicherheitsrelevante Informationen nicht zeitnah abgearbeitet werden können, was sich gegebenenfalls auch auf die materielle Sicherheit auswirken kann.

In einem Fall wurde Outlook in großem Umfang als „Nebenakte" genutzt. Gespeichert wurde dort neben zahlreichen Dokumenten aus den Sicherheitsüberprüfungsverfahren auch interne Korrespondenz, zum Teil mit personenbezogenen Daten unbeteiligter Dritter. Ich habe die kontrollierte Stelle aufgefordert, die Ordner in Outlook einmal monatlich auf unzulässige personenbezogene Daten zu kontrollieren, um zukünftige Verstöße zu vermeiden.

In einem Fall war das sicherheitsüberprüfte Personal eines Unternehmens in großem Umfang nicht der deutschen Sprache mächtig und Deutsch war offenkundig nicht die Arbeitssprache. Die Formulare und Ausfüllhinweise sind dort bislang ausschließlich in deutscher Sprache verfügbar. In diesem speziellen Einzelfall war zweifelhaft, ob die zuständige Stelle ihrer Pflicht nach § 11 Abs. 1 S. 2 SÜG nachgekommen war, wonach u. a. die betroffene Person auf den Zweck der Erhebung, die Auskunftspflichten nach dem SÜG und auf eine dienst-, arbeitsrechtliche oder sonstige vertragliche Mitwirkungspflicht, sowie ansonsten auf die Freiwilligkeit ihrer Angaben hinzuweisen ist. Ich habe der kontrollierten Stelle empfohlen, in derartigen Fällen eine Höflichkeitsübersetzung vorzuhalten.

Die vorstehenden Ausführungen zeigen eines deutlich: Der Beratungsbedarf ist nach wie vor ungebrochen, ebenso wie das Schulungsbedürfnis seitens der zuständigen Stellen und geheim- und sabotageschutzbetreuten Unternehmen. Sehr oft klagen die zuständigen Bearbeiterinnen und Bearbeiter der kontrollierten Stellen, überwiegend im öffentlichen Bereich, über mangelnde personelle Ausstattung, fehlende technische Unterstützung oder mangelnde Aus- und Fortbildungsmöglichkeiten.

Auch die Bürgerinnen und Bürger als (mit-)betroffene Personen einer Sicherheitsüberprüfung wenden sich immer wieder mit Fragen und Problemen bei der Durchsetzung ihrer Betroffenenrechte an mich; nicht selten werden dabei Doppelüberprüfungen oder (Sicherheits-) Überprüfungen ohne Rechtsgrundlage beklagt. So wurde auch eine meiner diesjährigen Kontrollen aufgrund einer Bürgereingabe veranlasst.

Positive Entwicklungen und neue Beratungsformate

Im Berichtsjahr zeigten sich erfreulicherweise auch positive Entwicklungen aufgrund von Beratungsaktivitäten und weiteren Maßnahmen meiner Behörde. So sorgte die Zollverwaltung ebenso wie das Bundesamt für Justiz und das Bundesministerium für Gesundheit jeweils aufgrund meiner Beanstandung für personelle Verstärkung in den Organisationseinheiten der Geheim- und Sabotageschutzbetreuung. Das Bundesministerium des Innern und für Heimat stoppte als Aufsichtsbehörde umgehend nach Erhalt meines Kontrollberichts per Erlass die Vorratsüberprüfungen von Ersatzkandidatinnen und Ersatzkandidaten im Bewerbungsverfahren beim Bundesamt für Migration und Flüchtlinge. Um an diese positiven Entwicklungen anzuknüpfen, werde ich künftig der datenschutzrechtlichen Information und Beratung bei meinen Kontrollbesuchen einen noch höheren Stellenwert beimessen und meine Öffentlichkeitsarbeit weiter ausbauen.

Unabhängig von den Kontrollen führte mein Haus anlässlich der im Gesetz über den Bundesnachrichtendienst und im Bundesverfassungsschutzgesetz mit Wirkung zum 1. Januar 2024 bzw. 30. Dezember 2023 eingeführten Eigensicherungsvorschriften beim Bundesamt für den Verfassungsschutz und dem Bundesnachrichtendienst jeweils einen Informations- und Beratungsbesuch durch. Die in diesem Rahmen von den Behörden vorgestellte Umsetzung der neuen Regelungen offenbarte keine datenschutzrechtlichen Defizite.

Zudem veranstalteten meine Mitarbeitenden in diesem Jahr erstmals einen informellen Austausch mit der Datenschutzbeauftragten und der Geheimschutzbeauftragten des Bundesministeriums der Verteidigung (BMVg) zu Themen rund um Sicherheitsüberprüfungen im Geschäftsbereich des BMVg. Gegenstand des Austausches war insbesondere die geplante Einführung der elektronischen Sicherheitsakte.

Querverweis:

7.4.5 Sicherheitsüberprüfungen in der Wirtschaft

8.1.3 Kontrolle der Anti-Terror-Datei und der Rechtsextremismus-Datei

Wie in den vergangenen Jahren[151] habe ich auch in diesem Berichtszeitraum die Pflichtkontrollen zur Anti-Terror-Datei (ATD) und Rechtsextremismus-Datei (RED) durchgeführt. Bei den bereits Ende 2023 begonnen Kontrollen verfolgte ich dieses Mal einen behördenübergreifenden Beratungs- und Kontrollansatz, der primär der Effizienz diente.

151 31. TB Nr. 9.4.4

Die von mir zu kontrollierenden Bundesbehörden sind in Bezug auf die ATD das Bundeskriminalamt (BKA), die Bundespolizei (BPOL), das Zollkriminalamt (ZKA), das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für den militärischen Abschirmdienst (BAMAD) und der Bundesnachrichtendienst (BND), sowie in Bezug auf die RED das BKA, die BPOL, das BfV und das BAMAD. Beim ZKA, dem BND, dem BAMAD, dem BfV und der BPOL habe ich keine datenschutzrechtlichen Defizite festgestellt. Sämtliche Verarbeitungen standen im Einklang mit den gesetzlichen Vorgaben. Im Übrigen waren die Kontrollen zum Zeitpunkt der Erstellung dieses Berichtes noch nicht abgeschlossen. Es steht jedoch bereits fest, dass jedenfalls keine größeren Datenschutzverstöße vorliegen.

Neuer behördenübergreifender Kontrollansatz

Bei der ATD und RED sind die Behörden auf unterschiedliche Weise an diese Dateien angebunden; nicht alle nutzen eine automatisierte Speicherungsschnittstelle. Darüber hinaus kommen die einzuspeichernden Dateien aus verschiedenen Quelldateien. Auch habe ich eine unterschiedliche Dokumentationspraxis der beteiligten Sicherheitsbehörden beobachtet.

Obwohl vor diesem Hintergrund ein einheitlicher Beratungs- und Kontrollansatz nicht leicht zu verwirklichen ist, sollte dieses Mal zur bestmöglichen Vereinheitlichung und Effizienzmaximierung der einzelnen Beratungen und Kontrollen ein übergreifender Ansatz für die von mir kontrollierten Bundesbehörden angewendet werden. Um die bei einigen kontrollierten Stellen aufwendige Einsichtnahme vor Ort zu verschlanken, wollte ich mir zur präziseren Vorbereitung im schriftlichen Verfahren einen Überblick über den aktuellen Datenbestand und die Veränderungen an beiden Dateien im Kontrollzeitraum verschaffen. Die dazu notwendigen Zulieferungen gestalteten sich schwierig und langwierig.

Obwohl in meiner Behörde alle Erfordernisse des Geheimschutzes eingehalten werden, hatten die beteiligten Behörden aufgrund des Umfangs der angeforderten Daten Bedenken, diese zu übersenden. Ich habe dafür zwar dem Grunde nach Verständnis, sehe aber durch die Weigerung meine Kontrollrechte ohne objektiven Grund eingeschränkt. Um den Kontrollbeginn nicht noch weiter in die Zukunft zu schieben, konnte schließlich ein Kompromiss gefunden werden. Der von mir erhoffte Effizienzgewinn konnte als Folge des Kompromisses nicht gehoben werden. Ich sehe nach den hier gemachten Erfahrungen insbesondere die Gefahr, dass meine Beratungs- und Kontrolltätigkeit durch zögerliche Übersendung von Unterlagen erschwert wird.

Trotzdem konnte ich durch meinen neuen Kontrollansatz anhand der übergreifenden Auswertung der Protokolldaten erkennen, ob mehrere Behörden Speicherungen zu gleichen Personen vorgenommen hatten. Diese Speicherungen habe ich bei den jeweiligen Behörden sodann besonders intensiv geprüft und habe erfreulicherweise festgestellt, dass diese Mehrfachspeicherungen im Einklang mit den gesetzlichen Vorschriften standen. Durch meinen neuen Ansatz konnte ich somit – trotz der verzögerten Übersendung der Unterlagen – eine Erhöhung der Beratungs- und Kontrollqualität erreichen. Die künftigen Beratungen und Kontrollen möchte ich daher auch weiterhin optimieren, um meiner gesetzlichen Pflicht zur Beratung und Kontrolle in gebotenem Maße und mit Detailtiefe effizient nachkommen zu können. Dabei sollten mich die kontrollierten Stellen auch weiterhin aktiv unterstützen und offen für meine Information und Beratung sein.

ATD und RED werden kaum genutzt

Die Möglichkeit des Vergleichs der Nutzung durch die diversen Bundesbehörden im Wege des übergreifenden Kontrollansatzes bestätigte erneut den schon in meinen vorherigen Berichten immer wieder beschrieben Eindruck, dass es sich bei der ATD und der RED um wenig nützliche Instrumente für die Sicherheitsbehörden handelt, die dementsprechend auch nur wenig genutzt werden. Angesichts des gleichzeitig weitreichenden Grundrechtseingriffs aufgrund der großen Anzahl der angeschlossenen Behörden und der gespeicherten sensiblen Daten halte ich an meiner Forderung [152] einer Reform beider Dateien weiterhin fest.

Ich empfehle dem Gesetzgeber, gemeinsam mit meiner Behörde und allen beteiligten Behörden über eine Reform der ATD und der RED zu sprechen.

8.1.4 Kontrolle des Gemeinsamen Extremismus- und Terrorismusabwehrzentrums

Im Berichtsjahr habe ich u. a. auf Basis der neuen Übermittlungsvorschriften für die Nachrichtendienste die Kontrolle des Gemeinsamen Extremismus- und Terrorismusabwehrzentrums (GETZ) begonnen.

Bereits in den Jahren 2022/2023 habe ich mit dem Gemeinsamen Terrorismusabwehrzentrum (GTAZ) eines

152 31. TB Nr. 9.4.4

der Gemeinsamen Zentren kontrolliert, in dem verschiedene Sicherheitsbehörden des Bundes und der Länder zusammenarbeiten. Dabei habe ich festgestellt, dass nicht jedes Arbeitsformat im GTAZ mit datenschutzrechtlichen Bestimmungen in Einklang zu bringen ist.[153] Ferner wurden damals Praxisempfehlungen zur Stärkung des Datenschutzes ausgesprochen.

Auch habe ich damals begrüßt, dass die Bundesregierung die Schaffung von expliziten Rechtsgrundlagen für die Gemeinsamen Zentren in den Koalitionsvertrag aufgenommen hat und ihr zu diesem Thema ein Beratungsangebot unterbreitet. Ich bedauere, dass dieses Vorhaben in der 20. Legislaturperiode nicht aufgegriffen wurde.

Da mit dem Gesetz zum ersten Teil der Reform des Nachrichtendienstrechts vom 22. Dezember 2023 der Gesetzgeber allerdings die Übermittlungsvorschriften aus dem Bereich der Nachrichtendienste reformiert und Protokollierungsvorschriften angepasst hat, habe ich mich dazu entschieden, trotz fehlender spezialgesetzlicher Übermittlungsvorschriften auch in diesem Berichtsjahr mit dem GETZ erneut ein Gemeinsames Zentrum zu kontrollieren.

Ziel des GETZ ist die Bekämpfung des Rechts-, Links- und auslandsbezogenen Extremismus sowie der Spionage einschließlich Proliferation. Für alle diese vier Phänomenbereiche finden in unterschiedlichen Intervallen Sitzungen in speziellen Arbeitsgruppen statt. Neben den 16 Landeskriminalämtern und 16 Landesämtern für Verfassungsschutz sind folgende Bundesbehörden im GETZ vertreten: Bundesamt für Verfassungsschutz, Bundesamt für den Militärischen Abschirmdienst, Bundesnachrichtendienst, Bundeskriminalamt, Generalbundesanwalt, Bundespolizei, Generalzolldirektion/Zollkriminalamt sowie das Bundesamt für Migration und Flüchtlinge. Dementsprechend besteht mein Beratungs- und Kontrollteam aus Mitarbeitenden der für diese Behörden zuständigen Referate.

In der Kontrolle prüfe ich phänomenbereichsübergreifend in vier Arbeitsgruppen, u. a. in der Arbeitsgruppe Lage, in welcher aktuelle lagerelevante Erkenntnisse ausgetauscht werden, ob die im GETZ vertretenen Bundesbehörden die gesetzlich geregelten Voraussetzungen für die Übermittlung von personenbezogenen Daten einhalten und ihr Handeln entsprechend dokumentieren. Dafür hat sich mein Kontrollteam zunächst in einem Informationsbesuch sämtliche Arbeitsgruppen des GETZ inklusive Arbeitsabläufen vorstellen lassen und offene Fragen geklärt. Sowohl im Rahmen des Informationsbesuches als auch im eigentlichen Kontrollzeitraum hat das Kontrollteam an mehreren Sitzungen der Arbeitsgruppen teilgenommen. Da die Kontrolle vor Ort zum Zeitpunkt des Redaktionsschlusses noch andauerte, werde ich über das Ergebnis meiner Kontrolle im nächsten Tätigkeitsbericht informieren.

8.1.5 Beratung und Kontrolle des BfV

Der Berichtszeitraum war wieder umfänglich mit Kontroll- sowie Beratungs- und Informationsbesuchen beim Bundesamt für Verfassungsschutz (BfV) ausgefüllt. Ich habe Speicherungen im Nachrichtendienstlichen Informationssystem (NADIS) einer Kontrolle unterzogen. Die Kontrolle und auch Beratung zu der elektronischen Akte beim BfV wurde als Schwerpunkt in Bezug auf Personensuchen fortgesetzt und konnte zuletzt erfolgreich abgeschlossen werden. Aber auch die heimliche Informationsbeschaffung, die Aufklärung im Internet sowie die verschiedenen Dateien des BfV wurden unter die hiesige „Datenschutzlupe" genommen, um das BfV in Sachen Datenschutz bestmöglich unterstützen zu können. Des Weiteren habe ich die Kontrolle der Datenverarbeitung in Zusammenhang mit der Berichterstattung des BfV zu Ende geführt.

Kontrolle NADIS

NADIS ist die gemeinsame Datei des Verbundes aus Bundesamt für Verfassungsschutz und Landesbehörden für Verfassungsschutz (VS-Verbund) – seit Neuerem auch mit Anbindung des Bundesamts für den Militärischen Abschirmdienst (BAMAD). NADIS enthält Speicherungen aller Personen und Objekte, die für den Beobachtungsauftrag des Verfassungsschutzes als relevant betrachtet werden. Die Datei ermöglicht Verknüpfungen der Informationen und ist damit ein wichtiges Analysetool der Behörden. Bei meiner diesjährigen Beratung und Kontrolle habe ich konkrete Speicherungen von personenbezogenen Daten im NADIS überprüft und dabei einen Schwerpunkt auf dem Prozess der Erstspeicherung gelegt.

Die Kontrolle hat keine wesentlichen Verstöße gegen datenschutzrechtliche Bestimmungen hinsichtlich des Kontrollgegenstandes ergeben. Positiv kann herausgestellt werden, dass alle kontrollierten Speicherungen in der Sache als plausibel bewertet werden konnten. Ich habe aber auch Verbesserungspotential hinsichtlich der Praxis zur Dokumentation der Erstspeicherungen an das BfV beratend herangetragen. Das BfV strebt hier

153 32. TB Nr. 9.1.9

nunmehr eine hausweite Standardisierung der Speicherverfügung an.

Die Speicherungen in NADIS, deren Voraussetzungen sowie die genaue Ausgestaltung und Darstellung in dieser zentralen Datenbank des VS-Verbundes werden auch in Zukunft wichtige Themen meiner Beratung und Kontrolle bleiben.

Elektronische Akte beim BfV

Zwischenzeitlich konnte die bereits im vorherigen Tätigkeitsbericht[154] vorgestellte Folgekontrolle der elektronischen Akte des BfV erfolgreich abgeschlossen werden. Die Beratung und Kontrolle befasste sich schwerpunktmäßig mit den Möglichkeiten der Personensuche im elektronischen Aktenbestand des BfV. Eine solche Suche ist überhaupt nur unter Beachtung des engen gesetzlichen Rechtsrahmens des Bundesverfassungsschutzgesetzes (BVerfSchG) zulässig. Der positive Ersteindruck bestätigte sich bis zum Abschluss der Kontrolle. Ich konnte keine materiellen Datenschutzverstöße feststellen.

Der Kontrollansatz wurde zusammen mit dem BfV als Kompensation für technische Maßnahmen entwickelt und die unmittelbar daraus resultierende Eigenkontrolle des BfV durch meine Behörde als Folgekontrolle eng begleitet. Das BfV führt aktuell eigenverantwortlich die weitere Folgekontrolle für den neuen Kontrollzeitraum durch und berichtet mir die (Zwischen)Ergebnisse. In Bezug auf die künftige elektronische Akte und das Dokumentenmanagementsystem im Verfassungsschutzverbund (Verbund-DMS) rate ich weiterhin die Entwicklung von technischen organisatorischen Maßnahmen zur Begrenzung der Volltextsuche an.

Ich bin zuversichtlich, dass die kürzlich seitens des BfV durchgeführten Sensibilisierungsmaßnahmen bei seinen Mitarbeitenden sowie die meinerseits initiierten Beratungs- und Kontrollmaßnahmen wieder zu einem ähnlich erfreulichen Ergebnis führen werden und dadurch noch einmal die positive Auswirkung meiner Beratungs- und Kontrollbesuche – insbesondere auch vor Ort – unterstrichen wird.

Informationsschreiben des BfV

In meinem 31. Tätigkeitsbericht[155] habe ich dargestellt, dass die Übermittlung personenbezogener Daten im Rahmen der Berichterstattung des BfV nicht den gesetzlichen Bestimmungen entspricht. In die Berichte wurden teilweise personenbezogene Daten aufgenommen, ohne dass für alle Datenübermittlungen eine Rechtsgrundlage erkennbar gewesen wäre. Es wurde nicht hinreichend zwischen den sehr unterschiedlichen Empfängern und den jeweiligen Aufgabenbereichen des BfV (z. B. Links- oder Rechtsextremismus) differenziert, sondern die Informationsschreiben pauschal immer an einen großen Verteiler gesendet.

Im Rahmen einer schriftlichen Kontrolle habe ich die Berichte von mehreren Monaten geprüft und die enthaltenen Datenverarbeitungen ausgewertet. Im Anschluss habe ich das BfV dahingehend beraten, welche Übermittlungen rechtlich zulässig sind. Das BfV hat seine Verfahrensweise daraufhin angepasst und die Verwendung personenbezogener Daten deutlich eingeschränkt. Somit konnte ich die Kontrolle im Frühjahr 2024 ohne Beanstandung abschließen.

Kontrolle von Datenabrufen im AZR

Das Ausländerzentralregister (AZR) stellt die zentrale Informationsdrehscheibe im Ausländer- und Asylrecht dar und enthält über 26 Millionen personenbezogene Datensätze über Ausländerinnen und Ausländer, die sich länger als drei Monate in Deutschland aufhalten. Auch personenbezogene Daten über Unionsbürger werden im AZR gespeichert, sofern diese bspw. nicht mehr freizügigkeitsberechtigt sind. Das Register wird beim Bundesamt für Migration und Flüchtlinge (BAMF) geführt.

Nicht nur die besonders große Datenmenge im AZR, sondern gerade auch die Speicherung von äußerst sensiblen Daten (z. B. Gesundheitsdaten oder Fingerabdrücke) hat mich dazu veranlasst, Zugriffe des BfV im AZR zu prüfen und eine datenschutzrechtliche Beratung und Kontrolle durchzuführen. Nachrichtendienste des Bundes sind berechtigt, Datenabrufe im AZR im sog. automatisierten Verfahren gemäß § 22 Abs. 1 S. 1 Nr. 9 Ausländerzentralregistergesetz (AZRG) durchzuführen. Nach Erhalt der erforderlichen Zulassung durch das Bundesverwaltungsamt (BVA), welches für das BAMF als Dienstleister tätig ist, kann das BfV im Direktzugriff umfangreiche Daten im AZR einsehen und verarbeiten. Der Direktzugriff bietet für das BfV den Vorteil, dass ohne Kenntnisnahme durch das BVA oder das BAMF Daten abgerufen und gespeichert werden können. Anders als bei Übermittlungen, die ein vorhergehendes Ersuchen bzw. Antragsverfahren voraussetzen, wird die Erforderlichkeit des Abrufs ausschließlich vom BfV und nicht vom BVA oder vom BAMF beurteilt und kontrolliert.

154 32. TB Nr. 9.1.7
155 31. TB Nr. 7.8

Meine datenschutzrechtliche Beratung und Kontrolle dauert zum Ende des Berichtszeitraums noch an. Allerdings hat das BfV bereits jetzt Verbesserungen zum Verfahrensablauf vorgenommen und die Dokumentation von AZR-Abrufen näher konkretisiert. So wurde u. a. das gesetzlich vorgesehene Berechtigungskonzept (§ 22 Abs. 3 S. 3 AZRG) angepasst und transparenter gestaltet. Auch das Prozedere zur Ermächtigung von Mitarbeitenden zum Datenabruf im AZR wurde infolge meiner Beratung geändert. Weitergehende Informationen kann ich derzeit aufgrund der andauernden Prüfung sowie aus Gründen der Geheimhaltung nicht erteilen.

Kontrolle der Aufklärung im Internet

Die Aufklärung im Internet, auch bekannt als Open Source Intelligence oder kurz OSINT, ist ein Schwerpunkt der Aufgaben des BfV. Folglich ist sie auch ein dauerhafter Schwerpunkt meiner Beratung und Kontrolle. Im Berichtszeitraum habe ich die verschiedenen Maßnahmen von der Einsichtnahme in allgemein zugängliche Informationen bis hin zur eingriffsintensiven Aufklärung im Internet durch heimliche Informationsbeschaffung kontrolliert. Dieser Bereich unterliegt aufgrund einer stetigen Weiterentwicklung der Plattformen und der häufig wechselnden Art der Nutzung der verschiedenen Kommunikationswege einem stetigen Wandel.

Im Rahmen meiner Kontrolle habe ich die aktuelle Vorgehensweise des BfV geprüft und ein besonderes Augenmerk auf die Frage gelegt, ob die Tiefe des Eingriffes in Bezug auf die vorliegenden Erkenntnisse nachvollziehbar sind. Hierbei habe ich festgestellt, dass die rechtlichen Grundlagen für die durch das BfV vorgenommenen Erhebungen und Weiterverarbeitungen von Daten aus dem Internet nicht immer nachvollziehbar sind.

Dass eine Verarbeitung von frei zugänglichen Daten im Internet für das BfV im Rahmen seiner Aufgabenerfüllung grundsätzlich möglich ist, steht hierbei außer Frage. Allerdings müssen die Befugnisse des BfV sowohl durch eine klare gesetzliche Regelung als auch durch aktuelle interne Handlungsanweisungen klar definiert und im Verhältnis zum Zweck der Verarbeitung angemessen sein. Dies ist nach derzeitigem Stand nur eingeschränkt der Fall. Es bedarf einer rechtlichen Präzisierung und einer klaren internen Handlungsvorgabe.

Analoge heimliche Informationsbeschaffung

Neben der gerade dargestellten Informationsbeschaffung im Internet sammeln Nachrichtendienste auch weiterhin Informationen in der realen Welt. Geschieht dies heimlich, spricht man von nachrichtendienstlichen Mitteln. Nur einige davon sind im BVerfSchG explizit geregelt, wie z. B. der Einsatz verdeckter Mitarbeiter oder Vertrauensleuten (auch oft V-Personen genannt).

Eine vollständige Aufzählung dieser nachrichtendienstlichen Mittel findet sich, wie in § 8 Abs. 2 S. 4 BVerfSchG geregelt, bislang nur in einer Dienstvorschrift des BfV, die der Zustimmung des Bundesministeriums des Innern und für Heimat (BMI) unterliegt. Diese Dienstvorschrift ist als Verschlusssache eingestuft. Daher kann ich an dieser Stelle auch nur sehr abstrakt berichten, dass ich im Berichtszeitraum den Einsatz eines solchen Mittels kontrolliert habe. Beim Einsatz selbst habe ich in meiner Kontrolle keine datenschutzrechtlichen Defizite festgestellt.

Allerdings ist das fragliche Mittel in der genannten Dienstvorschrift nicht ausdrücklich beschrieben. Das BfV subsumierte es unter ein dort namentlich genanntes Mittel. Diese Auffassung konnte ich nicht nachvollziehen und kontaktierte das BMI als zuständige Fachaufsicht. Aus meiner Sicht muss jedes nachrichtendienstliche Mittel ausdrücklich benannt und die Anforderungen für seinen Einsatz festgelegt sein.

Das BMI hat hier, für mich nicht nachvollziehbar, keinen Handlungsbedarf gesehen und auf eine ohnehin anstehende Gesetzesnovellierung zum BVerfSchG verwiesen, mit der allerdings im Berichtszeitraum leider noch nicht begonnen wurde.

Informationsbesuche zu verschiedenen Dateien des BfV

Sofern das BfV personenbezogene Daten in Dateien speichern möchte, bin ich vor Inbetriebnahme der Datei im Rahmen eines Dateianhörungsverfahrens gemäß § 14 BVerfSchG zu beteiligen. Bereits im vergangenen Berichtsjahr habe ich in diesem Zusammenhang über ein Werkzeug zur Beobachtung des Internets berichtet, bei dem ich bereits frühzeitig im Beschaffungsprozess eingebunden wurde und vor Ort das „Proof of Concept“ (PoC), also die Testphase der Datei, kontrolliert habe. [156]

Im Rahmen dieses PoC habe ich mehrere datenschutzrechtliche Verstöße und Mängel festgestellt, die bei der Inbetriebnahme der Datei zu einer Beanstandung geführt hätten. Diese bezogen sich u. a. auf fehlende technisch organisatorische Maßnahmen gemäß § 27 Nr. 2 BVerfSchG i. V. m. § 64 Abs. 1 S. 1 BDSG. Auf weitere Details kann ich aus Geheimschutzgründen nicht

156 32. TB Nr. 9.1.7

eingehen. Da sich das BfV aber bereits kurz nach meiner Beratung und Kontrolle dazu entschieden hat, das PoC einzustellen und die Datei nicht einzuführen, habe ich von einer Beanstandung abgesehen.

In diesem Berichtsjahr habe ich mir in einem Informationstermin diejenige Datei vorführen lassen, die nunmehr alternativ zu dem eingestellten Verfahren eingeführt werden soll. Der neue PoC, in dessen Rahmen die Software umfangreichen technischen und fachlichen Tests unterzogen wird, war zum Redaktionsschluss noch nicht abgeschlossen. Auch diesen Prozess werde ich weiterhin eng beratend begleiten und datenschutzrechtlich bewerten.

Dieses Dateianhörungsverfahren ist nicht das einzige im Berichtsjahr, das Verfahren zur Beobachtung und Aufklärung im Internet zum Gegenstand hat. Das erklärt sich aufgrund der Vielfalt von Internetdiensten, der hier mit spezialisierten Verfahren zur Aufklärung begegnet wird.

Neben den neuen Dateien zur eigentlichen Internetbeobachtung gibt es auch eine weitere Datei in einem laufenden Anhörungsverfahren, die aufgrund der rapide wachsenden Größe und Vielfalt unstrukturierter Daten zur Auswertung durch den Verfassungsschutz eingeführt werden soll. Auch hier stehen ebenfalls Geheimschutzgründe einer genaueren Beschreibung entgegen. Aber es ist naheliegend, dass dieses gesamte Themenumfeld der Datenerhebung im Internet und der Umgang mit unter anderem dabei entstehenden komplexen unstrukturierten Datenmengen aktuell ein Schwerpunkt meiner Arbeit ist.

Querverweis:

7.4.2 OSINT-Beobachtungen im Internet

8.1.6 Beratung und Kontrolle des BAMAD

Das Bundesamt für den Militärischen Abschirmdienst (BAMAD) hat umfassende nachrichtendienstliche Befugnisse. Datenschutzrechtlich relevant sind hier, ähnlich wie beim Bundesamt für Verfassungsschutz, u. a. die Aufklärung im Internet und die Anbindung der Behörde an die Verbunddatei des Nachrichtendienstlichen Informationssystems (NADIS). Dass es dabei zu Friktionen kommen kann, zeigt sich insbesondere in der Bearbeitung der Eingaben von Bürgerinnen und Bürgern, die mich im Rahmen von Auskunftsersuchen um Unterstützung bitten.

Ich habe die Pflicht, Bürgerinnen und Bürger auf dem Weg des Auskunftsersuchens im Bereich der Nachrichtendienste des Bundes individuell zu begleiten. Ich nehme damit stellvertretend die Rechte der Betroffenen wahr, da diese über keine eigenen Einsichtsrechte verfügen und Auskünfte seitens der Dienste mitunter Beschränkungen unterliegen können.

In diesem Kontext ist es mir in meinem Zuständigkeitsbereich auch möglich, vorgetragene Sachverhalte durch konkrete Kontrollmaßnahmen zu überprüfen, datenschutzrechtlich zu bewerten und das BAMAD als verantwortliche Stelle zu informieren und beraten. Die erforderliche Sachverhaltsklärung erfolgt durch meine Mitarbeitenden zunächst im Rahmen einer ersten schriftlichen Kontaktaufnahme mit dem dafür zuständigen Datenschutzreferat des BAMAD. Darüber hinaus erforderliche Beratungen und Einsichtnahmen vor Ort werden durch meine Mitarbeitenden koordiniert und durchgeführt, wenn dies angezeigt ist. So kann regelmäßig eine umfassende und zielgerichtete Bewertung der zugrundeliegenden Sachverhalte und Beratung für einen datenschutzkonformen Umgang sichergestellt werden.

Das ist wichtig, weil sich leider immer wieder zeigt, dass das Auskunftsrecht seitens des BAMAD häufig restriktiv ausgelegt wird. Dabei könnten nach meiner Auffassung anstelle einer Nicht- oder Teilauskunft oftmals sehr wohl mehr Informationen mitgeteilt werden, ohne dadurch womöglich geheimhaltungsbedürftige nachrichtendienstliche Arbeitsweisen offenzulegen oder gegen Vorschriften des Geheimschutzes zu verstoßen.

Aus meiner Sicht zeichnet sich für die Beratung und Kontrolle des BAMAD eine positive Tendenz bzw. Entwicklung ab. Bei den von mir bearbeiteten Fällen konnten im Nachgang mehrfach noch weitere Informationsbedürfnisse der Petentinnen und Petenten befriedigt und datenschutzrechtliche Belange im Einvernehmen erörtert werden. Das begrüße ich deutlich. Ich wünsche mir für die Zukunft auf Seiten des BAMAD noch mehr Offenheit und Eigeninitiative bei der Beantwortung von Auskunftsersuchen. Das schafft Rechtssicherheit für den Datenschutz und die Betroffenen zugleich. Ich werde dem BAMAD hierzu auch weiter beratend zur Verfügung stehen.

Anbindung des BAMAD an NADIS

Im Laufe des Jahres 2023 wurde die Vollanbindung das BAMAD an das NADIS, die gemeinsame Datei des Verbundes aus Bundesamt für Verfassungsschutz und Landesbehörden für Verfassungsschutz, umgesetzt. Ich

hatte die Verflechtung der Dateiensysteme der verschiedenen Nachrichtendienste des Bundes kritisch begleitet.[157] Das BAMAD hatte angekündigt, dass die Zulässigkeit der jeweiligen Abrufe aus NADIS durch mehrere Sicherungsinstanzen technischer und organisatorischer Art gewährleistet werden wird. Im diesjährigen Berichtszeitraum habe ich daher eine Kontrolle der Nutzung des NADIS durch das BAMAD durchgeführt. Zum Zeitpunkt des Redaktionsschlusses dauerte diese Kontrolle noch an, so dass ich erst im nächsten Tätigkeitsbericht über die Ergebnisse berichten kann.

Aufklärung im Internet

Verfassungsfeindliche und staatsgefährdende Aktivitäten verlagern sich zunehmend ins Internet und insbesondere in die Sozialen Netzwerke. Als Reaktion hierauf ist auch die Sammlung und Auswertung von frei verfügbaren und nicht frei zugänglichen Informationen im Internet seit Jahren eine wichtige Aufgabe der nachrichtendienstlichen Tätigkeit. Deshalb habe ich auch die Verarbeitung von personenbezogenen Daten im Zusammenhang mit der Internetbearbeitung einer Fachabteilung des BAMAD kontrolliert.

Datenschutzrechtliche Verstöße habe ich nicht festgestellt. Aus datenschutzrechtlicher Sicht ist vielmehr zu begrüßen, dass das BAMAD für den Bereich der Internetbearbeitung der kontrollierten Abteilung eine interne Bereichsvorschrift erlassen hat, die als Anlage auch den Auftragsvordruck enthält. Im Rahmen der Beratung und Kontrolle musste ich allerdings feststellen, dass in der Praxis in vielen Fällen die Anordnungen nicht gemäß der eigenen Bereichsvorschrift erfolgten. Entweder weil der Auftragsvordruck überhaupt nicht verwendet oder von einer nicht anordnungsbefugten Person gezeichnet wurde.

Da das BAMAD bereits in der Kontrolle die Mängel eingesehen und Abhilfe zugesagt hat, wurde – trotz der Vielzahl an Fällen – von einer Beanstandung dieser Mängel gemäß § 16 Abs. 2 S. 2 BDSG abgesehen und stattdessen lediglich Praxisempfehlungen ausgesprochen.

Querverweis:

7.4.2 OSINT-Beobachtung im Internet

8.1.7 Das Militärische Nachrichtenwesen in der Diskussion

Bereits seit geraumer Zeit fordere ich vom Gesetzgeber die Schaffung einer einfachgesetzlichen Grundlage für das Militärische Nachrichtenwesen (MilNW). Neben dem Bundesnachrichtendienst (BND), dem Bundesamt für Verfassungsschutz (BfV) und dem Bundesamt für den Militärischen Abschirmdienst (BAMAD) ist das MilNW der vierte Nachrichtendienst auf Bundesebene. Doch während BND, BfV und BAMAD jeweils auf Grundlage eines spezifischen Gesetzes ihrem Auftrag nachkommen, fehlt diese spezialgesetzliche Rechtsgrundlage beim MilNW.

Beim MilNW handelt es sich um unterschiedliche Bereiche der Bundeswehr, die – wie ein Nachrichtendienst – für die weltweite Gewinnung von Informationen zuständig sind. Aufgabe und Ziel dieser Nachrichtengewinnung und Aufklärung ist die Deckung des militärischen Informationsbedarfes für die Bundesregierung, für die Leitung des Bundesministeriums der Verteidigung (BMVg) und für die militärischen Führungsebenen wie zum Beispiel die Kommandeure.

Fehlen einer einfachgesetzlichen Rechtsgrundlage

Das MilNW bildet, in enger Zusammenarbeit mit dem BND, den militärischen Auslandsnachrichtendienst der deutschen Streitkräfte. Diese Aufgabe ist „in der Zeitenwende“ noch wichtiger geworden ist. Die Zusammenarbeit erstreckt sich auf den personellen und technischen Bereich sowie den stetigen Austausch von erlangten Informationen und Analysen. Ebenso unterstützt der BND die Bundeswehr bei mandatierten Auslandseinsätzen.

Obwohl das MilNW zum Teil exakt wie der BND agiert, sieht die Bundesregierung keinen Anlass für die Schaffung einer einfachgesetzlichen Grundlage. Spätestens seit dem Urteil des Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung des BND aus dem Jahr 2020[158] sehe ich die Erforderlichkeit der Schaffung von expliziten Rechtsgrundlagen für das MilNW als höchstrichterlich bestätigt an.

Daher halte ich meine Forderung nach der Schaffung einer einfachgesetzlichen Rechtsgrundlage aus datenschutzrechtlichen Gründen weiter aufrecht. Für die Handlungs- und Rechtssicherheit des MilNW ist es erforderlich, Datenverarbeitungsbefugnisse durch das Parlament zu setzen.

---

157 31. TB Nr. 9.4.10 und 32. TB Nr. 9.1.8

158 Urteil des BVerfG vom 19. Mai 2020, 1 BvR 2835/17, abrufbar unter: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html

Gerne biete ich hierzu meine Unterstützung und Beratung an.

Kontrollen beim MilNW

Abseits meiner Forderung zur Schaffung einer expliziten Rechtsgrundlage für das MilNW habe ich im Berichtszeitraum zwei datenschutzrechtliche Beratungen und Kontrollen beim MilNW durchgeführt. Der Rahmen wird durch die hilfsweise anzuwendenden allgemeinen Datenschutzvorschriften der DSGVO gebildet.

Eine im Jahr 2023 begonnene und im Jahr 2024 abgeschlossene Beratung und Kontrolle bezog sich auf das zentrale Datenverarbeitungssystem des MilNW. Dabei wurden mehrere datenschutzrechtliche Verstöße und Mängel festgestellt. Eine von mir festgestellte Vorratsdatenspeicherung mit einem damit einhergehenden Verstoß gegen den Beschäftigtendatenschutz habe ich auf Grund der Schwere des Verstoßes beanstandet. Aufgrund der bereits im Kontrolltermin bei den Vertreterinnen und Vertretern des MilNW bestehenden Einsicht und Bereitschaft, die übrigen von mir festgestellten Verstöße und Mängel schnellstmöglich abzustellen, habe ich von einer weiteren Beanstandung abgesehen. Stattdessen habe ich beratend mehrere Praxisempfehlungen ausgesprochen. In der Stellungnahme des BMVg zu meinem Kontrollbericht wurde zugesagt, dass sämtliche von mir aufgeführten Punkte bereits aufgegriffen wurden bzw. zeitnah aufgegriffen werden. Ich werde prüfen, ob meine Empfehlungen vollständig umgesetzt wurden.

Die zweite Beratung und Kontrolle bezog sich auf eine Datei, welche zur Krisenfrüherkennung und Lageanalyse eingesetzt wird. Hierfür hat sich zunächst das Kompetenzzentrum für Krisenfrüherkennung bei der Universität der Bundeswehr in München meinen Mitarbeitenden vorgestellt. In einem weiteren Termin haben meine Mitarbeitenden die eigentliche Datei kontrolliert. Schwerwiegende Datenschutzverstöße habe ich nicht festgestellt. Zu den von mir zur Beratung und Information ausgesprochenen Praxisempfehlungen zum weiteren Umgang mit der Datei werde ich in engem Kontakt mit dem dem BMVg bleiben.

Ich halte meine Forderung nach der Schaffung einer einfachgesetzlichen Rechtsgrundlage für das Militärische Nachrichtenwesen weiter aufrecht. Für die Handlungs- und zugleich Rechtssicherheit der Bundeswehr ist es erforderlich, notwendige Befugnisse in demokratisch legitimierten Gesetzen zu regeln.

8.1.8 Informations- und Beratungsbesuch beim BND

Wie bereits im vorigen Jahr, habe ich mir auch dieses Jahr einen Bereich des Bundesnachrichtendienstes (BND) genauer angeschaut. Die Wahl ist auf den Bereich gefallen, der im BND für die Informationsbeschaffung verantwortlich ist. Dort wird die Informationserhebung zunächst koordiniert und dann durch spezialisierte Beschaffungsreferate gezielt umgesetzt.

Der BND hat sich eine neue Struktur mit sechs zentral zuständigen Bereichen gegeben. Bereits im vorigen Jahr habe ich einen dieser Bereiche – den Bereich Auswertung – kontrolliert.[159]

In diesem Berichtsjahr habe ich mich dem Bereich der Beschaffung gewidmet. Damit der BND seinem Aufklärungsauftrag nachkommen kann, müssen zunächst Informationen gewonnen werden. Hierzu darf der BND unterschiedliche Mittel einsetzen. Neben offenen Informationen, Satellitenbildern und menschlichen Quellen gehören hierzu auch technische Werkzeuge wie die Fernmeldeaufklärung oder Cyberoperationen.

Im Rahmen eines Informations- und Beratungsbesuches habe ich mir die unterschiedlichen Organisationseinheiten und Abläufe im Bereich Beschaffung darstellen lassen. Der Termin war von Transparenz und Offenheit geprägt. Alle datenschutzrechtlichen Fragestellungen konnten abschließend beantwortet werden.

8.1.9 Keine Beeinträchtigung der sicherheitsbehördlichen Arbeit durch die Kontroll- und Beratungstätigkeit der BfDI

Ich sehe mich oft dem Vorwurf ausgesetzt, dass meine Beratungs- und Kontrollpraxis bei den beaufsichtigten Stellen zu einem sehr großen Aufwand führe, der die eigentliche Arbeit der jeweiligen Stelle dadurch erheblich beeinträchtige. Dieser Aussage möchte ich entschieden widersprechen. Nicht zuletzt aufgrund der mir zukommenden Kompensationsfunktion ist meine Aufsichtstätigkeit gerade im Sicherheitsbereich essentiell zur demokratischen Grundrechtssicherung; zumal ich einen Schwerpunkt auf Beratung lege und den Aufwand für die kontrollierten Stellen so gering wie möglich halte.

Kontrollinstanzen sind ein wesentliches Merkmal unserer Demokratie. Wir finden sie in den Parlamenten, bei den Gerichten, in den Medien und natürlich in der Öffentlichkeit. Darüber hinaus sieht die Verwaltungsorganisation durch Fach-, Rechts- und Dienstaufsichten

159 32. TB Nr. 9.1.10

eine verwaltungsinterne Kontrollstruktur vor. Meine Behörde hat in diesem Konstrukt eine Spezialzuständigkeit für die Wahrung des Grundrechts auf informationelle Selbstbestimmung.

Mir ist bewusst, dass sich Sicherheitsbehörden einer hohen Kontrolldichte ausgesetzt sehen. Jedoch sind es gerade die Sicherheitsbehörden, die besonders sensible personenbezogene Daten verarbeiten und über schlagkräftige Befugnisse verfügen, die schwerwiegende Konsequenzen für Betroffene mit sich bringen und damit erheblich in das Grundrecht auf informationelle Selbstbestimmung eingreifen können.

Insbesondere im Bereich der Nachrichtendienste erfolgt diese Informationsverarbeitung in der Regel im Verborgenen und ohne Wissen der Betroffenen. Das Bundesverfassungsgericht hat mir daher eine Kompensationsfunktion zugesprochen. Ich soll mit meiner Aufsichtstätigkeit ausgleichen, was der Einzelne mangels Kenntnis über die Verarbeitung seiner Daten nicht für sich selbst leisten kann. Gerade vor diesem Hintergrund ist meine Beratungs- und Kontrolltätigkeit notwendig. Ich überprüfe anstelle der Betroffenen unabhängig, ob sich die Sicherheitsbehörden an die für sie geltenden gesetzlichen Vorgaben halten. In der Regel ist dies der Fall.

Es liegt in der Sache, dass meine Termine vor Ort ebenso wie meine schriftlichen Nachfragen zu Aufwand bei den kontrollierten Stellen führen. Meine Termine und Nachfragen sind aber auch immer eine Gelegenheit für die kontrollierten Stellen zur Klärung offener Fragen. Gerade in den Terminen vor Ort lassen sich datenschutzrechtliche Fragen und Anforderungen oftmals abschließend erörtern, sodass die Stellen im Anschluss an den Beratungs- und Kontrolltermin über mehr Rechts- und damit über mehr Handlungssicherheit verfügen. Für künftige Projekte kennen sie ihre Spielräume innerhalb der von mir aufgezeigten „roten Linien".

Grundsätzlich erwarte ich in meinen Kontroll-, Informations- und Beratungsterminen weder die Anwesenheit vieler Mitarbeitenden noch aufwendige Vorträge oder „Generalproben" vor meinen Besuchen. Vielmehr bin ich bemüht, den Aufwand bei den kontrollierten Stellen so gering wie möglich zu halten. Um mir beispielsweise ein Bild von datenverarbeitenden Systemen zu machen, reicht mir häufig die schlichte Einsichtnahme und eine allgemeine Vorstellung der Funktionalitäten am System. Ich kündige meine Besuche frühzeitig an, berücksichtige die Verfügbarkeit der handelnden Akteure, führe die Termine bei den kontrollierten Stellen vor Ort durch und konkretisiere mein Informationsinteresse vor jedem Besuch. Schließlich sind von meinen Besuchen und Nachfragen regelmäßig unterschiedliche Fachbereiche der kontrollierten Stelle betroffen, sodass – neben dem behördlichen Datenschutz – stets weitere Organisationseinheiten im Fokus eines Termins stehen.

Der mit meiner Tätigkeit für die beaufsichtigten Stellen verbundene Aufwand steht daher in einem angemessenen Verhältnis zu meinem gesetzlichen Auftrag in unserer freiheitlich-demokratischen Gesellschaft. Dieser Rolle und ihrer Verantwortung beim Eingriff in das Recht auf informationelle Selbstbestimmung sollten sich die kontrollierten Stellen bewusst sein und meine Arbeit als inhärente Legitimationsbedingung für eine rechtmäßige Verarbeitung personenbezogener Daten verstehen.

Ungeachtet dieser aus meiner Sicht dringend erforderlichen Klarstellung möchte ich auch noch einmal explizit erwähnen, dass die Zusammenarbeit bei Kontroll- und Beratungsbesuchen mit vielen öffentlichen Stellen sehr gut funktioniert.

8.1.10 Datenschutz im Schengen-Raum: Aufsicht über das SIS

Mit 91 Millionen gespeicherten Ausschreibungen und 15 Milliarden durchgeführten Suchen in 2023[160] gehört das Schengener Informationssystem (SIS) zu den wichtigsten IT-Großsystemen der EU. Das SIS dient dem Informationsaustausch in den Bereichen Sicherheit und Grenzmanagement in Europa. Vor diesem Hintergrund lag im aktuellen Berichtsjahr erneut ein Beratungs- und Kontrollschwerpunkt auf dem SIS.

Auch nach der Inbetriebnahme der erweiterten, dritten Generation des SIS[161] ist es wichtig zu überprüfen, wie die angebundenen Behörden personenbezogene Daten im System verarbeiten. Im Berichtsjahr habe ich hierzu eine Kontrolle bei der Bundespolizei abgeschlossen. Prüfgegenstand waren die nach Art. 24 Abs. 1 lit. a) der Verordnung (EU) 2018/1861 im SIS eingespeicherten Ausschreibungen zur Einreise- und Aufenthaltsverweigerung.

Dabei wurden keine wesentlichen datenschutzrechtlichen Defizite festgestellt. Ich habe jedoch beratend darauf hingewirkt, dass der in diesem Kontext als Vor-

160 siehe Statistikbericht der Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), abrufbar unter https://www.eulisa.europa.eu/our-publications/reports

161 32. TB Nr. 7.7

aussetzung für eine Ausschreibung zentrale Begriff der schweren Straftat hinreichend restriktiv ausgelegt und verstanden wird. Die Kontrolle ergab außerdem, dass besser dokumentiert werden muss, wenn und warum betroffene Personen nicht über eine SIS-Ausschreibung informiert werden.

Darüber hinaus haben meine Mitarbeitenden mit der Prüfung der 2023 neu eingeführten Ausschreibungskategorien im SIS begonnen. Hierzu wurden im Berichtsjahr deutsche Ausschreibungen nach Art. 40 der Verordnung (EU) 2018/1862 kontrolliert. Mit diesen Ausschreibungen können unbekannte gesuchte Personen über Finger- oder Handflächenabdrucksätze zur Identifizierung ausgeschrieben werden, wenn diese mit sehr hoher Wahrscheinlichkeit einem Täter einer terroristischen oder sonstigen schweren Straftat zugeordnet werden können. Um eine rechtmäßige datenschutzkonforme Anwendung zu gewährleisten, werden diese Ausschreibungen und die datenschutzrechtlichen Rahmenbedingungen derzeit überprüft. Über das Ergebnis der Kontrolle werde ich im nächsten Tätigkeitsbericht informieren.

Auf europäischer Ebene befasse ich mich im Rahmen des Coordinated Supervision Committee (CSC) fortlaufend mit datenschutzrechtlichen Fragestellungen zum SIS. Ein Thema dort war die Auswertung der europaweit koordinierten Kontrollen von Ausschreibungen zur verdeckten und gezielten Kontrolle im SIS.[162] Ein Bericht, der unter intensiver Beteiligung meiner Mitarbeitenden erstellt wurde, fasst die Prüferkenntnisse zusammen und gibt klare Empfehlungen an die verantwortlichen Stellen[163].

Schengenweite Überprüfungen zum SIS führen meine Mitarbeitenden außerdem im Rahmen der Schengen Evaluierungen durch.[164] Nach der Teilnahme an der Expertenmission in Finnland in 2023 erfolgte im Berichtsjahr eine Teilnahme an der Evaluierung in Ungarn.

Auch im Rahmen der Beschwerdebearbeitung habe ich mich immer wieder eingehend mit der Verarbeitung personenbezogener Daten im SIS befasst. Insgesamt haben meine Mitarbeitenden im Jahr 2024 etwa 150 Anfragen und Beschwerden zum SIS bearbeitet.

Querverweis:

4.2.3 Bericht aus dem CSC

8.1.11 Beratung und Kontrolle beim GBA

Die Beratung und Kontrolle beim Generalbundesanwalt beim Bundesgerichtshof (GBA) führte zu keiner Beanstandung. Gegenstand waren Datenübermittlungen des GBA nach der Anordnung über Mitteilungen in Strafsachen (MiStra) und dem Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG).

Aus dem Gerichtsverfassungsgesetz ergibt sich die Befugnis der Gerichte und Staatsanwaltschaften, personenbezogene Daten von Amts wegen an öffentliche Stellen für andere Zwecke als die des Strafverfahrens zu übermitteln. Beispielsweise können Informationen über bestimmte Strafverfahren gegen Inhaber waffenrechtlicher Erlaubnisse der Waffenbehörde mitgeteilt werden. Eine Verpflichtung besteht, wenn dies in besonderen Vorschriften oder aber in den Verwaltungsvorschriften der MiStra, geregelt ist. Die Staatsanwaltschaft hat dabei, in bestimmten Konstellationen den Beschuldigten über eine erfolgte Übermittlung zu benachrichtigen.

In der Kontrolle wurden keine wesentlichen datenschutzrechtlichen Defizite festgestellt. Ich konnte mich vergewissern, dass die Akten des GBA sehr gewissenhaft und gründlich geführt werden. Lediglich in einem Fall wurde der Beschuldigte nicht über die Übermittlung in Kenntnis gesetzt. Da es sich um einen Fehler im Einzelfall handelte und seitens des GBA bereits vor dem Kontrolltermin Maßnahmen zur Vermeidung von vergleichbaren Fehlern getroffen wurden, habe ich von einer Beanstandung abgesehen und lediglich beratend Praxisempfehlungen ausgesprochen.

8.1.12 Kontrolle des BKA im Bereich der politisch motivierten Kriminalität im links zugeordneten politischen Spektrum

Im Bereich der politisch motivierten Kriminalität (PMK) differenziert das Bundeskriminalamt (BKA) nach verschiedenen politischen Strömungen. Die Kontrolle der als „links“ eingestuften Taten und der dazu gespeicherten Personen förderte keine strukturellen Probleme zu Tage, warf jedoch in Einzelfällen Fragen auf.

Die Speicherungen im Bereich PMK-links verteilen sich beim BKA derzeit auf insgesamt fünf Dateien mit unterschiedlichen Zwecken. Meine Kontrolle konzentrierte sich auf die Zentralstellendatei PMK-links-Z, die Strafverfolgungsdatei PMK-links-S sowie die Speicherung

162 32. TB Nr. 7.7

163 Bericht zu Ausschreibungen im SIS des EDSA, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/csc-documents/report-article-36-alerts-schengen-information-system_en

164 31. TB Nr. 3.5.4

zu Personen, die polizeilich als sog. „Gefährder“ und „Relevante Person“ eingestuft sind.

Die Datei PMK-links-Z wird im einheitlichen Fallbearbeitungssystem (eFBS) des BKA geführt. Positiv hervorzuheben ist – insbesondere im Vergleich zu einer im Jahr 2012 durchgeführten Kontrolle [165] – die Umsetzung der Negativprognosen, also der individualisierten Begründung, warum mit der Begehung weiterer Straftaten durch die jeweilige Person zu rechnen ist. Kritisch sehe ich hingegen die Datenqualität. Obwohl es sich mit 171 zum Kontrollzeitpunkt erfassten Personen nicht um ein Massenverfahren handelt, stellten meine Mitarbeitenden in immerhin sechs von 124 geprüften Personendatensätzen Mängel wie z. B. eine Doppelerfassung und ein falsches Geburtsdatum fest.

Inhaltlich fiel auf, dass ein Großteil der Speicherungen zum Kontrollzeitpunkt auf Aktionen der Gruppe „Letzte Generation“ zurückzuführen waren. Bei einer dieser Speicherungen habe ich mir die Beanstandung vorbehalten, da meinem Verständnis nach überhaupt keine Straftat zugrunde lag und der Sachverhalt weiter aufzuklären war.

Beanstandet habe ich Speicherungen zu einer erheblichen Tat. Den gespeicherten Personen können jeweils aber keine Tatbeiträge nachgewiesen werden. Obwohl das staatsanwaltliche Ermittlungsverfahren seit Jahren eingestellt ist und gegen die Personen keinerlei weitere Erkenntnisse vorliegen, berufen sich das Bundesministerium des Inneren und für Heimat (BMI) und das BKA hier auf einen Restverdacht, der die Speicherung weiterhin rechtfertige.

Zu beiden kritischen Sachverhalten habe ich Einsicht in die staatsanwaltlichen Ermittlungsakten genommen und sehe mich danach in meiner Ansicht bestätigt. Das BKA hatte diese Einsichtnahme jeweils nicht vorgenommen, sondern sich auf teils veraltete und unzutreffende Angaben der Landespolizeibehörden verlassen. Hier sehe ich angesichts des erheblichen Eingriffsgewichts großes Verbesserungspotential auf Seiten des BKA. Einen der Sachverhalte hat das BKA nunmehr gelöscht.

In der Datei PMK-links-S speichert das BKA diverse Ermittlungsverfahren, jeweils auf Grundlage von § 483 StPO. Hier habe ich nur eine Stichprobe geprüft. Ich musste die Speicherung einer sogenannten Kontaktperson beanstanden. Das zugehörige Ermittlungsverfahren ist seit langer Zeit eingestellt und die Speicherung der betroffenen Person sehe ich als nicht mehr erforderlich an. Auch hier sind BMI und BKA abweichender Ansicht.

Zudem habe ich die Datenspeicherung im Kontext der polizeilich als sog. „Gefährder“ oder „Relevante Person“ eingestuften Personen im Phänomenbereich der PMK-links überprüft. Die Ein- und Ausstufung erfolgt ausschließlich durch die Landeskriminalämter. Zum Kontrollzeitpunkt handelte es sich um 84 Personen, von denen zehn als sog. „Gefährder“ erfasst sind. Die Speicherungen über als „Gefährder“ eingestufte Personen habe ich alle prüfen können. Zudem habe ich 14 weitere Speicherungen von Daten zu sog. „Anlasspersonen“, Beschuldigten oder Verurteilten geprüft. Dabei konnte ich keine datenschutzrechtlichen Probleme feststellen.

8.1.13 Kontrolle verdeckter Maßnahmen beim BKA

Beim Bundeskriminalamt (BKA) führe ich alle zwei Jahre eine Pflichtkontrolle der sogenannten verdeckten Maßnahmen durch. Diese Kontrolle dient in besonderem Maße der Kompensation dafür, dass betroffene Personen von solchen Maßnahmen in der Regel erst spät oder sogar niemals Kenntnis erhalten.

Die Pflichtkontrolle hinterließ insgesamt einen sehr positiven Eindruck. Gegenstand der Kontrolle waren Maßnahmen zur Terrorabwehr nach dem fünften Abschnitt des Bundeskriminalamtgesetzes (BKAG) sowie nach § 34 BKAG zur Eigensicherung bei Strafverfolgungsmaßnahmen und nach § 64 BKAG zu Schutzzwecken.

Ein datenschutzrechtlicher Verstoß wurde nicht festgestellt. Die Prüfung umfasste insgesamt sieben Verfahren, in denen verdeckte Maßnahmen durchgeführt wurden. Alle Anordnungen konnten eingesehen werden. Ich konnte ferner die komplette Dokumentation einsehen. Das BKA hatte alle Maßnahmen umfassend und gut festgehalten. Auch die erforderlichen Benachrichtigungen betroffener Personen sowie deren Dokumentation konnte überprüft werden, sie wurden ebenfalls sorgfältig umgesetzt.

8.2 Allgemeine Beratungs- und Kontrollbesuche

8.2.1 Erfahrungsaustausch mit den bDSB der gesetzlichen Krankenkassen

Austausch zu aktuellen datenschutzrechtlichen Themen mit behördlichen Datenschutzbeauftragten (bDSB) der gesetzlichen Kranken- und Pflegekassen.

165 24. TB Nr. 7.4.4

Im Juni 2024 haben sich in Bonn behördliche Datenschutzbeauftragte (bDSB) der gesetzlichen Kranken- und Pflegekassen mit Mitarbeiterinnen und Mitarbeitern aus meinem Haus zu aktuellen datenschutzrechtlich relevanten Themen in der gesetzlichen Krankenversicherung ausgetauscht. Teilgenommen hatten auch Vertreterinnen und Vertreter des Bundesamtes für Soziale Sicherung. Mit Rundschreiben vom 17. Juli 2024 hatte ich darüber berichtet.[166]

Im Mittelpunkt standen die sich aus den Art. 15, 33 und 34 DSGVO ergebenden Fragen in der täglichen Praxis der Kranken- und Pflegekassen sowie aktuelle Rechtsetzungsvorhaben und deren Umsetzung. Gleichzeitig waren die herausfordernden technischen Themen wie die Einbindung von Videoinhalten auf Webseiten öffentlicher Stellen, die Kriterien für die Nutzung souveräner Clouds, Microsoftanwendungen sowie die Herausforderungen und Lösungsansätze bei der Nutzung von Künstlicher Intelligenz Gegenstand dieses Treffens. Der fachliche und persönliche Austausch mit den bDSB der verschiedenen Kranken- und Pflegekassen war für alle Beteiligten informativ und anregend. Die Wiederholung eines solchen Termins zum Austausch ist für 2025 vorgesehen.

8.2.2 Beratungs- und Kontrollbesuche bei gesetzlichen Kranken- sowie Pflegekassen

Ich ziehe eine positive Bilanz aus den im Berichtszeitraum durchgeführten Beratungs- und Kontrollbesuchen bei den gesetzlichen Kranken- sowie Pflegekassen in meinem Zuständigkeitsbereich. Die Kassen sind sich bewusst, dass sie ein gesteigertes Datenschutzniveau gewährleisten müssen.

Im Berichtsjahr führte ich bei den gesetzlichen Kranken- und Pflegekassen meines Zuständigkeitsbereichs vier Vor-Ort-Kontrollen, einen Beratungsbesuch sowie zwölf schriftliche Fragebogenkontrollen durch.

Schwerpunkte der Vor-Ort-Kontrollen bei den Krankenkassen waren das Krankengeldfall- und Reha-Entlassmanagement, der Umgang mit digitalen Identitäten sowie die Neugestaltung der Sicherheitsauthentifizierung eines Online-Kundenportals bzw. einer App-Anwendung. Zudem erfolgte eine Schwerpunktkontrolle im Bereich der gesetzlichen Pflegekasse.

Die Beratungs- und Kontrollbesuche geben meinen Mitarbeitenden vor Ort wichtige Einblicke in die Arbeitsabläufe und die damit einhergehende Datenschutzorganisation der beaufsichtigten Stellen. Bestandteil sind auch immer Gespräche mit den behördlichen Datenschutzbeauftragten im vertraulichen Rahmen. Der Beratungsaspekt steht hierbei im Fokus.

Darüber hinaus erfolgten schriftliche Fragebogenkontrollen zur Datenschutzorganisation bei den Kranken- und Pflegekassen. Dieses Format ergänzt die Kontrollen vor Ort und gewährleistet so eine höhere Kontrolldichte. Dabei sind Quervergleiche möglich, da zu dem gewählten Kontrollthema mehrere beaufsichtigte Stellen parallel betrachtet werden.

Insgesamt betrachtet war mein Eindruck positiv. Die gesetzlichen Kranken- und Pflegekassen haben erhöhte Anforderungen an den Datenschutz, weil besonders zu schützende Gesundheitsdaten verarbeiten werden und neben der DSGVO auch sozialrechtliche Vorgaben wie das Sozialgeheimnis zu beachten sind. Diesen Herausforderungen wird im Wesentlichen – auch im Hinblick auf die fortschreitende Digitalisierung – nachgekommen.

8.2.3 Aus der Beratungs- und Kontrollpraxis bei Telekommunikationsanbietern

Viele Unternehmen der Telekommunikationsbranche nehmen meine Hinweise bereitwillig auf und nutzen das Beratungsangebot. Andere Anbieter zeigen sich weniger kooperativ.

In der Aufsicht und Beratung von Telekommunikationsanbietern zeigt sich ein breites Spektrum an Reaktionen. Viele Anbieter nehmen meine Beratungsangebote an und berücksichtigen den Datenschutz bereits in einem frühen Stadium. Erkannte Defizite werden nach einem formlosen Hinweis behoben. Meine Mitarbeitenden geben hier regelmäßig Praxishinweise und beraten zu möglichen Lösungsvarianten.

Jedoch gibt es auch Anbieter, denen bereits bewusst ist, dass Teile ihrer Datenverarbeitung nicht rechtskonform sind. Bis eine Kontrolle ins Haus steht, werden die notwendigen Anpassungen immer wieder verschoben. Dann entsteht auf einmal Zeitdruck. Es gibt wenige Unternehmen, die eine Zusammenarbeit mit mir verweigern. In diesen negativen Fällen muss ich von meinen Abhilfebefugnissen aus der DSGVO Gebrauch machen. Werden Anweisungen nicht befolgt, setze ich Zwangsgelder fest, die dann von den Vollstreckungsbehörden beigetrieben werden. Dies ist aber nur das letzte Mittel und erfreulicherweise selten notwendig.

166 BfDI-Rundschreiben vom 17. Juli 2024, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2024/Rundschreiben-Erfahrungsaustausch-bDSB-KK-PfK.html

Ein Telekommunikationsanbieter stach 2024 besonders negativ heraus. Das Unternehmen versendete Briefe über vermeintlich abgeschlossene Verträge und in der Folge auch Mahnschreiben. Mir liegen hierzu zahlreiche Beschwerden vor. Betroffene konnten sich häufig nicht daran erinnern, überhaupt einen Vertrag abgeschlossen zu haben. Nutzten Betroffene dann ihr Auskunftsrecht nach Art. 15 DSGVO, bekamen sie nicht die ihnen zustehenden Informationen zur Verarbeitung ihrer personenbezogenen Daten. Mit dem Auskunftsrecht sollen Betroffene Überblick und damit auch Kontrolle über die konkrete Verarbeitung ihrer personenbezogenen Daten behalten. Sie haben Anspruch auf eine Übersicht und auf eine Kopie der personenbezogenen Daten (beispielsweise die Kopie über den Vertragsabschluss). Ich setze mich hier mit allen rechtlichen Mitteln dafür ein, Betroffenen zu ihrem Recht auf Auskunft zu verhelfen.

Ein weiterer Anbieter verweigert ebenfalls beharrlich, die Betroffenenrechte einer Kundin zu erfüllen. Dieser Anbieter zahlte Zwangsgelder in vierstelliger Höhe. Dies hätte er vermeiden können, indem er dieser Kundin den Anspruch auf Auskunft erfüllt hätte.

8.2.4 Das Cloud-Reallabor

Die Öffentliche Verwaltung erwägt zunehmend, in die Cloud zu wechseln. Die Verlagerungen bestimmter Verfahren in die Cloud kann beispielsweise wirtschaftlicher sein als ein Betrieb auf der eigenen Infrastruktur. Es zeigt sich jedoch auch, dass viele Infrastrukturanbieter ihre Lösungen vermehrt komplett in die Cloud verlagern, so dass ein Eigenbetrieb nicht mehr möglich ist. Besonders für Behörden ist der Gang in die Cloud oft mit Herausforderungen verbunden. Diese können regulatorischer Art sein, aber auch strategische Fragen sind hier relevant: Die öffentliche Verwaltung muss langfristig souverän handlungsfähig sein und darf sich nicht von einzelnen Anbietern abhängig machen.

Der GovTech Campus bietet Vertretern der öffentlichen Verwaltung, Wissenschaft, Wirtschaft und Zivilgesellschaft eine Plattform, um im Rahmen verschiedener Projekte die Digitalisierung der öffentlichen Verwaltung zu modernisieren. [167] Anfang des Jahres 2024 wurde dort das „Cloud-Reallabor“ ins Leben gerufen, das Blaupausen für die sichere Nutzung von Cloud-Lösungen erarbeiten soll. Projektmitglieder sind dabei Bedarfsträger der öffentlichen Verwaltung, insbesondere der Sozialversicherungen, verschiedene Cloudanbieter aus den USA, Deutschland und anderen europäischen Ländern sowie das Bundesamt für Sicherheit in der Informationstechnik (BSI). Ich begleite das Projekt beratend.

Zunächst sollen die Mitglieder der öffentlichen Verwaltung die Angebote der Cloudanbieter auf Nutzbarkeit prüfen. Des Weiteren werden in verschiedenen Proof-of-Concepts (PoC) bestimmte Einsatzszenarien durch die Projektbeteiligten praktisch getestet und untersucht. So arbeiten in zwei PoCs jeweils zwei Cloudanbieter zusammen mit einem Vertreter der öffentlichen Verwaltung, um den sicheren Wechsel von Anwendungen zwischen den Clouds zu testen. In einem anderen PoC wird erprobt, welche Mehrwerte sich durch den Einsatz von Confidential Computing, einer Technologie, die es ermöglicht, Daten in einer besonders geschützten Umgebung zu verarbeiten, auf Public-Cloud-Plattformen ergeben.

Meine Behörde berät das Cloud-Reallabor in den datenschutzrechtlichen Aspekten. Von Anfang an muss der Datenschutz gemäß den Grundsätzen Data-Protection-by-Design und Data-Protection-by-Default mitgedacht werden. Erste Zwischenergebnisse wurden Ende 2024 veröffentlicht [168]. Ein weiterer Bericht ist für Ende 2025 geplant, eine Fortsetzung des Projektes darüber hinaus wird im Laufe des Jahres geprüft.

8.2.5 Datenschutzrechtliche Kontrolle im Finanzamt Überlingen

Personenbezogene Daten aller Bürgerinnen und Bürger sind von der Steuerverwaltung betroffen. Dies beginnt bereits unmittelbar nach der Geburt in Form der Zuweisung der steuerlichen Identifikationsnummer und setzt sich im Regelfall beispielsweise mit Blick auf die jährliche Veranlagung zur Einkommensteuer gegenüber dem jeweils zuständigen Finanzamt ein Leben lang fort. Die Steuerverwaltung steht daher im Fokus meiner Aufsichtstätigkeit, welche auch die regelmäßige Beratung und Kontrolle örtlicher Finanzämter umfasst.

Im Berichtszeitraum wurde das Finanzamt Überlingen durch mein Haus beraten und geprüft. Der Schwerpunkt lag neben einer allgemeinen datenschutzrechtlichen Beratung und Kontrolle auf der elektronischen Aktenführung im Erhebungsverfahren. Aufgrund größtenteils erfreulicher Ergebnisse waren lediglich allgemeine Hinweise und Empfehlungen erforderlich. [169] So wurde

167 Webseite des GovTech Campus: https://govtechcampus.de/

168 Veröffentlichungen des Cloud-Reallabors: https://reallabor.cloud/insights/

169 Bericht zur Kontrolle des Finanzamts Überlingen, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Kontrollberichte/Kontrolle-Finanzamt-Ueberlingen-2024.html

beispielsweise empfohlen, die Beschäftigten des Finanzamtes nicht nur anlassbezogen, sondern möglichst in regelmäßigen Intervallen datenschutzrechtlich zu sensibilisieren. Angeregt wurde die zentrale Dokumentation von Ermessenentscheidungen im Erhebungsverfahren, damit sich diese bei Bedarf einfacher nachvollziehen lassen.

Bezogen auf die personelle Ausstattung der für das Finanzamt Überlingen zuständigen behördlichen Datenschutzbeauftragten (bDSB) musste ich datenschutzrechtliche Defizite feststellen. Die DSGVO gibt in Art. 38 Abs. 2 vor, dass der Verantwortliche den bDSB bei der Erfüllung seiner Aufgaben unterstützen muss, indem er die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen zur Verfügung stellt. Um die vielfältigen Rechte und Befugnisse der DSGVO nutzen zu können, benötigen bDSB ausreichend Zeit für die Wahrnehmung ihrer Aufgaben. Damit eine ordnungsgemäße Aufgabenerfüllung sichergestellt werden kann, vertrete ich bezüglich öffentlicher Stellen grundsätzlich die Auffassung, dass bDSB jedenfalls ab einer Anzahl von 500 Beschäftigten zu 100 Prozent freigestellt werden sollten. Diese Personalausstattung sehe ich bereits allein aufgrund der Pflichtaufgaben bei der Sicherstellung des Personaldatenschutzes und der Funktion als Anlaufstelle für mein Haus als notwendig an.

Die der bDSB des Finanzamtes Überlingen zur Verfügung gestellten Personalressourcen stellten sich leider als nicht angemessen dar. Mit seinen rund 100 Beschäftigten übernimmt das Finanzamt Überlingen zentrale Aufgaben im Steuersystem. Dementsprechend hat auch die bDSB vielfältige Beratungs-, Überwachungs- und Kooperationsaufgaben wahrzunehmen. Zu betonen ist hier, dass sich Datenschutzbeauftragte keinesfalls darauf beschränken sollten, auf Anforderungen seitens ihrer Organisation oder auf Beschwerden und Eingaben von Betroffenen zu reagieren. Gefordert ist vielmehr eine eigeninitiativ tätige bDSB, die sich zu datenschutzrelevanten Planungen aktiv einbringt und unaufgefordert die Einhaltung der datenschutzrechtlichen Bestimmungen überwacht.

Zudem habe ich zu berücksichtigen, dass die bDSB des Finanzamtes Überlingen gemäß Art. 37 Abs. 3 DSGVO als gemeinsame bDSB für mehrere Behörden bestellt ist. So ist die bDSB des Finanzamtes Überlingen vorliegend für 72 Behörden mit insgesamt mehr als 17.000 Beschäftigten zuständig. Sie kann in ihrem Arbeitsbereich zur Erfüllung ihrer vielen Aufgaben nur auf Zeitanteile von insgesamt nur rund 0,6 Vollzeitäquivalenten (VZÄ) zurückgreifen. Ihr selbst stehen nur rund 0,3 VZÄ zur Verfügung. Ein gesonderter Ausweis der Zeitanteile betreffend das kontrollierte Finanzamt Überlingen ist nicht erfolgt. Dieser beläuft sich jedoch aller Voraussicht nach nur auf einen kleinen Bruchteil der vorgenannten Zeitanteile und ist offensichtlich unzureichend.

Auf meine Beratung und Kontrolle hat die Finanzverwaltung Baden-Württemberg entschieden, die erforderliche Evaluation der festgestellten Arbeitssituation nicht auf das Finanzamt Überlingen zu beschränken, sondern den Arbeitsbereich der gemeinsamen bDSB insgesamt zu überprüfen und adäquat auszustatten. Ich werde diesen Prozess aufmerksam und konstruktiv begleiten. Bestmöglich lassen sich hieraus auch grds. Erkenntnisse zur erforderlichen Personalausstattung gemeinsamer bDSB in der Finanzverwaltung herleiten, welche auf andere Bundesländer übertragen werden können. Zudem zeigen sich entsprechende Entwicklungen in anderen Verwaltungsbereichen. Die Ergebnisse können daher bereichsübergreifend wertvolle Hinweise für die angemessene Personalisierung der bDSB geben und hierdurch die Durchsetzung der datenschutzrechtlichen Vorschriften insgesamt wirksam stärken.

8.2.6 Kontrolle des IT-Systems „ANSWER“ beim BZSt

Methoden Künstlicher Intelligenz (KI) gehören bei vielen Verantwortlichen bereits zum Arbeitsalltag. Daher stehen diese im Mittelpunkt dieser Kontrolle des Systems ANSWER beim Bundeszentralamt für Steuern (BZSt).

Die Steuerverwaltung nimmt regelmäßig eine Vorreiter- und Schlüsselrolle bei der Verwaltungsdigitalisierung ein. Insbesondere werden dort an mehreren Stellen Schritte u. a. in das Feld der Methoden Künstlicher Intelligenz unternommen.

Gegenstand eines Beratungs- und Kontrollbesuchs war das System „Analyse und Auswertung“ (ANSWER) des BZSt. Hierbei lag ein besonderes Augenmerk auf den verwendeten KI-Komponenten. Das ANSWER System soll als zentrales IT-System Fachbereiche gemäß ihren jeweiligen Anforderungen mit Verarbeitungsprozessen unterstützen. Durchgeführt werden zurzeit im ANSWER System hauptsächlich Textanalysen für den Fachbereich DAC-6 [170], der für den automatischen Austausch von Steuergestaltungen zuständig ist. Der Ausbau des ANS-

170 Informationen des BZST zum Verfahren DAC 6, abrufbar unter: https://www.bzst.de/DE/Unternehmen/Intern_Informationsaustausch/DAC6/Verfahren/verfahren_node.html

WER Systems geht stetig voran und die Anbindung eines weiteren Fachbereiches ist bereits vorgesehen.

Erfreulich ist, dass der Datenschutz beim Verfahren ANSWER einen hohen Stellenwert genießt. Der Fachbereich bindet die dortige behördliche Datenschutzbeauftragte (bDSB) häufig und frühzeitig ein. Diese pflegt wiederum einen regelmäßigen Austausch mit meinem Haus.

An einigen Stellen gibt es dennoch Verbesserungspotential. So empfahl ich zum Beispiel, das Rechte-Rollen-Konzept bezogen auf einzelne, hochrangige Rollen zu verfeinern, um einen Generalzugriff auf die in ANSWER vorhandenen oder zugreifbaren Daten anderer Fachbereiche zu vermeiden. Es ist eine neuartige Entwicklung, dass KI-Methoden Einzug in das Arbeitsumfeld der bDSB erhalten. Aus diesem Grund habe ich außerdem empfohlen, dass das BZSt die Ressourcen der bDSB mithilfe von Schulungen speziell bezogen auf KI ergänzt.

Das Verfahren ANSWER wird durch mein Haus auch in Zukunft weiter konstruktiv begleitet.

8.2.7 Kontrolle in der deutschen Botschaft in London

Der Betrieb und die Nutzung des Auslandsportals im Bereich Passwesen war Schwerpunkt meines Beratungs- und Kontrollbesuchs der deutschen Botschaft in London.

Mit dem Auslandsportal setzt das Auswärtige Amt (AA) die Vorgaben des Onlinezugangsgesetzes um. Mit dem Portal sollen zukünftig alle Dienstleistungen an den Auslandsvertretungen auch online beantragt werden können. Das Rollout verschiedener Funktionen erfolgt stufenweise. Im Zuge dessen wurde die Beantragung des Reisepasses für Erwachsene an der Vertretung in London am 1. Dezember 2023 pilotiert.

Bei dem Besuch meiner Mitarbeitenden am 15. und 16. Mai 2024 haben die Kolleginnen und Kollegen der Botschaft erläutert, dass die Nutzung des Auslandsportals vor der eigentlichen Passbeantragung auf freiwilliger Basis erfolgt. Antragstellerinnen und Antragsteller können über das Portal vorab die Unterlagen einreichen, sodass die Auslandsvertretung bereits vor Antragstellung die Vollständigkeit der Unterlagen prüfen und bestätigen kann.

Bei dem persönlichen Termin, in dem der offizielle Antrag gestellt wird, können die Bearbeiterinnen und Bearbeiter die Daten einschließlich der antragsbegründenden Dokumente im Vorgangsbearbeitungssystem RK-Pass[171] zur eigentlichen Bearbeitung übernehmen.

Dieses Vorgehen ist vereinbar mit dem Passgesetz (PassG), da die Antragstellung selbst nicht über das Auslandsportal erfolgt. Die Datenverarbeitung als solche basiert auf Art. 6 Abs. 1 lit. e) DSGVO i. V. m. § 19 Abs. 2 PassG. Datenschutzrechtliche Bedenken gegen die Umsetzung bestehen somit nicht.

Das AA beteiligt mich regelmäßig bei geplanten Weiterentwicklungen des Systems, sodass ich auch den Ausbau des Auslandsportals aus datenschutzrechtlicher Sicht weiterhin begleiten werde.

Bei meinem Besuch habe ich nur geringfügige datenschutzrechtliche Defizite festgestellt. Diese betrafen beispielsweise eine allgemeine Regulierung zur Aufbewahrung verschiedener Listen und die Verwendung einheitlicher Formblätter und Aushänge. Eine Behebung dieser Mängel ist zwischenzeitlich erfolgt.

8.2.8 Datenschutz bei Vereinsverbotsverfahren

Insbesondere die Verarbeitung personenbezogener Daten bei Vereinsverbotsverfahren war Gegenstand eines Beratungs- und Kontrollbesuchs beim Bundesministerium des Innern und für Heimat (BMI).

Vom 9. bis 11. April 2024 statteten meine Mitarbeitenden dem BMI einen Beratungs- und Kontrollbesuch ab. Die Kontrolle bezog sich auf die Verarbeitung personenbezogener Daten bei Vereinsverbotsverfahren sowie die allgemeine Datenschutzorganisation beim BMI. Beide Prüfungsgegenstände haben keine wesentlichen datenschutzrechtlichen Defizite ergeben.

Im BMI sind thematisch sehr heterogene Bereiche angesiedelt wie Öffentliche Sicherheit und Bundespolizei, Digitale Verwaltung, Sport und Heimat sowie Digitale Verwaltung, um nur einige zu nennen. Daraus resultiert innerhalb des Hauses regelmäßig umfänglicher datenschutzrechtlicher Beratungs- und Koordinationsbedarf. Das BMI hat dafür neben dem Team der behördlichen Datenschutzbeauftragten auch einen Bereich operativer Datenschutz eingerichtet. Im Rahmen meiner Kontrolle habe ich die Einrichtung dieses Bereichs an zentraler Stelle begrüßt und gleichzeitig eine personelle Stärkung angeregt. Das BMI ist dieser Anregung bereits gefolgt und hat erste Maßnahmen umgesetzt.

Unsere Verfassung verbietet in Art. 9 Abs. 2 Grundgesetz (GG) Vereinigungen, deren Zwecke oder deren Tätig-

171 Anwendung zur Eingabe, Verwaltung und zum Druck von Reisepassanträgen und vorläufigen Passdokumenten sowie zur elektronischen Archivierung von einzureichenden Dokumenten

keit den Strafgesetzen zuwiderlaufen, die sich gegen die verfassungsmäßige Ordnung oder gegen den Gedanken der Völkerverständigung richten. Verbote werden gemäß § 3 Vereinsgesetz festgestellt. Die Möglichkeit, das Verbot eines verfassungswidrigen Vereins in einem rechtsstaatlichen Verfahren festzustellen, ist Ausdruck der wehrhaften Demokratie, wie sie das GG vorsieht. Zur Aufgabenerfüllung kann das BMI als Verbotsbehörde für Vereine, deren Organisation oder Tätigkeit sich über das Gebiet eines Bundeslandes hinaus erstrecken, die Hilfe von Sicherheitsbehörden auf Bundes- und Landesebene in Anspruch nehmen.

Die Durchführung von Vereinsverbotsverfahren erfordert auf verschiedene Art und Weise die Verarbeitung personenbezogener Daten. Meine Mitarbeitenden haben sich insbesondere zur Übermittlung von Daten zwischen den beteiligten Behörden, die Aktenführung und der sicheren Aufbewahrung von Unterlagen unterrichten lassen und hierzu beraten. Darüber hinaus habe ich mir beispielhaft ein Bild zu einem potentiellen Umgang mit personenbezogenen Daten Dritter bei Vereinsverbotsverfahren verschafft. Datenschutzrechtliche Defizite habe ich dabei nicht festgestellt.

8.2.9 Beratungs- und Kontrollbesuch im StBA

Die Umsetzung des Abschottungs- und Trennungsgebots stellt angesichts des sich verändernden Aufgabenspektrums des Statistischen Bundesamtes (StBA) eine neue Herausforderung dar.

Die Kernaufgabe des StBA ist die Produktion von Statistiken. In den vergangenen Jahren ist daneben auch der Aufbau und die Führung von Verwaltungsregistern als neue Aufgabe hinzugekommen. Seit Juli 2021 bietet das StBA mit der Verwaltungsdaten-Informationsplattform (VIP) einen umfassenden Überblick über die in deutschen Verwaltungen geführten Datenbestände. Seit Oktober 2022 ist das StBA die Registerbehörde für das Bewacherregister (BWA), in dem alle Gewerbetreibenden des Sicherheitsgewerbes ihre Unternehmen sowie ihr Sicherheitspersonal registrieren. Als weiteres Verwaltungsregister in der Zuständigkeit des StBA befindet sich das Basisregister für Unternehmen im Aufbau.

Durch den Ausbau des StBA auch zu einer Verwaltungsregisterbehörde rückt aus datenschutzrechtlicher Sicht die Einhaltung des Abschottungs- und Trennungsgebots in den Blick. Meine Mitarbeitenden haben daher im Berichtsjahr die Umsetzung des Gebots im StBA an den Standorten Wiesbaden und Bonn kontrolliert.

Abschottungs- und Trennungsgebot

Das Abschottungs- und Trennungsgebot ist vom Bundesverfassungsgericht im sogenannten Volkszählungsurteil* als verfassungsrechtlicher Grundsatz im Zusammenhang mit der Wahrnehmung von Aufgaben der amtlichen Statistik aufgestellt worden. Seine Einhaltung ist eine notwendige Bedingung für die Rechtmäßigkeit eines Eingriffs in das Grundrecht auf informationelle Selbstbestimmung.

Unter „Abschottung und Trennung“ in diesem Sinne ist die räumliche, personelle und organisatorische Separierung des Statistikbetriebs von Nichtstatistik-Einrichtungen zu verstehen. Danach hat die Verarbeitung von statistischen Einzeldatensätzen, in einem von den übrigen Verwaltungsstrukturen getrennten Bereich zu erfolgen. Mit dem Abschottungs- und Trennungsgebot wird die Datenverarbeitung zu Zwecken der amtlichen Statistik gegen eine Verarbeitung zu anderen Zwecken abgesichert und zugleich das Vertrauen der auskunftspflichtigen Personen in die amtliche Statistik gestärkt.

* Urteil des BVerfG vom 15. Dezember 1983, 1 BvR 209/83

Das StBA hat sich intensiv mit der Bedeutung des Abschottungs- und Trennungsgebots und seinen konkreten Auswirkungen auf die Wahrnehmung der unterschiedlichen Aufgaben der Behörde auseinandergesetzt.
Die konkrete Umsetzung der Separierung der neuen (Verwaltungs-)Aufgabenbereiche des Amtes von den etablierten Statistikaufgaben bedingt entsprechende Maßnahmen in organisatorischer, räumlicher, personeller und technischer Hinsicht. Eine abgeschottete Aufgabenwahrnehmung innerhalb des StBA ist bereits gängige Praxis. Die durch die Kontrolle gewonnenen Eindrücke lassen Verbesserungspotential für die räumliche Abschottung am Stammsitz in Wiesbaden erkennen, auch die Organisationsstruktur kann optimiert werden. Hierfür stehe ich dem StBA weiter beratend zur Seite.

Die Auswertung der Kontrollergebnisse war zum Zeitpunkt des Redaktionsschlusses für die Erstellung dieses Berichts noch nicht vollständig abgeschlossen.

9 BfDI intern

9.1 Personalentwicklung 2024

Im Berichtsjahr lag mein Fokus im Personalbereich unvermindert auf der Personalgewinnung. Dadurch ist es mir gelungen, den Aufwuchs meiner Behörde weiter voranzutreiben.

Auch im Jahr 2024 war meine Behörde auf verschiedenen Karrieremessen vertreten, so. z. B. auf den Fakultätskarrieretagen in Bonn und Köln, dem Fachbereichstag der Hochschule des Bundes in Brühl sowie dem Unternehmenstag der Hochschule Bonn-Rhein-Sieg. Um die gemeinwohlorientierten und abwechslungsreichen Tätigkeiten sowie Karrierechancen innerhalb meiner Behörde noch deutlicher herauszustellen, wurde der Messestand rundum erneuert und modernisiert.

Eine weitere Maßnahme, um den Bewerberradius auszuweiten, bildete die Überarbeitung des Internetauftritts im Bereich „Arbeiten bei der BfDI“. Neben konkreten Beispielen in Form von Jobprofilen, die einen Einblick in den Arbeitsalltag ermöglichen, und FAQs zum Bewerbungsprozess können sich Interessierte auch über die vielfältigen Vorzüge einer Tätigkeit in meiner Behörde informieren. Den Kolleginnen und Kollegen, die u. a. im Rahmen des hausinternen Fotoshootings mitgewirkt haben, danke ich für ihre Bereitschaft und Einsatz für das gesamte Haus.

Im Berichtsjahr 2024 habe ich 32 Stellenbesetzungsverfahren (sowohl Einzel- als auch Sammelbesetzungsverfahren) durchgeführt. Insgesamt habe ich 661 Bewerbungen erhalten. Von diesen wurden 296 Bewerberinnen und Bewerber zu Vorstellungsgesprächen eingeladen.

Vom Haushaltsgesetzgeber wurden mir im Berichtsjahr 2024 für meinen Personalhaushalt insgesamt 417,9 Stellen zugesprochen. Diese setzen sich aus 397,4 Planstellen für Beamtinnen und Beamte sowie aus 20,5 Stellen für Tarifbeschäftigte zusammen.

Neben insgesamt 12 geplanten sowie ungeplanten Personalabgängen konnte ich mich im Jahr 2024 gleichzeitig über 54 hinzugewonnene Kolleginnen und Kollegen freuen. Darüber hinaus rechne ich in den kommenden Wochen noch mit 13 weiteren Neuzugängen aus bereits abgeschlossenen Bewerbungsverfahren. Insgesamt verfügte meine Behörde zum Stichtag 31. Dezember 2024 damit über eine Personalstärke von 369 Personen.

9.2 Presse- und Öffentlichkeitsarbeit

Die Kommunikation mit Bürgerinnen und Bürgern ist wichtiger Teil meines gesetzlichen Auftrags. Die Mitarbeitenden meiner Presse- und Öffentlichkeitsarbeit sind mit großem Engagement auf verschiedenen Wegen und Kanälen aktiv. Dabei ist mir wichtig, dass meine Behörde nicht nur Informationen bereitstellt, sondern auch Möglichkeiten für den Austausch eröffnet.

Pressearbeit

Im Berichtsjahr hat meine Pressestelle sehr viele Anfragen erhalten, die sich mit dem Amtswechsel in der Person der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beschäftigt haben.

Eine Vielzahl von Anfragen betraf außerdem inhaltliche Themen. Zusammengefasst stachen dabei Anfragen zum Gesundheitsbereich hervor, was erkennbar mit der Einführung der elektronischen Patientenakte für alle gesetzlich Versicherten zum Januar 2025 zu tun hat. Doch auch darüber hinaus beschäftigen sich viele Medienschaffende mit den datenschutzrechtlichen Aspekten der Digitalisierung des Gesundheitswesens. Dabei ging es sowohl um technische Lösungen als auch um praktische Fragen, wie etwa die Ausübung von Betroffenenrechten.

Ein weiterer Schwerpunkt der Anfragen lag beim Thema Künstliche Intelligenz (KI). Hierzu haben sicher die weitere Verbreitung und die alltäglichere Nutzung der Technologie beigetragen. Allerdings wurden auch bereits existierende Maßnahmen und Werkzeuge durch die Medien oder die einsetzenden Stellen nun als KI

bezeichnet und rückten damit erneut ins Zentrum des Interesses.

Nicht zuletzt erreichen meine Pressestelle immer dann viele Anfragen, wenn Medien und Soziale Medien selbst zum Thema werden. Beispielsweise gab es viele Anfragen zur Nutzung der Plattform TikTok durch den Bundeskanzler und zu den Überlegungen des Europäischen Datenschutzausschusses zu Abomodellen von Sozialen Medienanbietern.

„Consent or Pay"- oder „Pay or Okay"-Modelle

„Consent or Pay"- oder „Pay or Okay"-Modelle finden sich auf verschiedenen Internetseiten, etwa von Medienhäusern oder Anbietern sozialer Medien. Nutzende haben in diesen Modellen häufig nur zwei Möglichkeiten, um auf die Inhalte der Webseiten zuzugreifen: Entweder zahlen sie einen bestimmten Geldbetrag („Pay") oder sie willigen ein, dass ihre Daten für Profilbildung und personalisierte Werbung genutzt werden („Consent" bzw. „Okay"). In der Regel erfolgt diese Auswahl über ein den Cookie-Bannern ähnliches Fenster.

In der Praxis haben sich unterschiedliche Arten solcher Modelle herausgebildet. So kann die Bezahloption als Einmalzahlung (bspw. Zugriff auf einen Artikel einer Onlinezeitung) oder als regelmäßiges Abonnement (bspw. Nutzung eines Sozialen Mediums gegen monatliche oder jährliche Zahlung) ausgestaltet sein. Zudem deckt die Auswahl zwischen „Consent" oder „Pay" häufig nur den Zugriff auf die Basiswebseite oder den Basisdienst ab. Für den Zugriff auf einzelne weitere Inhalte auf der Webseite, etwa besondere Artikel, Rubriken oder Dienste wird häufig eine zusätzliche Zahlung verlangt.

Meine Behörde hat im Berichtszeitraum 16 Pressemitteilungen herausgegeben und wurde zweimal in die Bundespressekonferenz eingeladen. Außerdem hat meine Behörde 9 Gastbeiträge und Aufsätze für verschiedene Medien verfasst. Meine Pressestelle hat 302 Anfragen per Mail und 269 telefonische Anfragen beantwortet.

Webauftritt und Social Media

Auf meinem Webauftritt habe ich einige Änderungen vorgenommen, um die Informationen zielgruppengerechter bereitzustellen. Dafür wurden in den Bereichen Sicherheit, Telekommunikation und Digitale Dienste die Struktur angepasst und neue Inhalte bereitgestellt.

Außerdem habe ich neue Formulare eingestellt. Diese sind übersichtlicher, einfacher zu bedienen und ermöglichen meinen Mitarbeiterinnen und Mitarbeitern eine einfachere Bearbeitung. Die Funktionalität und Nutzendenfreundlichkeit der Formulare möchte ich auch weiterhin verbessern.

Neben der Webseite als primärem Onlinekanal betreibe ich weiterhin die Mastodon-Instanz social.bund.de. Ich würde weiter sehr begrüßen, wenn die Bundesregierung dieses sehr erfolgreiche Projekt, das sie (zumindest in Teilen) selbst auch nutzt, übernehmen würde. Die Nutzungszahlen im Fediverse steigen weiterhin stetig, wenn auch nicht mehr ganz so schnell wie 2023. Dennoch erreiche ich über meinen Kanal social.bund.de/@bfdi über 45.000 Bürgerinnen und Bürger.

Dass ein hohes Interesse an der Nutzung der Instanz besteht, sehe ich daran, dass ich immer wieder Institutionen einen Zugang verwehren muss, weil diese nicht unsere Kriterien erfüllen. Da die Stärke des Fediverse in der Dezentralität liegt, würde ich es ohnehin begrüßen, mehr Instanzen für verschiedene Bereiche zu sehen, beispielsweise für Rettungs- und Einsatzkräfte, für Länderbehörden oder wissenschaftliche Einrichtungen.

Das Datenschutzforum (https://bfdi.bund.de/forum) erfreut sich ebenfalls weiterhin großer Beliebtheit bei Datenschutzexpertinnen und Datenschutzexperten. Beide Plattformen werde ich im Rahmen der mir zu Verfügung stehenden fiskalischen Möglichkeiten weiter betreiben.

Besuchergruppen

Meine Mitarbeitenden des Berliner Verbindungsbüros betreuten Besuchergruppen von Mitgliedern des Deutschen Bundestages. Vier Gruppen mit bis zu 50 Teilnehmenden wurden empfangen.

In Bonn empfingen wir 2024 eine Delegation der Datenschutzaufsichtsbehörde von Sri Lanka zum Erfahrungsaustausch.

Informationsmaterial

In 2024 lag der Fokus auf der generellen Überarbeitung bestehender Informationsmaterialien, insbesondere mit Blick auf mögliche neue Informationskanäle. Es wurde damit begonnen, Absatzwege neu auszurichten. Angesichts der Nachfrage zu konkreten Informationen wurden neue Formate vorbereitet, die in 2025 umgesetzt werden sollen.

Wie bereits in den vergangenen Jahren ist das Interesse an den BfDI-Pixi-Büchern ungebrochen. Fast eine halbe Million Pixi-Bücher wurden im Berichtsjahr zur Ver-

fügung gestellt. Insbesondere die Nachfrage von Grund- und weiterführenden Schulen ist angewachsen. Aus diesem Grund wird es im Jahr 2025 Unterrichtsmaterialien zu den Pixi Wissen Büchern „Was ist Datenschutz?“ und „Was ist Informationsfreiheit?“ geben.

9.3 Veranstaltungen der BfDI

Öffentliche Veranstaltungen sind weiterhin fester Bestandteil der Öffentlichkeitsarbeit meiner Behörde. Bei den verschiedenen Formaten kommen wir, meine Mitarbeitenden und oft auch ich selbst, mit vielen verschiedenen Gruppen ins Gespräch – angefangen von den ganz Kleinen am Weltkindertag bis hin zu den Entscheidern in Politik und Gesellschaft bei unseren Foren.

Fest der Demokratie

Am 25. Mai hat sich meine Behörde mit einem Stand am Fest der Demokratie beteiligt. Das Gelände der Villa Hammerschmidt in Bonn zog trotz der schwierigen Wetterverhältnisse viele tausende Besucherinnen und Besucher an. Die Mitarbeitenden boten neben dem direkten Dialog mit Bürgerinnen und Bürgern auch eine praktische Vorführung zu datenschutzrechtlichen Laboruntersuchungen und diverse Aktivitäten für Kinder an.

Weltkindertag

Wie bereits in 2023 veranstaltete ich den Weltkindertag am 20. September 2024 mit und war in der Stadtbibliothek Bonn. Dieses Jahr stand er unter dem Motto „Mit Kinderrechten in die Zukunft“. Erneut luden wir zu einer Vormittags- und Nachmittagsveranstaltung ein. Zwei Grundschulklassen aus Bonn waren mit großer Freude dabei, sich meinem Datenschutz-Quiz erfolgreich zu stellen sowie sichere Passwörter zu erfinden.

Beim Familienfest am Nachmittag war ich von der Vielzahl der Besuchenden beeindruckt. Das Interesse der Kinder lag vorrangig auf unserem Mega-Puzzle; die Eltern hingegen wollten es genau wissen und stellten konkrete Fragen zu datenschutzrelevanten Themen.

Veranstaltungen wie diese erweisen sich immer wieder als ein ideales Mittel, um das Thema Datenschutz bereits frühzeitig im Lebensalltag und damit im Bewusstsein von Kindern und Familien zu etablieren. Das ist nicht nur mein gesetzlicher Auftrag aus § 14 Abs. 1 Nr. 2 BDSG und Art. 57 Abs. 1 lit. b) DSGVO, sondern unabhängig davon Ausdruck meiner Motivation, mit meinem Amt der Gesamtgesellschaft zu dienen. Kinder über Datenschutz aufzuklären und sie für das Thema zu sensibilisieren, ist von großer Bedeutung, um ihnen einen selbstbestimmten und sicheren Umgang mit digitalen Medien und den sich hieraus ergebenden Herausforderungen zu ermöglichen.

Strategic Foresights

Am 5. Dezember veranstaltete ich in Kooperation mit dem Weizenbaum-Institut erstmals einen Strategic Foresight. Hierzu fand sich in Berlin das Direktorium des Weizenbaum-Instituts mit zahlreichen Wissenschaftlerinnen und Wissenschaftlern zusammen. Themen des Strategic Foresights waren demokratische Digitalisierungsstrategien, der Zugang zu Gesundheitsdaten sowie die gesellschaftsfördernde Entwicklung und Anwendung von Künstlicher Intelligenz.

Strategic Foresights sind mehrphasige Prozesse, die sich mit möglichen zukünftigen Entwicklungen innerhalb bestimmter Themenkomplexe befassen. Sie dienen dem Austausch zwischen internen sowie externen Expertinnen und Experten. Der Prozess unserer Strategic Foresights orientiert sich an einem wissenschaftlichen Konzept und stellt sich wie folgt dar: (1) Themenfindung, (2) partizipativer Problematisierungsprozess, (3) interner Reflexionsprozess, (4) datenschutzrechtliche Positionierung und stetige Evaluation.

Den Bereich Strategic Foresights werde ich in den nächsten Jahren noch weiter ausbauen, insbesondere in meinen Schwerpunktthemen Künstliche Intelligenz, Gesundheit und Sicherheit.

Polizei-Symposium

Am 12. September hat meine Behörde ein Symposium zur Arbeit der Polizei veranstaltet. Der Tag in meinem Berliner Verbindungsbüro orientierte sich thematisch an der Frage „Automatisierte Datenanalyse und KI-Innovative Polizeiarbeit mit Diskriminierungspotential?“. In Kurzvorträgen und Diskussionen haben Expertinnen und Experten aus Forschung und Praxis den Istzustand der automatischen Datenanalyse in der Polizeiarbeit und im Strafverfahren beleuchtet und mögliche Entwicklungen aufgezeigt. Zu den Vortragenden gehörten: Prof. Dr. Christoph Krehl, Richter am Bundesgerichtshof a. D., Markus Hartmann, Leitender Oberstaatsanwalt und Leiter der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen, Gül Pinar, Fachanwältin für Strafrecht sowie Alexander Poitz, stellvertretender Bundesvorsitzender der Gewerkschaft der Polizei. Die anschließende erste Diskussionsrunde legte ein besonderes Augenmerk auf die Strafverfolgung. Führt der Einsatz von neuen Technologien zu mehr Gerechtigkeit und sind die neuen Ermittlungsmöglichkeiten mit dem Datenschutzrecht vereinbar?

Das Nachmittagspanel wurde mit Vorträgen von Tobias Wiemann, Leiter der Unterabteilung Rechts- und Grundsatzangelegenheiten im BMI, Eric Töpfer, wissenschaftlicher Mitarbeiter am Deutschen Institut für Menschenrechte und Prof. Dr. Michael Bäuerle, LL. M., Professor an der Hessischen Hochschule für öffentliche Sicherheit und Management sowie stellvertretender Direktor des hessischen Zentrums verantwortungsbewusste Digitalisierung, eingeleitet. Die zweite Diskussionsrunde stellte dann die automatisierte Datenanalyse und Methoden der KI in der Polizeiarbeit in den Vordergrund. Hier wurden Möglichkeiten der Ausgestaltung sowie Grenzen der automatisierten Datenanalyse thematisiert.

Eine Aufzeichnung der Veranstaltung finden Sie auf meiner Webseite.

Politisches Frühjahrsforum

Im März 2024 konnten wir erstmals Veranstaltungsgäste im neuen Berliner Verbindungsbüro am Spittelmarkt begrüßen. Die Besucherinnen und Besucher des Politischen Frühjahrsforums erwartete nicht nur ein neuer Veranstaltungsbereich, sondern auch ein interessanter Abend zum Thema „Ausschließlich digital? – Wie weit geht das Recht auf ein analoges Leben?“

Prof. Dr. Reinhold Popp, Zukunftsforscher an der Sigmund Freud PrivatUniversität Wien hielt den Auftaktimpuls „Digitale Phobie – Wie steht es um unsere Angst vor Veränderung?“. Er verwies darauf, dass Zukunftsangst auch durch die Behauptung entstehe, dass die Digitalisierung schicksalhaft bzw. alternativlos auf uns zukomme. Dabei läge es an uns, selber zu entscheiden, wie wir die Zukunft als Gesellschaft und als Individuum für uns gestalten wollen.

Im Anschluss diskutierten Carolin Kleinert (Landessprecherin Berlin Startup-Verband), Rena Tangens (Digitalcourage e. V.), Prof. Dr. Reinhold Popp und Prof. Ulrich Kelber das Phänomen des sogenannten Digitalzwangs. Durch die Debatte führte der freie Autor und Journalist Falk Steiner. In großen Schritten, so Prof. Kelber, vollziehe sich die Digitalisierung. Allerdings bräuchten digitale Lösungen bisweilen auch weiter analoge Lösungen, damit niemand abgehängt oder ausgeschlossen werde. Er erinnerte dabei an unzureichende technische Barrierefreiheit oder mangelnden Datenschutz.

Abschließend stellte Rena Tangens insbesondere die Initiative von Digitalcourage vor, das Recht auf ein analoges Leben im Grundgesetz zu verankern.

Eine Aufzeichnung der Veranstaltung finden Sie auf meiner Webseite.

Politisches Herbstforum

Für mein Herbstforum habe ich unter dem Titel „Daten im Dienst der Patientinnen und Patienten“ ein Schwerpunktthema meiner Amtszeit gewählt: die Vereinbarkeit von Datennutzung und Datenschutz in der Medizin. Der inhaltliche Schwerpunkt lag dabei auf der elektronischen Patientenakte (ePA).

In seinem empfehlenswerten Impulsvortrag („Die Digitalisierung des Gesundheitswesens in Österreich am Beispiel der elektronischen Gesundheitsakte ELGA – Wo stehen und wie diskutieren unsere Nachbarn?“) stellte Dr. Franz Leisch, der entscheidend an der elektronischen Gesundheitsakte in Österreich beteiligt war, die Diskussionen und Entwicklungen in seinem Land vor.

Gemeinsam mit der Moderatorin Teresa Sickert diskutierte ich im Anschluss mit Prof. Dr. Dr. Eva Winkler, Vorsitzende der Zentralen Ethikkommission bei der Bundesärztekammer, Dr. Florian Hartge, Geschäftsführer der gematik, Michaela Schröder, Mitglied der Geschäftsleitung beim Verbraucherzentrale Bundesverband sowie Herrn Dr. Leisch, wie die Vereinbarkeit von Datennutzung und Datenschutz im Gesundheitswesen aussehen könne. Einigkeit bestand darüber, dass eine umfassende Digitalisierung nur dann gelingen kann, wenn die technischen Lösungen mit rechtlichem Sachverstand einhergehen und Bürgerinnen und Bürger Vertrauen in die neuen digitalen Lösungen haben können. Dabei kommt einem effektiven Datenschutz eine sehr wichtige Rolle zu.

Eine Aufzeichnung der genannten Veranstaltungen finden Sie auf meiner Webseite[172].

9.4 Zahlen und Fakten zum Berichtsjahr

Auch aus der Statistik lassen sich Einblicke über meine Tätigkeit gewinnen. Es zeigt sich, dass das Arbeitsaufkommen meiner Behörde in letzter Zeit steigt.

Beschwerden und Anfragen

Im Berichtsjahr wurden insgesamt 8.670 Beschwerden und Anfragen an mich gerichtet. Es zeigt sich hier ein weiterer Anstieg der Fallzahlen, der sich im Wesentlichen in allen Referaten meines Hauses wiederspiegelt.

172 Alle Aufzeichnungen sind abrufbar unter: https://www.bfdi.bund.de/DE/Service/Mediathek/Veranstaltungen/Veranstaltungen-node.html

Beschwerden und Anfragen	2021	2022	2023	2024
Allgemeine Anfrage	4329	4434	5162	5225
Beschwerde Art. 77 DSGVO	2383	2115	2513	3313
Beschwerde Art. 80 DSGVO	19	3	11	10
Beschwerde § 60 BDSG	54	29	50	75
Eingabe gegen Nachrichtendienste	44	38	46	47

Sowohl bei den allgemeinen Anfragen als auch bei den Beschwerden nach DSGVO und BDSG (siehe Tabelle) kann ein klarer Anstieg des Volumens verzeichnet werden. Lediglich zur Einführung der DSGVO im Jahr 2018 konnte meine Behörde höhere Eingangszahlen verzeichnen. Neben schriftlichen bzw. elektronischen Anfragen sowie den Beschwerden haben meine Mitarbeiterinnen und Mitarbeiter in 5.221 Fällen Personen telefonisch beraten.

Beratung und Kontrolle

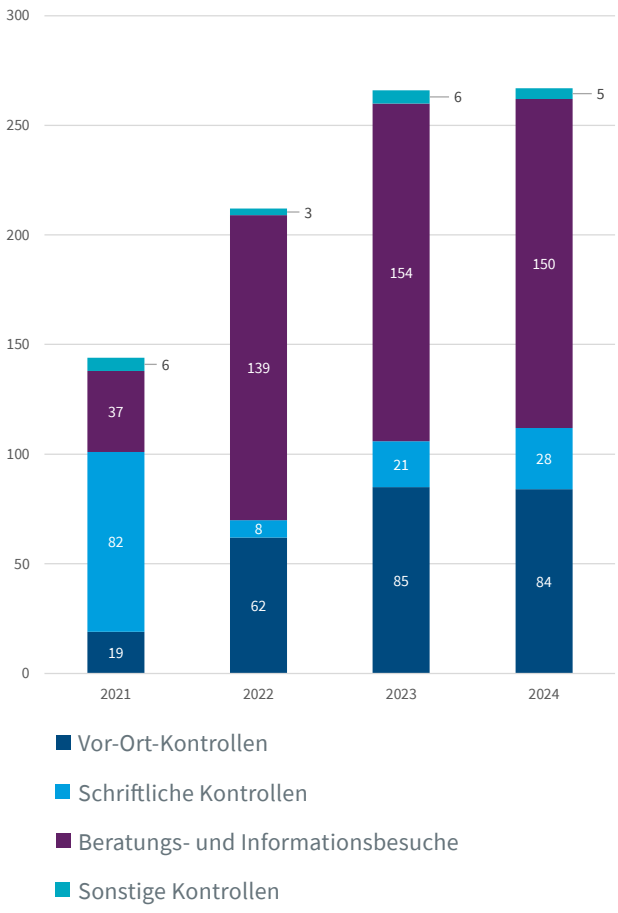
Als Aufsichtsbehörde stellen Beratung und Kontrolle wichtige Arbeitsbereiche für meine Behörde dar, die mitunter stark vom persönlichen Kontakt mit den beaufsichtigten verantwortlichen Stellen leben. Die Anzahl der Beratungs- und Kontrolltermine bewegt sich im Berichtsjahr auf dem Niveau des Vorjahres. Das in der Pandemie vielfach genutzte Instrument der schriftlichen Kontrolle wird weiterhin dort eingesetzt, wo es sich als sinnvoll erwiesen hat.

Es ist erfreulich, dass meine Behörde von den beaufsichtigten Stellen als beratender Ansprechpartner geschätzt wird. Dies kommt durch eine hohe Anzahl der Beratungs- und Informationsbesuche zum Ausdruck. Bei diesen Terminen werden konkrete Problemstellungen und datenschutzfreundliche Lösungsmöglichkeiten besprochen. Oftmals werden die Themen von den beaufsichtigten Stellen an mich herangetragen. Mein Ziel ist es, die Informations- und Beratungsangebote weiter auszubauen und einen lösungsorientierten Datenschutz in den Mittelpunkt meiner Aktivitäten zu stellen.

Meldungen von Datenschutzverstößen

Weiterhin rückläufig zeigte sich die Anzahl der Meldungen von Datenschutzverstößen. Im Berichtsjahr habe ich 8.787 Meldungen entgegengenommen. Wesentlichen Anteil an diesem Rückgang hat meine Konkretisierung gegenüber den Finanzbehörden, in welchen Fällen es sich um meldepflichtige Verstöße handelt.

Beratungen und Kontrollen seit 2021



Abhilfemaßnahmen

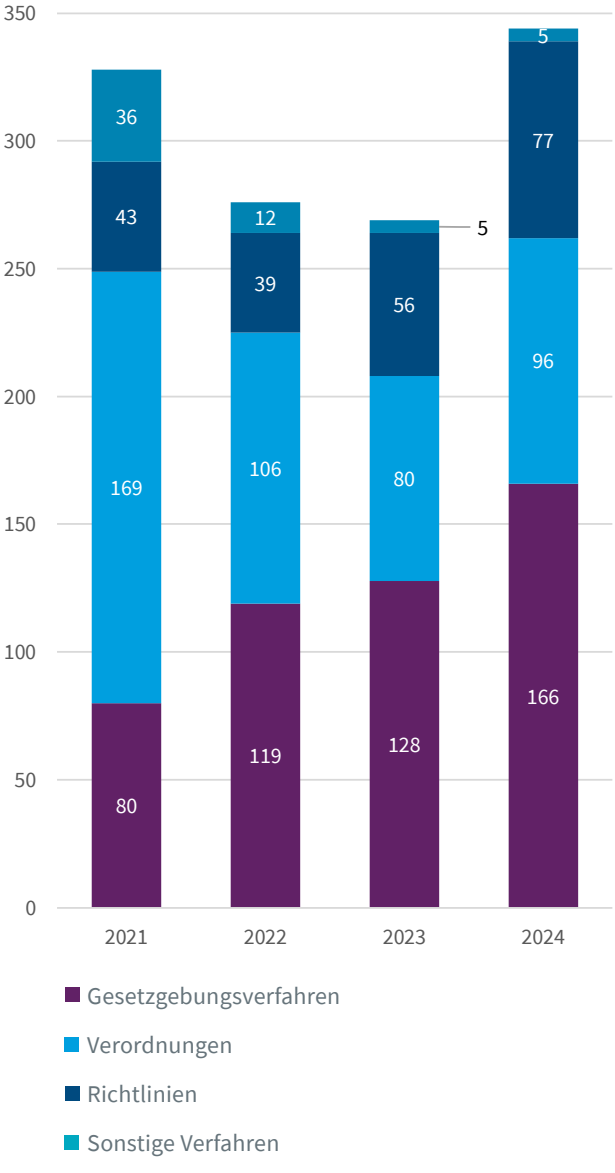
Im Berichtsjahr hat meine Behörde 119 aufsichtsrechtliche Maßnahmen wie z. B. Verwarnungen, Anweisungen oder die Festsetzung von Zwangsgeldern vorgenommen. Eine ausführliche Auflistung findet sich in den Anlagen 2 und 3.

Meldungen von Datenschutzverstößen	2021	2022	2023	2024
Meldungen nach Art. 33 DSGVO	10106	10614	9234	8740
Meldungen nach § 169 TKG	51	44	29	47

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. Aus der Statistik für das Berichtsjahr lässt sich ein erhöhtes Niveau bei der Beteiligung zu förmlichen Gesetzen erkennen. Es zeigt sich hier das übliche höhere Aufkommen zum Ende einer Legislaturperiode, das in meinem Haus entsprechenden Bedarf nach sich zieht. Mein Ziel ist, mit einer lösungsorientierten Beratung bereits vor der formellen Beteiligung von den federführenden Ressorts vertrauensvoll in die Erarbeitung von Gesetzesentwürfen einbezogen zu werden.

Beteiligungen nach § 21 GGO



In die Gesetzgebung wurde ich auch durch den Deutschen Bundestag eingebunden. In 9 Fällen wurde ich von Ausschüssen als Sachverständige gehört. Auf nationaler Ebene wurde ich darüber hinaus in 90 Fällen zur Prüfung von Dateianordnungen bei Sicherheitsbehörden beteiligt.

Auf europäischer Ebene war ich außerdem bei der Erstellung von 6 Verordnungen und einer Richtlinie eingebunden.

Gremiensitzungen

Über meine Mitgliedschaft in Organisationen wie der Datenschutzkonferenz (DSK), dem Europäischen Datenschutzausschuss (EDSA) und vielen weiteren – oft internationalen – Gremien bin ich im Austausch mit unterschiedlichsten Akteuren im Bereich des Datenschutzes.

Im Berichtsjahr haben meine Mitarbeitenden als (Co-)Vorsitz/Rapporteur insgesamt 259 Sitzungen geleitet und darüber hinaus als Mitglied an 713 Sitzungen teilgenommen. In diese Gremien hat mein Haus 10 Entschließungs- bzw. Beschlussentwürfe eingebracht.

9.5 Aufbau Future Foresight bei der BfDI

Neue Technologien werden oft erst als datenschutzrelevant erkannt, nachdem diese bereits im Einsatz sind. Eine rechtzeitige Erkennung der Datenschutzrelevanz erfordert somit die (systematische) Verfolgung technologischer Entwicklungen, welche durch den im März 2024 in meiner Behörde etablierten Aufgabenbereich „Future Foresight“ in aufeinanderfolgenden Phasen realisiert werden soll. In der ersten Phase von Future Foresight haben meine Mitarbeitenden unter anderem den für 2030 angestrebten 6G-Mobilfunkstandard

als Technologietrend mit potenziellen maßgeblichen Auswirkungen auf den Datenschutz identifiziert und in der 74. Sitzung der Berlin Group im November 2024 vorgestellt, woraufhin das Thema 6G für ein künftiges Arbeitspapier der Berlin Group vorgesehen ist.

Der technologische Datenschutz steht vor dem grundlegenden Problem, dass neue Technologien oft erst nach ihrem Einsatz als datenschutzrelevant erkannt werden. Dies liegt zum Teil daran, dass diese oft einem sog. „Hype-Zyklus" folgen. Technologische Entwicklungen führen nach dem Hype-Zyklus typischerweise in einer ersten Klimax zu überzogenen Erwartungen am Anfang, gefolgt von Enttäuschungen, bevor es zu realistischen Anwendungen kommt, wodurch eine rechtzeitige und fundierte Bewertung aus Sicht des Datenschutzes erschwert wird. Sinnvoll ist daher ein technologischer Datenschutz durch eine möglichst technologieneutrale Gesetzgebung, die gleichzeitig Räume bietet, technologiespezifische Bewertungen zu maßgeblichen Zukunftsentwicklungen mit Relevanz für den Datenschutz vorzunehmen. Dem wird in bestehender Gesetzgebung auf nationaler und europäischer Ebene insofern Rechnung getragen, als in Erwägungsgrund 15 der DSGVO die zuvor genannte Technologieneutralität begründet und die Verfolgung maßgeblicher Entwicklungen der Informations- und Kommunikationstechnologie im BDSG als Aufgabe der BfDI bestimmt wird[173]. Diese Aufgabe meiner Behörde wird unter anderem durch den im März 2024 etablierten Aufgabenbereich „Future Foresight" in fünf aufeinanderfolgenden Phasen realisiert, wobei ein Prognosehorizont von fünf Jahren mit jährlicher Aktualisierung angestrebt wird.

In der ersten Phase 1 (Trend-Identifizierung) wird ein datenschutzrelevantes Verständnis der sich kontinuierlich entwickelnden technologischen Landschaft angestrebt. Ziel der Phase 1 ist eine Identifizierung der Neuentwicklungen in der Informations- und Kommunikationstechnik (sog. Technologietrends) mit potenziellen maßgeblichen Auswirkungen auf den Datenschutz.

In der Phase 2 (Szenario-Entwicklung) werden für die in der Phase 1 identifizierten Technologietrends potenzielle (datenschutzrelevante) Zukunftsszenarien entwickelt. Es handelt sich dabei um hypothetische Zukunftsentwicklungen, die möglichst viele Alternativen nachvollziehbar aufzeigen.

In der Phase 3 (Folgenabschätzung) wird eine Bewertung potenzieller Folgen für einige in der Phase 2 entwickelten Szenarien vorgenommen, um die resultierenden Risiken und Chancen abzuschätzen, welche anschließend in der Phase 4 (Risikobewertung) bewertet werden.

In der letzten Phase 5 (Verwertung) wird die Risikobewertung aus Phase 4 verwertet mit dem Ziel, geeignete technische und organisatorische Maßnahmen für potenzielle Verantwortliche zu „Data Protection by Design" gem. Art. 25 DSGVO abzuleiten.

Eine weitere Zielsetzung auf Basis des Erkenntnisgewinns nach Durchführung der Phasen 1–5 ist die Beratung einschlägiger Einrichtungen und Gremien des Bundes gem. § 14 Abs. 1 Nr. 3 BDSG in Verbindung mit Art. 57 Abs. 1 lit. c) DSGVO.

Im ersten Anlauf von Future Foresight wurden in der ersten Phase vier Technologietrends mit potenziellen maßgeblichen Auswirkungen auf den Datenschutz identifiziert. Drei dieser identifizierten Technologietrends werden derzeit in Arbeitspapieren der Berlin Group (s. Kapitel 4) thematisiert, nämlich Neurotechnology, Extended Reality und Confidential Computing. Ein weiterer Technologietrend mit maßgeblicher Datenschutzrelevanz wurde nach Teilnahme meiner Mitarbeitenden an der 83. Sitzung des Arbeitskreises „Technische und Organisatorische Datenschutzfragen" der DSK im September 2024 identifiziert. Es handelt sich dabei um den für 2030 angestrebten 6G-Mobilfunkstandard, welcher im Zusammenhang mit Future Foresight in der 74. Sitzung der Berlin Group im November 2024 vorgestellt wurde. Daraufhin wurde das Thema 6G für ein künftiges Arbeitspapier der Berlin Group aufgegriffen.

Die Datenschutzrelevanz im Zusammenhang mit dem 6G-Mobilfunkstandard entsteht dadurch, dass die bestehende Funk-Kommunikation so angepasst werden soll, dass sie gleichzeitig als Funk-Sensorik (durch Radarfunktionalität) genutzt werden kann. Durch den flächendeckenden Einsatz dieser Kombination von Funk-Kommunikation und Funk-Sensorik (genannt JCAS – Joint Communication and Sensing) können unter anderem umfassende Umgebungsdaten erfasst werden, deren Verarbeitung erhebliche Datenschutzrisiken bergen kann, vor allem in Bezug auf Art. 7 DSGVO (Einwilligung) sowie Art. 12 DSGVO (Transparenz).

Im Rahmen von Future Foresight wird derzeit für die vier genannten Technologietrends an deren Szenario-Entwicklung und Folgenabschätzung gearbeitet, gefolgt von deren Risikobewertung und Verwertung.

173 § 14 Abs. 1 Nr. 9 BDSG in Verbindung mit Art. 57 Abs. 1 lit. i) DSGVO

9.6 Ein Behörden-Cluster für bessere Digitalisierung

Um den Herausforderungen der in allen Bereich immer relevanter werdenden Digitalisierung besser begegnen zu können, haben sich sechs Bonner Bundesbehörden zum Bonner Digital Cluster zusammengeschlossen. In diesem Rahmen tauschen sie sich zu aktuellen Fragen der Verwaltungsdigitalisierung und anderen Digitalthemen aus. Ziel ist es, auf diesem Weg nicht nur eine bessere Koordinierung der sich immer weiter überschneidenden Aufsichtszuständigkeiten gewährleisten zu können, sondern zudem auch über den Austausch von Erfahrungswerten bei Prozessen die eigene Verwaltungsdigitalisierung effizienter zu gestalten.

Auf eine Initiative von Bundesnetzagentur, Bundeskartellamt und meiner Behörde gründeten diese Behörden gemeinsam mit der Bundesanstalt für Finanzdienstleitungsaufsicht, dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Justiz im Berichtsjahr das Digital Cluster Bonn. Hierzu unterzeichneten die Leitungen der Behörden bei der Gründungsveranstaltung am 15. Januar 2024 ein Memorandum of Understanding[174], in dem die gemeinsamen Ziele und der grundlegende Rahmen für die künftige Zusammenarbeit festgehalten sind.

Hintergrund war zunächst die sich aus den neuen europäischen Digitalrechtsakten[175] ergebenden neuen horizontalen Zuständigkeiten bei Regulierung und Aufsicht, besser und strukturierter zu koordinieren. Durch Schaffung von Kommunikationskanälen und einen weitergehenden Austausch an Know-how soll eine noch kohärentere und rechtssicherere Anwendung der Gesetze zur Digitalisierung erreicht werden. Von dieser sollen nicht nur die Behörden selbst, sondern vor allem auch die durch die Gesetze Betroffenen, wie Unternehmen, Behörden oder Bürgerinnen und Bürger profitieren.

Hierzu organisiert sich das Cluster zu relevanten Themen in verschiedenen Arbeitskreise, die von einem Lenkungsausschuss mit Vertretern der Behörden eingesetzt werden. Vorschläge für diese Arbeitskreise und die zu behandelnden Themen kommen dabei unmittelbar aus der Fachbereichen der Clustermitglieder. Es ist allerdings nicht erforderlich, dass alle Behörden auch zwingend in allen Arbeitskreisen mitwirken. Vielmehr können sich je nach Interesse, Bedarf und Kapazitäten einbringen.

Neben den Arbeitskreisen im Kontext der Digitalrechtsakte, z. B. zum Thema Interoperabilität oder zu Fragen der Aufsicht im Bereich der KI-Verordnung oder des Digital Services Acts, stellte sich zudem recht schnell heraus, dass die Behörden auch ein großes Interesse am Austausch über Themen der internen Verwaltungsdigitalisierung haben. Denn gerade in diesem Bereich zeigt sich bei den einzelnen Behörden ein durchaus heterogenes Bild des Digitalisierungsfortschritts. Gleichzeitig liegen aber auch verschiedene für Digitalisierungsprozesse gleichsam erforderliche Expertisen vor, die in das Cluster eingebracht werden können. Damit wird gleichzeitig ein Forum geschaffen, das durch Wissens- und Erfahrungsaustausch sowie die Identifizierung von gemeinsamen Lösungsansätzen Synergien schafft, von denen die Clustermitglieder profitieren. Zum Zeitpunkt des Redaktionsschlusses befassten sich daher von den acht bestehenden Arbeitsgruppen die Hälfte mit Fragen und Themen der Binnendigitalisierung, wie z. B. Überlegungen zu Cloud-Strategien, Möglichkeiten zum behördeninternen Einsatz von KI oder Lösungsansätze für ein effizientes Wissens- und Change-Management.

9.7 Aus dem KI-Workshop des Digital Cluster Bonn

Im Digital Cluster Bonn diskutiert mein Haus u. a. auch KI-Themen mit den anderen in Bonn ansässigen Digitalbehörden. Einen Use-Case haben meine Mitarbeitenden in dieser Initiative vorgestellt.

Der behördenübergreifende Austausch ist für mein Haus von großer Bedeutung. Im Zuge des Digital Cluster Bonn ergibt sich die Möglichkeit, sich dauerhaft über Digitalisierungsthemen mit anderen Digitalbehörden Bonns auszutauschen. Neben meinem Haus sind die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Justiz (BfJ), das Bundeskartellamt (BKartA) und die Bundesnetzagentur (BNetzA) Mitglieder dieser Initiative.

Nach der Auftaktveranstaltung am 15. Januar 2024 wurde ein Gremium zum Austausch bzgl. KI-Themen gegründet. In diesem Gremium sind alle o. g. Behörden vertreten. Ziel ist es, Synergien zu schaffen und zu nutzen, Erfahrungen auszutauschen und gegenseitig voneinander zu profitieren.

---

174 Memorandum of Understanding des Bonner Digital Cluster vom 15. Januar 2024, abrufbar unter: https://www.digitalclusterbonn.de/DCB/MoU.pdf?__blob=publicationFile&v=3

175 31. TB Nr. 4.2 sowie 32. TB Nr. 5.3

Das Gremium ist im Berichtzeitraum drei Mal zusammengetreten. In den Terminen ergeben sich insbesondere zwei Kernthemen, nämlich einerseits berichten alle teilnehmenden Behörden über ihrerseits identifizierte sog. Use-Cases, also Bereiche, die die Häuser identifiziert haben, in denen sie jeweils Bedarf oder Potential für KI-Anwendungen sehen. Andererseits tauschen sich die teilnehmenden Behörden über Leitlinien zum KI-Einsatz aus. Mein Haus hat hierbei bisher einen Use-Case für KI-Einsatz identifiziert und diesen auch im Gremium vorgestellt.

Der identifizierte Use-Case bezieht sich auf die bei meinem Haus eingehenden Meldungen von Datenschutzverstößen und deren Verteilung an die jeweils zuständige Organisationseinheit. Zunächst ist zu betonen, dass zurzeit keine konkrete Umsetzung dieses Use-Cases in meinem Haus geplant ist, sondern es sich um eine Vorüberlegung handelt. Die herausgearbeitete Idee sieht vor, dass ein Programm, welches – soweit notwendig – KI-Komponenten enthält und eingehende Meldungen von Datenschutzverstößen verarbeitet. Insbesondere soll der Inhalt der Meldung analysiert werden. Weiterhin soll das Programm erkennen, um welchen Verantwortlichen es sich handelt, um anhand dessen eine Zuweisung an die zuständige Organisationseinheit vorzunehmen. In jedem Fall wird die Meldung der zuständigen Organisationseinheit zur Bearbeitung vorgelegt, sodass jede Meldung von Datenschutzverstößen auch bei Umsetzung dieses Use-Cases weiterhin durch Mitarbeitende meines Hauses bearbeitet wird. Eine Vorhersage über die Schwere des Datenschutzverstoßes durch das Programm soll bei der Dringlichkeitsbewertung unterstützen. Mitarbeitende sollen Rückmeldung zur kontinuierlichen Verbesserung des Programms geben können, um dieses ggf. durch sog. Reinforcement-Learning besser an den Anwendungskontext anzupassen oder andere Anpassungen vorzunehmen.

10 Zentrale Anlaufstelle

Die in meinem Haus angesiedelte Zentrale Anlaufstelle (ZASt) unterstützt die Aufsichtsbehörden des Bundes und der Länder bei der Zusammenarbeit in EU-Angelegenheiten. Die ZASt setzt sich als Scharnier zwischen der deutschen und der europäischen Datenschutzaufsicht für eine gute gesamteuropäische Zusammenarbeit ein.

Leitung der Unterarbeitsgruppe „Statistik“

Der Datenschutz steht seit der Einführung der DSGVO unter besonderer politischer Aufmerksamkeit. So ist die Europäische Kommission gemäß Art. 97 DSGVO zur regelmäßigen Berichterstattung an das Europäische Parlament und den Rat über die Anwendung und die Wirkungsweise der DSGVO verpflichtet. In Vorbereitung dieser Berichte verlangt die Europäische Kommission eine Vielzahl von Kennzahlen und Auskünften von den Datenschutzaufsichtsbehörden. Auch der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlamentes ist bereits mit einem umfangreichen Fragenkatalog an die Datenschutzaufsichtsbehörden herangetreten. Die Koordinierung der Antworten der deutschen Datenschutzaufsicht und die Bereitstellung der gebündelten Auskünfte oblag der ZASt, die auf diesem Wege erhebliche Erfahrungswerte bei der Erstellung und Bearbeitung von Statistiken erworben hat.

Auf Initiative und unter der Leitung der ZASt wurde innerhalb des Arbeitskreises Organisation & Struktur der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) eine Unterarbeitsgruppe „Statistik“ gegründet, die konzeptionelle Überlegungen zu einem gemeinsamen nationalen Datenkranz anstellt. Die Datenschutzaufsichtsbehörden sollen so in die Lage versetzt werden, besser über ihre geleistete Arbeit gegenüber Europäischer Kommission, Europäischem Parlament sowie nationalen Parlamenten Rechenschaft ablegen zu können. Die auf diese Weise einheitlich gewonnenen Daten können von den Behörden weiterhin als internes Steuerungsinstrument genutzt werden. Ferner sollen diese Daten auch als Grundlage für Ressourcenforderungen an die jeweiligen Haushaltsgesetzgeber dienen. Parallel hierzu findet ein entsprechender Prozess auf EDSA-Ebene unter Leitung der Enforcement Expert Subgroup des EDSA statt. Die ZASt wirkt in ihrer Arbeit auf eine möglichst gleichförmige Entwicklung der Arbeiten an den Datenkränzen auf nationaler und europäischer Ebene hin.

Beiträge zur Stellungnahme des EDSA zum Verordnungsentwurf zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO

Wie bereits im Vorjahr, hat sich die ZASt im Berichtsjahr im Zuge der Stellungnahme des EDSA zu den Vorschlägen des Europäischen Parlaments und des Rats der Europäischen Union für eine europäische Verfahrensverordnung zur besseren Durchsetzung der DSGVO engagiert. Bereits voriges Jahr hatte die ZASt intensiv an der Stellungnahme der DSK sowie des EDSA zum ersten Verordnungsentwurf der Europäischen Kommission mitgewirkt.[176] Die ZASt hat auf dieses Rechtsetzungsvorhaben auf europäischer Ebene einen innerhalb der deutschen Datenschutzaufsicht besonderen Blickwinkel, der primär auf die Zuständigkeiten und Verfahren sowie Fristen gerichtet und immer mit der Überlegung verbunden ist, welche Anpassungen nationaler Prozesse und Arbeitsweisen durch die Vorgaben der Verfahrensverordnung erforderlich oder sinnvoll werden könnten.

Sobald eine finale Verordnung im Trilog der europäischen Gesetzgeber verabschiedet wird, sieht es die ZASt als ihre Aufgabe an, proaktiv Vorschläge für geeignete Anpassungen bei den bestehenden Prozessen und Koordinationsmechanismen in den Arbeitskreis Organisation & Struktur der DSK einzubringen. Ziel wird es hierbei sein, die absehbar komplexer werdenden europäischen

176 33. TB Nr. 11.1

Prozessschritte der grenzüberschreitenden Zusammenarbeit so zu adaptieren, dass die deutsche Datenschutzaufsicht weiterhin in hoher Qualität und unter Wahrung der neuen europäischen Fristen in koordinierter Art und Weise am europäischen Kooperations- und Kohärenzverfahren teilnehmen kann.

Entwicklungen rund um das Binnenmarktinformationssystem

Wie schon zuvor, hat die ZASt auch im aktuellen Berichtsjahr eine Grundlagenschulung und einen Workshop für die deutsche Datenschutzaufsicht in Bezug auf die grenzüberschreitende Zusammenarbeit im Binnenmarktinformationssystem (IMI) ausgerichtet. Beide Angebote wurden wieder sehr gut angenommen.

Weitergehend wurde die Zusammenarbeit mit dem Bundesministerium für Wirtschaft und Klimaschutz (BMWK), welches als zuständiges Ressort Deutschland in allgemeinen IMI-Angelegenheiten gegenüber der Europäischen Kommission vertritt, sowie mit der nationalen IMI-Koordinatorin im Bundesverwaltungsamt (BVA) gestärkt. Die ZASt konnte dem BMWK wichtige Impulse aus der praktischen Arbeit der deutschen und europäischen Datenschutzaufsichtsbehörden für die Sitzung des Europäischen IMI-Komitees und für einen Bericht an den Bundesrechnungshof mitgeben. Aufgrund der großen Anzahl von Nutzenden im IMI-Modul für die Zusammenarbeit der Datenschutzaufsichtsbehörden und deren institutionalisierter Austausch über die IT Users Expert Subgroup des EDSA kann erhebliches Anwenderwissen generiert werden. Die ZASt als zentrale deutsche Schnittstelle und Vertretung des Bundes in der IT Users Expert Subgroup ist fortlaufend bestrebt, diese vorhandene Expertise zur Verbesserung des IMI-Systems nutzbar zu machen. Die Zusammenarbeit in diesem Kontext soll daher weiter ausgebaut und intensiviert werden.

Koordinierung EU-geförderter Projekte

Ebenfalls im Berichtsjahr konnten die Abstimmungsprozesse unter den deutschen Aufsichtsbehörden in einem neuen Aspekt noch weiter verbessert werden. So wurden nach konzeptioneller Vorarbeit durch die ZASt die Prozesse im Zusammenhang mit der Beantragung EU-geförderter Projekte durch die Datenschutzaufsichtsbehörden des Bundes und der Länder neu organisiert. Um weiterhin schnell und effizient gegenüber Zuwendungsgebern, wie z. B. der Europäischen Kommission reagieren zu können, wurde nach entsprechender Beratung im Arbeitskreis Organisation & Struktur der DSK die Koordinierung einer abgestimmten Bewerbung deutscher Aufsichtsbehörden der ZASt übertragen. Die letztliche fachliche Entscheidung über etwaige Bewerbungen auf derartige Projekte liegt gleichwohl einzig bei den Datenschutzaufsichtsbehörden. Die ZASt agiert auch hier als Schnittstelle zwischen den deutschen Aufsichtsbehörden und der EU. Hierdurch ist nicht lediglich das Koordinationsportfolio der ZASt ausgeweitet worden, sondern es wird dadurch auch den rechtlichen Maßgaben in § 18 BDSG und dem DSGVO-Erwägungsgrund 119 Rechnung getragen, wonach sie für die gesteuerte Kommunikation gerade auch in Richtung der Europäischen Kommission zuständig ist.

Adressverteiler spezifischer Aufsichtsbehörden

Der im BDSG gebotenen Zusammenarbeit der DSK mit den sogenannten spezifischen Aufsichtsbehörden in den Bereichen Rundfunk und Religion konnte neuer Schub verliehen werden. Um die Einbindung der spezifischen Aufsichtsbehörden in die Arbeiten der DSK auch zwischen deren Sitzungen und der ihrer Arbeitskreise weiter zu stärken, hat die ZASt anknüpfend an einen entsprechenden Beschluss auf der 104. DSK einen Adressverteiler aufgesetzt und veröffentlicht. Dies ermöglicht den Datenschutzaufsichtsbehörden der DSK und den spezifischen Aufsichtsbehörden, jederzeit und schnell die richtigen Ansprechpersonen für einen zielgerichteten Austausch untereinander zu ermitteln. Ferner wird durch die Veröffentlichung des Adressverteilers auf der Internetseite der BfDI mit weiteren Erläuterungen auch der interessierten Öffentlichkeit Zugriff auf diese Informationen ermöglicht. Ein entsprechender Link auf der Website der DSK auf diese Veröffentlichung rundet das Informationsangebot ab.

Innerdeutsches Abstimmungsverfahren für Verhaltensregeln

Hinsichtlich Verhaltensregeln („Codes of Conduct“) für Unternehmen gemäß Art. 40 DSGVO wurden die Abstimmungsprozesse zwischen den deutschen Aufsichtsbehörden konkretisiert. Eine Arbeitsgruppe des Arbeitskreises Organisation und Struktur der DSK hat unter Beteiligung der ZASt einen Vorschlag für ein innerdeutsches Verfahren erarbeitet. Dieses stellt nun sicher, dass sich eine deutsche Datenschutzaufsichtsbehörde federführend mit den rechtlichen Fragestellungen der jeweiligen Verhaltensregeln befasst. Damit ist eine kontinuierliche Betreuung eines Vorganges sowohl auf deutscher als auch auf europäischer Ebene sichergestellt. Durch die nun geregelten Informationsprozesse und Beteiligungsgelegenheiten ist außerdem die Möglichkeit einer inhaltlichen Beteiligung für alle deutschen Aufsichtsbehörden gewährleistet. Der Vorschlag für das innerdeutsche Verfahren wurde anlässlich der 108. Datenschutzkonferenz im November 2024 angenommen.

Anlagen

Anlage 1

Kontrollierte Stellen

1&1 Mail & Media GmbH

Audi BKK

Auswärtiges Amt

Auswärtiges Amt, Botschaft Istanbul

Auswärtiges Amt, Botschaft London

Bahn BKK

Barmer

big direkt gesund

BKK Linde

BKK Pfalz

BKK ProVita

Blackpin GmbH

BMW BKK

Bundesamt für Bauwesen und Raumordnung

Bundesamt für das Personalmanagement der Bundeswehr

Bundesamt für den Militärischen Abschirmdienst

Bundesamt für die Sicherheit in der Informationstechnik

Bundesamt für Familie und zivilgesellschaftliche Aufgaben

Bundesamt für Migration und Flüchtlinge

Bundesamt für Verfassungsschutz

Bundesamt für Wirtschaft und Ausfuhrkontrolle

Bundesarbeitsgericht

Bundesbank

Bundeskriminalamt

Bundesministerium der Finanzen

Bundesministerium der Verteidigung

Bundesministerium des Innern und für Heimat

Bundesministerium für Wirtschaft und Klimaschutz

Bundesnachrichtendienst

Bundespolizei

Bundespolizeidirektion Berlin

Bundespolizeidirektion Sankt Augustin

Bundespolizeipräsidium

Bundesverwaltungsamt

Bundeszentralamt für Steuern

BWI GmbH

Cisco Systems GmbH

DAK-Gesundheit

Debeka BKK

Deutsche Industrie- und Handelskammer

Deutsche Rentenversicherung Bund

Deutsche Telekom AG

Deutscher Wetterdienst

Doctolib Siilo

Drillisch Online GmbH

Einsatzführungskommando der Bundeswehr

Eisenbahnbundesamt

FedEx Express Deutschland GmbH

Finanzamt Überlingen

Friedrich-Loeffler-Institut

Gemeinsames Extremismus- und Terrorismusabwehrzentrum

Generalbundesanwalt

Hauptzollamt Frankfurt am Main

Hauptzollamt Hamburg

hkk Krankenkasse

IKK classic

IKK Innovationskasse

Informationstechnikzentrum Bund

Jobcenter Baden-Baden

Jobcenter Mölln

Jobcenter Regensburg

Joint Intelligence Center

Karrierecenter der Bundeswehr Wilhelmshaven

Knappschaft Bahn See

Kraftfahrt-Bundesamt

Mobil Krankenkasse

Netcom Kassel Gesellschaft für Telekommunikation mbH

Pronova BKK

ready & go GmbH

Robert Koch-Institut

Scheval (Ungarn)

Stadtwerke Konstanz GmbH

Statistisches Bundesamt

Techniker Krankenkasse

Telefónica Germany GmbH & Co. OHG

Umweltbundesamt

Unternehmen (7) zum SÜG

Vodafone GmbH

Wirtschaftsprüferkammer

Zollkriminalamt

Anlage 2

Erlassene Maßnahmen/Beanstandungen gegenüber öffentlichen Stellen

Stelle	Maßnahme/Beanstandung	Grund
Agentur für Arbeit Elmshorn	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verspätete Auskunft
Agentur für Arbeit Leipzig	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Vertretung nach Eintritt Volljährigkeit nicht gelöscht
Agentur für Arbeit Rostock	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 DSGVO
Audi BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
Auswärtiges Amt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 S. 1 DSGVO und Art. 33 Abs. 1 DSGVO
Bahn-BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
Bahn-BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
Barmer Ersatzkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
Barmer Ersatzkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
Barmer Ersatzkasse	Verwarnung gemäß § 29 Abs. 3 TDDDG i. V. m. Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen § 25 TDDDG
Berufsgenossenschaft Verkehrswirtschaft Post-Logistik Telekommunikation	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Unrechtmäßige Datenweitergabe
Berufsgenossenschaft Verkehrswirtschaft Post-Logistik Telekommunikation	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 und Art. 9 Abs. 1 DSGVO
BITMARCK Technik GmbH	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
BKK firmus	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
BKK mkk - meine krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 Abs. 1 i. V. m. Art. 12 Abs. 3 DSGVO

Stelle	Maßnahme/Beanstandung	Grund
BKK mkk – meine krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
BKK mkk – meine krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
BKK Wirtschaft und Finanzen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
BKK Wirtschaft und Finanzen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Personalangelegenheiten werden innerhalb des BAAINBw unverschlüsselt an Funktionspostfächer übersandt (nur PersDat 2 klassifiziert)
Bundesamt für das Personalmanagement der Bundeswehr	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO, Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Speicherfristen der Bewerbungsunterlagen
Bundesamt für das Personalmanagement der Bundeswehr	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 15 Antrag zunächst nicht beantwortet
Bundesamt für Migration und Flüchtlinge	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 2 Abs. 1 S. 1 SÜG; Verstoß gegen § 15a SÜG; Verstoß gegen § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 64 BDSG
Bundesamt für Verfassungsschutz	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen Dokumentationspflichten nach Art. 20 Abs. 3 GG; gegen §§ 3 Abs. 1, 10 Abs. 1 Nr. 1 BVerfSchG; gegen § 17 Abs. 3 BVerfSchG; gegen §§ 12 Abs. 2, 13 Abs. 3 BVerfSchG; gegen § 12 Abs. 1 BVerfSchG; gegen § 28 Abs. 3 BVerfSchG
Bundesamt für Verfassungsschutz	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 36a Abs. 3 S. 1 und 2 SÜG; Verstoß gegen § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 64 BDSG; Verstoß gegen Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz
Bundesgesellschaft für Endlagerung mbH	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Fehlerhafte Zuweisung von Vorgesetzten in Zeiterfassungssystem
Bundesinnungs-krankenkasse Gesundheit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 6 Abs. 1 lit. a) DSGVO, Art. 15 Abs. 1 i. V. m. Art. 12 Abs. 3 DSGVO
Bundesinnungs-krankenkasse Gesundheit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
Bunndesministerium für Arbeit und Soziales	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 Abs. 1 DSGVO
Bundesministerium der Verteidigung	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Veröffentlichung Foto und Name in Y-Zeitschrift ohne Einwilligung

Stelle	Maßnahme/Beanstandung	Grund
Bundesnachrichtendienst	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verarbeitung der Kontoauszüge für TG-Empfänger
Bundesnachrichtendienst	Beanstandung gem. § 16 Abs. 2 BDSG	Verstoß gegen § 63 BNDG i. V. m. § 28 Abs. 3 BVerfSchG
Bundesnachrichtendienst	Beanstandung gem. § 16 Abs. 2 BDSG	Verstoß gegen § 63 BNDG i. V. m. § 28 Abs. 3 BVerfSchG
Bundespolizei	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 64 BDSG, Verstoß gegen § 3a Abs. 1 S. 1 und Abs. 2 S. 1 SÜG i. V. m. SÜG-AVV zu § 3a Abs. 1 und 2; Verstoß gegen § 2 Abs. 1 S. 1 SÜG i. V. m. SÜG-AVV zu § 2 Abs. 1 S. 1; Verstoß gegen § 19 Abs. 2 S. 1 und 2, 22 Abs. 2 Nr. 1 SÜG; Verstoß gegen § 22 Abs. 2 Nr. 1 SÜG
Bundespolizei	Beanstandung gemäß § 16 Abs. 2 BDSG	Keine Benennung aufgrund einer Einstufung
Bundespolizei	Beanstandung gemäß § 16 Abs. 2 BDSG	Keine Benennung aufgrund einer Einstufung
Bundespolizeipräsidium	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Weitergabe personenbezogener Daten an Gesundheitsamt und Landespolizei
Bundespresseamt	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 18 SÜG; Verstoß gegen § 2 Abs. 1 S. 3 SÜG; Verstoß gegen § 20 Abs. 1 SÜG i. V. m. § 36 Abs. 1 Nr. 2 SÜG und § 64 Abs. 1 S. 1 BDSG; Verstoß gegen §§ 19 Abs. 2 und 22 Abs. 2 SÜG
Bundesverwaltungsamt	Warnung gemäß § 16 Abs. 2 S. 4 BDSG, Art. 58 Abs. 2 lit. b) DSGVO	Warnung vor bevorstehendem Verstoß gegen § 2 Nr. 3 IDNrG wegen Datenübermittlung unter Verwendung der IDNr, bevor das Datenschutzcockpit in Betrieb ist.
Bundesverwaltungsamt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO wegen fahrlässiger Nichtlöschung und Weiterleitung nicht anonymisierter Echtdaten zu Testzwecken ohne Rechtsgrundlage sowie unzureichender Anonymisierungsmaßnahmen
Bundesverwaltungsamt	Verwarnung gemäß § 29 Abs. 3 TTDSG (nunmehr TDDDG) i. V. m. Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen § 25 Abs. 1 TTDSG wegen des Einsatzes eines Analyse-/Tracking-Tools (Webseite service.bund.de) mit Zugriff auf Endgerät ohne Einholung einer Einwilligung
Bundesverwaltungsamt	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 64 BDSG
Bundeswehr Logistikbataillon	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	E-Mail-Verteiler an private Adressen von Reservisten ohne bcc-Nutzung
Continentale BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO

Stelle	Maßnahme/Beanstandung	Grund
DAK-Gesundheit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
DAK-Gesundheit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
DAK-Gesundheit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO und Art. 32 Abs. 1 DSGVO
Deutsche Rentenversicherung Bund	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 DSGVO
Deutsche Rentenversicherung Bund	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 DSGVO
Deutsche Rentenversicherung Bund	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
Deutsche Rentenversicherung Bund	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 DSGVO
Deutsche Rentenversicherung Knappschaft-Bahn-See	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO und Art. 9 Abs. 1 DSGVO
Deutsche Rentenversicherung Knappschaft-Bahn-See	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO, Anweisung nach Art. 58 Abs. 2 lit. c) DSGVO	Verstoß gegen Art. 15 DSGVO
Familienkasse Bayern Nord	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 DSGVO – Offenbarung Namen und Geburtsdatum – keine geeigneten TOMs
Finanzamt Frankfurt am Main III	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) DSGVO – Unverzügliche Benachrichtigung gem. Art. 34 Abs. 1 DSGVO nicht erfolgt
Finanzamt für Groß- und Konzernbetriebsprüfung Herne	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstöße gegen Art. 15 und 12 Abs. 3 DSGVO – Auskunftsersuchen nicht unverzüglich und nicht umfänglich nachgekommen
Finanzamt Kleve	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstöße gegen Art. 33 Abs. 1 und 34 Abs. 1 DSGVO wegen Unterlassung der Meldung und Benachrichtigung über eine Datenschutzverletzung
Generalzolldirektion	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 33 – Meldung zur Offenlegung von Abwesenheitsgründen 267 Beschäftigter im SC Dresden über einen Zeitraum von 14 Jahren
Hauptzollamt Osnabrück	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Einführung von Teamkalender per Outlook

Stelle	Maßnahme/Beanstandung	Grund
Hauptzollamt Potsdam	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 und 12 Abs. 3 DSGVO – Auskunftsersuchen nicht unverzüglich und nicht umfänglich nachgekommen
HEK Hanseatische Krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 Abs. 1 und Art. 12 Abs. 3 DSGVO
IKK classic	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 lit. a) DSGVO; Verstoß gegen Art. 15 Abs. 1 und Art. 12 Abs. 3 DSGVO
IKK classic	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
IKK gesund plus	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
Informationstechnik-zentrum Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Auskunftsersuchen nach Art. 15 DSGVO nicht beantwortet
Informationstechnik-zentrum Bund	Verwarnung gemäß § 29 Abs. 3 TTDSG i. V. m. Art. 58 Abs. 2 lit. b) DSGVO	Verstoßes gegen § 25 Abs. 1 TTDSG Übermittlung von IP-Adressen an Twitter ohne Einwilligung
Informationstechnik-zentrum Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoßes gegen Art. 6 Abs. 1 DSGVO wegen der unverschlüsselten Ablage einer Liste mit ca. 1600 Telefonnummern von internen und externen Mitarbeitern auf einem Transferlaufwerk.
Informationstechnik-zentrum Bund	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen §§ 24, 25 Abs. 3 SÜG; Verstoß gegen § 2 Abs. 1 S. 1 SÜG; Verstoß gegen § 18 Abs. 1 und Abs. 3 S. 3 SÜG; Verstoß gegen § 20 Abs. 1 i. V. m. § 36 Abs. 1 Nr. 2 SÜG und § 64 Abs. 1 S. 1 BDSG; Verstoß gegen § 18 Abs. 1 und 2 SÜG; Verstoß gegen § 22 Abs. 2 Nr. 1 SÜG
Jobcenter Berlin Pankow	Warnung gemäß Art. 58 Abs. 2 lit. a) DSGVO	Anforderung doppelter und ungeschwärzter Kontoauszüge
Jobcenter Braunschweig, Stadt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Öffnung Unterlagen für Ärztlichen Dienst durch Jobcenter-Mitarbeiter
Jobcenter Düsseldorf	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verlust von Unterlagen
Jobcenter Frankfurt am Main	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO, Anweisung Art. 58 Abs. 2 lit. d) DSGVO	Dritterhebung
Jobcenter Frankfurt am Main	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Erhebung ungeschwärzte Kontoauszüge
Jobcenter Harburg	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Anforderung Kopie Personalausweis

Stelle	Maßnahme/Beanstandung	Grund
Jobcenter Kassel, Stadt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Ersterhebung – Vermieter
Jobcenter Köln	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Ersterhebungsgrundsatz; Offenbarung damaliger Leistungsbezug; Inhaltsangabe auf Umschlag Postzustellungsurkunde
Jobcenter Märkischer Kreis	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Weitergabe von Gesundheitsdaten des Petenten an die Schwerbehindertenvertretung ohne Wissen und Wollen des Petenten
Jobcenter Mettmann	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Führen einer elektronischen, für alle Beschäftigten zugänglichen Liste über Fehler aller Beschäftigten im Rahmen der fachlichen Aufgabenerledigung
Jobcenter Oberberg	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Auskunft nach Art. 15 DSGVO abgelehnt.
Jobcenter Ostholstein	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 DSGVO
Jobcenter Rhein-Sieg	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Rechtsgrundlose Speicherung von Beschäftigtendaten auf elektronischem Laufwerk einer Geschäftsstelle
Joint Intelligence Center Bundeswehr	Beanstandung gem. § 16 Abs. 2 BDSG	Vorratsdatenspeicherung
Karrierecenter der Bundeswehr Wilhelmshaven	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 19 Abs. 2 SÜG und § 18 Abs. 3a SÜG
Kassenärztliche Bundesvereinigung	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 Abs. 1 DSGVO
Militärhistorisches Museum der Bundeswehr	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Übermittlung Krankheitsdaten
Mobil BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO, Art. 9 Abs. 1 DSGVO
Mobil BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
Pronova BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO
Securvita BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
Siemens Betriebskrankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
Siemens Betriebskrankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
Techniker Krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 DSGVO

Stelle	Maßnahme/Beanstandung	Grund
Techniker Krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO und Art. 9 Abs. 1 DSGVO
Techniker Krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO und Art. 9 Abs. 1 DSGVO
Technisches Hilfswerk	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Nichteinhaltung der Bearbeitungsfristen gem. Art. 12 Abs. 3 und 4 DSGVO
vivida BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO

Nicht alle der oben aufgelisteten Maßnahmen und Beanstandungen sind bisher rechtskräftig.

Anlage 3

Erlassene Maßnahmen/Beanstandungen gegenüber nicht-öffentlichen Stellen

Stelle	Maßnahme/Beanstandung	Grund
Ein Postdienstleistungs-unternehmen	Verwarnung gem. Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 Abs. 1 lit. b) DSGVO wg. Unterlassung, geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen, dass ein Endpunkt einer IT-Anwendung aus dem Internet nur mit Authentisierung zugänglich war.
Ein Postdienstleistungs-unternehmen	Verwarnung gem. Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 44 DSGVO wegen Übermittlung personenbezogener Daten an ein Drittland, ohne die in Kapitel V der DSGVO niedergelegten Bedingungen einzuhalten
Ein Postdienstleistungs-unternehmen	Verwarnung gem. Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 Abs. 1 DSGVO
Ein Postdienstleistungs-unternehmen	Verwarnung gem. Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 DSGVO wegen mangelnder technischer und organisatorischer Maßnahmen, die sicherstellen, dass Ausweisdaten nur verschlüsselt an die Verantwortliche Stelle übermittelt werden.
Ein Postdienstleistungs-unternehmen	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 und Art. 32 Abs. 1 DSGVO
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung gemäß Art. 58 Abs. 2 lit. c) DSGVO	Verstöße gegen Art. 15 DSGVO, Art. 17 DSGVO. Das Unternehmen führt keine Löschung und Werbewidersprüche durch.
Ein Telekommunikations-dienstleistungs-unternehmen	Festsetzung Zwangsgeld nach Nichterfüllung einer Anweisung gemäß Art. 58 Abs. 1 lit. a) DSGVO	Keine Vorlage einer Datenschutzerklärung gemäß Art. 13 DSGVO, keine Mitteilung über den Versand der Datenschutzerklärung an Personen im Rahmen der Verfügbarkeitsprüfung und im Rahmen von Vertragsabschlüssen sowie über Speicherung von personenbezogenden Daten.
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung gemäß Art. 58 Abs. 2 lit. c) DSGVO	Verstöße gegen Art. 15 DSGVO, Art. 17 DSGVO. Das Unternehmen führt keine Löschung und Werbewidersprüche durch.
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung gemäß Art. 58 Abs. 2 lit. c) DSGVO	Verstoß gegen Art. 15 DSGVO; Unternehmen erteilt keine Auskunft.
Ein Telekommunikations-dienstleistungs-unternehmen	Festsetzung Zwangsgeld nach Nichterfüllung einer Anweisung gemäß Art. 58 Abs. 2 DSGVO	Keine Vorlage einer Datenschutzerklärung gemäß Art. 13 DSGVO; keine Mitteilung über den Versand der Datenschutzerklärung an Personen im Rahmen der Verfügbarkeitsprüfung und im Rahmen von Vertragsabschlüssen sowie über Speicherung von personenbezogenden Daten.

Stelle	Maßnahme/Beanstandung	Grund
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung gemäß Art. 58 Abs. 2 lit. c) DSGVO	Verstoß gegen Art. 15 DSGVO; Unternehmen erteilt keine Auskunft
Ein Telekommunikations-dienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO, § 29 Abs. 3 TDDDG	Entgegen der gebotenen Sorgfalt wurden Bestandsdaten nach Vertragsbeendigung sowie (nicht abrechnungsrelevante) Verkehrsdaten nicht unverzüglich gelöscht. (daneben Zwangsgeldandrohung).
Ein Telekommunikations-dienstleistungs-unternehmen	Festsetzung Zwangsgeld nach § 14 Verwaltungs-vollstreckungsgesetz (VwVG)	Anweisung, aufgeführte Informationen bzw. Erklärungen vorzulegen und für den Fall des Verstoßes wurde ein Zwangsgeld in Höhe von 6.000,00 EUR angedroht. Der Anweisung wurde nicht nachgekommen.
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung nach Art. 58 Abs. 1 lit. a) DSGVO	Nicht unverzüglich erstattete Meldung nach § 169 Abs. 1 S. 1 TKG, da Einzelverbindungsnachweise ohne Passwort über das Internet zugänglich waren.
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung nach Art. 58 Abs. 2 lit. c) DSGVO	Verstöße gegen Art. 15 DSGVO, Art. 17 DSGVO. Das Unternehmen führt keine Löschung und Werbewidersprüche durch.
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung nach Art. 58 Abs. 2 lit. c) DSGVO	Verstöße gegen Art. 15 DSGVO, Art. 17 DSGVO. Das Unternehmen führt keine Löschung und Werbewidersprüche durch.
Ein Telekommunikations-dienstleistungs-unternehmen	Festsetzung Zwangsgeld nach §§ 14, 19 Verwaltungs-vollstreckungsgesetz (VwVG)	Verstoß gegen Anweisung nach Art. 58 Abs. 2 lit. c) DSGVO. Daneben wurden in 30 Fällen die Betroffenenrechte nach der DSGVO nicht erfüllt. Zwangsgeld in Höhe von 60.000,00 EUR festgesetzt.
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung nach Art. 58 Abs. 2 lit. d)	Keine Benennung eines EU-Vertreters, Datenschutzerklärung nur in englischer Sprache
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen §§ 30, 19 Abs. 2 und §§ 31 S. 2, 22 Abs. 2 SÜG
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen §§ 30, 19 Abs. 2 und §§ 31 S. 2, 22 Abs. 2 SÜG; Verstoß gegen Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 30 i. V. m. § 18 Abs. 1 SÜG
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 64 BDSG; Verstoß gegen §§ 30, 19 Abs. 2 und §§ 31 S. 2, 22 Abs. 2 SÜG; Verstoß gegen § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 51 Abs. 1 BDSG; Verstoß gegen § 31 SÜG; Verstoß gegen § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 64 Abs. 1 S. 1 BDSG

Stelle	Maßnahme/Beanstandung	Grund
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen §§ 30, 18 Abs. 1 und 2 SÜG; Verstoß gegen §§ 30, 19 Abs. 2 SÜG und §§ 31 S. 2, 22 Abs. 2 Nr. 1 SÜG; Verstoß gegen § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 51 Abs. 1 BDSG

Nicht alle der oben aufgelisteten Maßnahmen und Beanstandungen sind bisher rechtskräftig.

Anlage 4

Übersicht Gremien national/ europäisch/international

Nationale Gremien:

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (kurz: Datenschutzkonferenz bzw. DSK)

Arbeitskreise (AK) der DSK:

- AK Auskunfteien und Inkasso (Vorsitz Bayern BayLDA)
- AK Beschäftigtendatenschutz (Vorsitz Niedersachsen)
- AK Datenschutz-/Medienkompetenz (Vorsitz Thüringen)
- AK Europa (Vorsitz BfDI)
- AK Gesundheit und Soziales (Vorsitz Berlin und Sachsen)
- AK Grundsatzfragen (Vorsitz BfDI)
- AK Internationaler Datenverkehr (Vorsitz Berlin und Bayern BayLDA)
- AK Justiz (Vorsitz Bayern LfD Bayern)
- AK Kreditwirtschaft (Vorsitz Nordrhein-Westfalen)
- AK Medien (Vorsitz Berlin und Hamburg)
- AK Organisation und Struktur (Vorsitz Hessen)
- AK Presse- und Öffentlichkeitsarbeit (Vorsitz BfDI)
- AK Sanktionen (Vorsitz Berlin)
- AK Schulen und Bildungseinrichtungen (Vorsitz Thüringen)
- AK Sicherheit (Vorsitz Schleswig-Holstein)
- AK Statistik (Vorsitz Nordrhein-Westfalen)
- AK Steuerverwaltung (Vorsitz BfDI)
- AK Technik (Vorsitz Mecklenburg-Vorpommern)
- AK Verkehr (Vorsitz BfDI)
- AK Versicherungswirtschaft (Vorsitz Niedersachsen)
- AK Verwaltung (Vorsitz Brandenburg und Baden-Württemberg)
- AK Videoüberwachung (Vorsitz Baden-Württemberg)
- AK Werbung und Adresshandel (Vorsitz Bayern BayLDA und Nordrhein-Westfalen)
- AK Wirtschaft (Vorsitz Nordrhein-Westfalen)
- AK Wissenschaft und Forschung (Vorsitz Hessen)
- AK Zertifizierung (Vorsitz Schleswig-Holstein)
- AK DSK 2.0 (Vorsitz Rheinland-Pfalz)
- AK Künstliche Intelligenz (Vorsitz Rheinland-Pfalz und Baden-Württemberg

Konferenz der Informationsfreiheitsbeauftragten in Deutschland

AK Informationsfreiheit der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

Gremien der Europäischen Union:

- Europäischer Datenschutzausschuss (EDSA)

Expert Subgroups des EDSA:

- Borders, Travel and Law Enforcement Expert Subgroup (Koordination BfDI)
- Compliance, e-Government and Health Expert Subgroup
- Cooperation Expert Subgroup (Co-Koordination BfDI)
- Coordinators Expert Subgroup (Co-Koordination BfDI)
- Cross-Regulatory Interplay and Cooperation Subgroup
- Enforcement Expert Subgroup
- Financial Matters Expert Subgroup
- International Transfers Expert Subgroup
- IT Users Expert Subgroup
- Key Provisions Expert Subgroup
- Social Media Expert Subgroup
- Strategic Advisory Expert Subgroup
- Technology Expert Subgroup (Co-Koordination BfDI)

Task Forces des EDSA:

- Taskforce Chat GPT
- Taskforce Fining (Co-Koordination BfDI)
- Taskforce International Engagement (Co-Koordination BfDI)

Coordinated Enforcement Framework des EDSA

Support Pool of Experts des EDSA

Coordinated Supervision Committee
(Stellvertretende Koordination BfDI)

ETIAS Fundamental Rights Guidance Board
(Vorsitz BfDI)

Internationale Gremien:

G7 DPA Roundtable (Vorsitz liegt bei jeweiliger G7-Präsidentschaft, 2024: Italien)

Arbeitsgruppen des G7 DPA Roundtable:

- Emerging Technologies Working Group (Koordinator Vereinigtes Königreich; BfDI ist Mitglied)
- Enforcement Cooperation Working Group (Koordinatoren U.S. FTC und Japan; BfDI ist Mitglied)
- Data Free Flow with Trust Working Group (Koordinatoren BfDI und Vereinigtes Königreich)

International Working Group on Data Protection in Technology (IWGDPT – „Berlin Group“)
(Vorsitz und Sekretariat BfDI)

Global Privacy Assembly (GPA)

Leitende Ausschüsse für die Vorsitzenden der GPA, in denen BfDI als Mitglied vertreten ist:

- Executive Committee (Vorsitz Mexico; BfDI ist gewähltes Mitglied)
- Strategic Direction Sub-Committee (Vorsitz Argentinien; BfDI ist Mitglied)
- Host Selection Sub-Committee (Vorsitz Mexico; BfDI ist Mitglied)

Arbeitsgruppen der GPA:

- Global Standards and Frameworks Working Group (Koordinator Vereinigtes Königreich, BfDI ist Mitglied)
- International Enforcement Cooperation Working Group (Koordinatoren Kanada, Japan, Hongkong und Kolumbien; BfDI ist Mitglied)
- Data Sharing Working Group (Koordinator Jersey; BfDI ist Mitglied)
- Ethics and Data Protection in Artificial Intelligence Working Group (Koordinatoren Frankreich und EDPS; BfDI ist Mitglied)
- Digital Economy and Society Working Group (Koordinator: Marokko; BfDI ist Mitglied)

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

- Working Party Data Governance and Privacy (Vorsitz Kanada; BfDI ist beratendes Mitglied der deutschen Delegation)
- Data Free Flow with Trust (DFFT) Expert Community (BfDI ist Mitglied)
- AI, Data and Privacy Expert Group (BfDI ist Mitglied)

Europarat – Beratender Datenschutz-Ausschuss
(T-PD; Vorsitz Deutschland, vertreten durch BMI; BfDI ist beratendes Mitglieder der deutschen Delegation

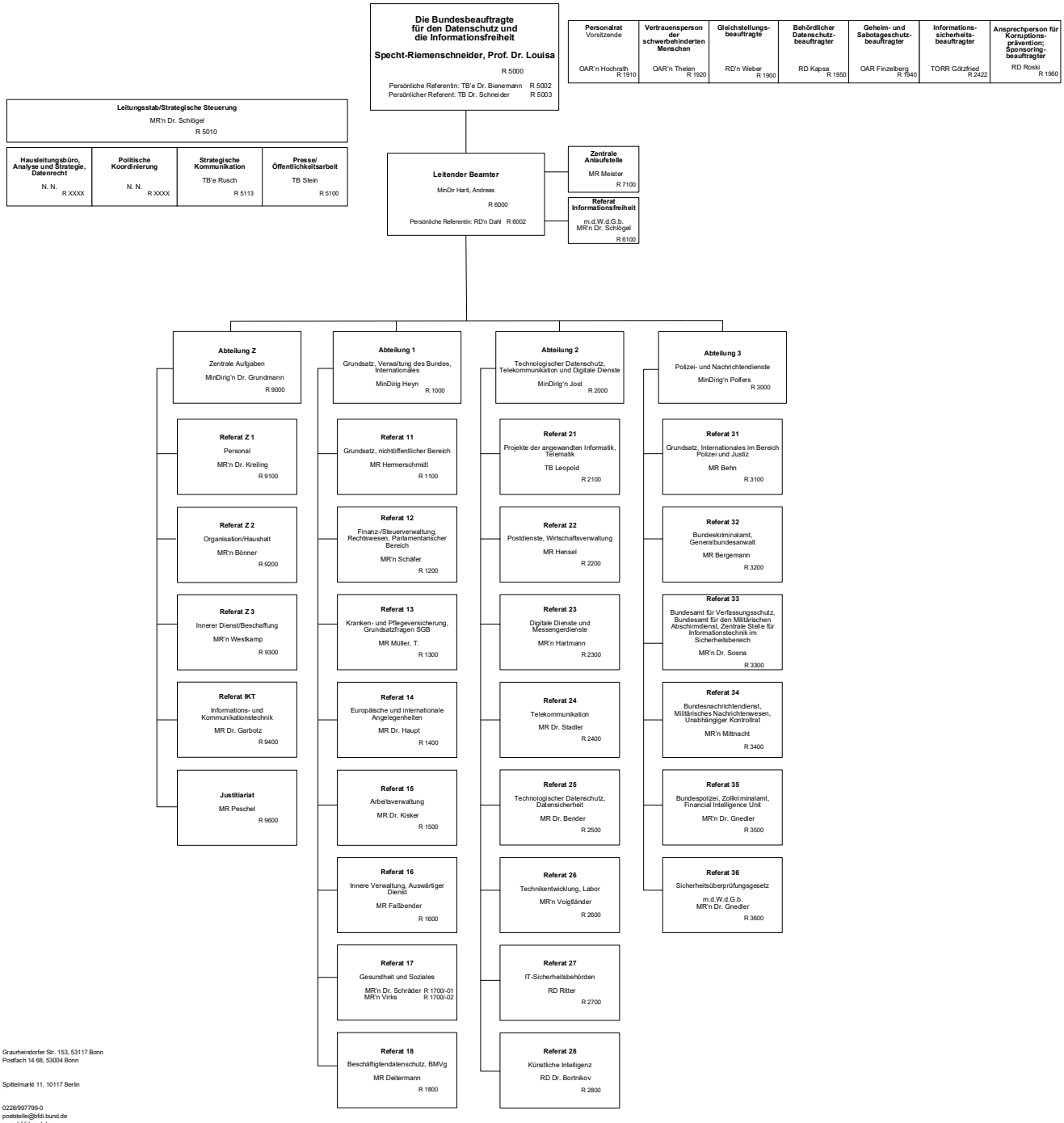
Global Privacy Enforcement Network
(GPEN; Komitee mit den USA, dem Vereinigten Königreich, Kanada, Israel und Hongkong; BfDI ist Mitglied)

Europäische Datenschutzkonferenz (Spring Conference)
(Vorsitz beim jeweiligen Gastgeber, 2024: Lettland, 2025: Georgien; BfDI ist Mitglied)

European Case Handling Workshop
(Vorsitz beim jeweiligen Gastgeber, 2024: Estland; BfDI ist Mitglied)

International Conference of Information Commissioners
(BfDI ist Mitglied des Executive Committee)

BfDI
Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit



hrift:
itsitz Bonn: Graurheindorfer Str. 153, 53117 Bonn
Postfach 14 68, 53004 Bonn

ndungsbüro
t: Spittelmarkt 11, 10117 Berlin

chbarkeit:
on: 0228/997799-0
il: poststelle@bfdi.bund.de
et: www.bfdi.bund.de

t: 17. Februar 2025

Abkürzungsverzeichnis

a. a. O.	am angegebenen Ort
AA	Auswärtiges Amt
Abs.	Absatz
AG	Aktiengesellschaft
AK	Arbeitskreis
ANSWER	Analyse- und Auswertung
Art.	Artikel
ATD	Anti-Terror-Datei
ATI	Access to Information
Az.	Aktenzeichen
AZR	Ausländerzentralregister
AZRG	Ausländerzentralregistergesetz
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BAMF	Bundesamt für Migration und Flüchtlinge
BBF	Bundesamt zur Bekämpfung der Finanzkriminalität
bDSB	behördliche Datenschutzbeauftragte
BDSG	Bundesdatenschutzgesetz
BeschDG	Beschäftigtendatenschutzgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfJ	Bundesamt für Justiz
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BIPAM	Bundesinstitut für Prävention und Aufklärung in der Medizin
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BKAmt	Bundeskanzleramt
BKartA	Bundeskartellamt
BKG	Bundes-Kindergrundsicherungs-Gesetz
BMAS	Bundesministerium für Arbeit und Soziales
BMBF	Bundesministerium für Bildung und Forschung
BMF	Bundesministerium der Finanzen
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern und für Heimat
BMJ	Bundesministerium der Justiz
BMVg	Bundesministerium der Verteidigung
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur
BPOL	Bundespolizei
BPolG	Bundespolizeigesetz
BPOLP	Bundespolizeipräsidium
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht

BWA	Bewacherregister
BWG	Bundeswahlgesetz
BWO	Bundeswahlordnung
BZgA	Bundeszentrale für gesundheitliche Aufklärung
BZSt	Bundeszentralamt für Steuern
CBPR	Global Cross-Border Privacy Rules
CEA	Coordinated Enforcement Action
CEF	Coordinated Enforcement Framework
CIS	Zollinformationssystem
CNIL	Commission Nationale de l'Informatique et des Libertés (Französische Datenschutzaufsichtsbehörde)
CSAM	Child sexual abuse material
CSA-VO	Verordnung zum Auffinden von Material des sexuellen Online-Kindesmissbrauchs
CSC	Coordinated Supervision Committee
DDG	Digitale-Dienste-Gesetz
DFFT	Data Free Flow with Trust
DigiG	Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens
DMA	Digital Markets Act
DPC	Data Protection Commission (Irische Datenschutzaufsichtsbehörde)
DPF	EU-U.S. Data Privacy Framework
DSA	Digital Services Act
DSC	Datenschutzcockpit
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhänigegen Datenschutzbehörden des Bundes und der Länder
e. V.	eingetragener Verein
ECRIS TCN	Europäisches Strafregisterinformationssystem für Drittstaatsangehörige und Staatenlose
EDHS	European Health Data Space Verordnung
EDPS	Europäischer Datenschutzbeauftragter
EDSA	Europäischer Datenschutzausschuss
EES	Entry-Exit-System
eFBS	einheitliches Fallbearbeitungssystem
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
eGK	elektronische Gesundheitskarte
EGMR	Europäischer Gerichtshof für Menschenrechte
EGovG	E-Government-Gesetz
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
EHDS	European Health Data Space
eID	elektronischer Personalausweis
eIDAS VO	Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
EnWG	Energiewirtschaftsgesetz
ePA	elektronische Patientenakte
ETIAS	European Travel and Authorization System
EU	Europäische Union
EUDI-Wallet	European Digital Identity Wallet
EuGH	Europäischer Gerichtshof
EZV	Ermittlungszentrum Vermögensverschleierung
f.	folgende
FAQ	Frequently asked questions
FDP	Frei Demokratische Partei
FDZ	Forschungsdatenzentrum Gesundheit

ff.	fortfolgende
FIU	Financial Intelligence Unit
FKBG	Finanzkriminalitätsbekämpfungsgesetz
FlugDaG	Fluggastdatengesetz
GBA	Generalbundesanwalt beim Bundesgerichtshof
GDNG	Gesundheitsdatennutzungsgesetz
gematik	Gesellschaft für Telematik
GenDG	Gendiagnostikgesetz
GETZ	Gemeinsames Extremismus- und Terrorismusabwehrzentrum
GG	Grundgesetz
ggf.	gegebenenfalls
GKV SV	Spitzenverband Bund der Krankenkassen
grds.	grundsätzlich
GS RegMo	Gesamtsteuerung Registermodernisierung
GTAZ	Gemeinsames Terrorismusabwehrzentrum
GVSG	Gesundheitsversorgungsstärkungsgesetz
GwG	Geldwäschegesetz
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HDL	Health Data Lab
HLG	High Level Group on access to data for effective law enforcement
i. S. v.	im Sinne von
ICIC	Internationale Konferenz der Informationsfreiheitsbeauftragten
IDNr	Identifikationsnummern
IDNrG	Identifikationsnummerngesetz
IFG	Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten
IMI	Binnenmarktinformationssystem
INPOL-Z	Polizeilicher Informationsverbund
IoT	Internet of Things
IP	Internet Protocol
IRD	Implantateregister
IT	Informationstechnologie
IT-PLR	IT-Planungsrat
IWGDPT	International Working Group on Data Protection in Technology
JCAS	Joint Communication and Sensing
JI-Richtlinie	Richtlinie zum Datenschutz bei Polizei und Justiz
KAS	Konrad-Adenauer-Stiftung
KI	Künstliche Intelligenz
LG	Landgericht
LIBE	Ausschuss für bürgerliche Freiheiten, Justiz und Inneres
lit.	Buchstabe
LLM	Large Language Model
MADG	Gesetz über den Militärischen Abschirmdienst
MII Broad Consent	Mustereinwilligung der Medizin-Informatik-Initiative
MilNW	Militärisches Nachrichtenwesen
MiStra	Anordnung über Mitteilungen in Strafsachen
MJP	Mein Justizpostfach
MsbG	Messstellenbetriebsgesetz

n. F.	neue Fassung
NADIS	Nachrichtendienstliches Informationssystem
NGO	Nichtregierungsorganisation
NIICS	Number-Independent Interpersonal Communication Services
NIS2-Richtlinie	Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union
NIS2UmsuCG	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
NOOTS	Nationales Once-Only-Technical-System
Nr.	Nummer
NWR	Nationales Waffenregister
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OLG	Oberlandesgericht
OSINT	Open Source Intellligence
OZG	Onlinezugangsgesetz
P 20	Polizei 20/20
PassG	Passgesetz
PAuswG	Personalausweisgesetz
PB Recht	Programmbereich Recht
PDLV	Postdienstleistungsverordnung
PIAV-S	Polizeilicher Informations- und Analyseverbund
PIN	persönliche Identifikationsnummer
PIU	Fluggastdatenzentralstelle
PMK	Politisch-Motivierte-Kriminalität
PNR	Passenger Name Records
PoC	Proof of Concept
PostG	Postgesetz
PUDLV	Post-Universaldiensleistungsverordnung
PUF	Public Use File
RED	Rechtsextremismus-Datei
RegMoB	Registermodernisierungsbehörde
RKI	Robert Koch-Institut
Rn.	Randnummer
S.	Satz
SaBe	Sabotageschutzbeauftragte
SAK	Sicherer Anschlussknoten
SCG	VIS Supervision Coordination Group
SDK	Software Development Kit
SG	Sozialgericht
SGB II	Sozialgesetzbuch Zweites Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SiBe	Sicherheitsbevollmächtigte
SOCMINT	Social Media Intelligence
sog.	sogenannte
SPD	Sozialdemokratische Partei Deutschlands
SPoE	Support-Pool-of-Experts
StBA	Statistisches Bundesamt
Steuer-ID	Steuer-Identifikationsnummer
StiftFinG	Stiftungsfinanzierungsgesetz

stopp	Strafprozessordnung
SÜG	Sicherheitsüberprüfungsgesetz
TB	Tätigkeitsbericht
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
Tech ESG	Technology Experts Subgroup
TFFD	Taskforce Forschungsdaten
TTDSG	Telekommunikation-Telemedien-Datenschutzgesetz
u. a.	unter anderem
UIG	Umweltinformationsgesetz
UKRat	Unabhänigiger Kontrollrat
US/U.S.	United States
USA	Vereinigte Staaten von Amerika
VIP	Verwaltungsdaten Informationsplattform
VIS	Visa-Informationssystem
VO	Verordnung
VSA	Verschlusssachenanweisung
VS-NfD	Verschlusssache – nur für den Dienstgebrauch
VS-Verbung	Verbund aus Bundesamt für Verfassungsschutz und Landesbehörden für Verfassungsschutz
VVBG	Vermögensverschleierungsbekämpfungsgesetz
VVO	Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO
VwVfG	Verwaltungsverfahrensgesetz
VZÄ	Vollzeitäquivalent
z. B.	zum Beispiel
ZASt	Zentrale Anlaufstelle
ZKA	Zollkriminalamt

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333