Tätigkeitsbericht 2023

32. Tätigkeitsbericht
für den Datenschutz und
die Informationsfreiheit

BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Tätigkeitsbericht für das Jahr 2023
– 32. Tätigkeitsbericht –

Dieser Bericht wurde der Präsidentin des Deutschen Bundestags, Frau Bärbel Bas, überreicht.

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

Inhaltsverzeichnis

1 Einleitung

Im Jahr 2023 wurden zahlreiche Themen, die wir national und international bereits im Vorjahr auf den Weg gebracht haben, in Form von Beschlüssen und Empfehlungen finalisiert oder zumindest weiterentwickelt.

Fünf Jahre nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) hat sich diese trotz der anfänglichen Unsicherheiten als Erfolgsmodell erwiesen und garantiert eine verbesserte Rechtsdurchsetzung in Europa. Hierzu trägt auch bei, dass wir im Europäischen Datenschutzausschuss (EDSA) die Leitlinien zur Bußgeldzumessung in Europa beschlossen und damit einen weiteren Meilenstein für die einheitliche Anwendung des Datenschutzrechtes in der EU gesetzt haben.

Der neue europäische Datenschutzstandard findet zunehmend auch international Eingang in die Datenschutzregelungen anderer Länder und hat sich damit als der Goldstandard für die internationale Zusammenarbeit erwiesen. So war unsere Beratung auch außerhalb der EU gefragt, unter anderem von einer Gruppe der größten Pazifik-Anrainer-Staaten (Global CBPR), die einen freien Datenverkehr untereinander und mit Europa erreichen wollen.

Auch in den internationalen Gremien, in denen ich aktiv mitwirke, wurde der Einsatz für freie und vertrauenswürdige globale Datenverkehre fortgesetzt („Data Free Flow with Trust" – DFFT). Eine wesentliche Bedingung hierfür sind grundrechtsbasierte, demokratische Regelungen für den Zugriff staatlicher Stellen auf privat gehaltene Daten zu Zwecken der nationalen Sicherheit oder Strafverfolgung.

Bei diversen weiteren internationalen Projekten setzte ich mein Engagement fort, etwa als Berichterstatter eines derzeit im Rahmen des G7 DPA Roundtable entwickelten Referenzdokuments zu Zertifizierungen nach europäischer Datenschutzgrundverordnung und ‚Global Cross-Border Privacy Rules'. Als Mitinitiator der diesjährigen „Resolution on Achieving Global Data Protection Standards" der Global Privacy Assembly setze ich mich für hohe internationale Datenschutzstandards auf globaler Ebene ein.

Ein weiteres wichtiges Thema, das mich im Berichtsjahr begleitet hat, waren die vielen verschiedenen europäischen Digitalrechtsakte. Deren horizontale Ausgestaltung wird in Zukunft die zwischenbehördliche Kommunikation und Zusammenarbeit auf nationaler und europäischer Ebene noch wichtiger machen, als sie ohnehin schon ist. Hierzu gab es bereits einen ersten Austausch. Unter anderem wurde ich gewählt, den EDSA im European Data Innovation Board der EU-Kommission zu vertreten.

Thematisch stach in 2023 sowohl international als auch national der Umgang mit Künstlicher Intelligenz (KI) in fast allen Bereichen heraus. Die unzähligen Möglichkeiten für den Einsatz von KI in allen Wirtschafts- und Verwaltungsbereichen, aber auch die unendlichen Möglichkeiten zum Missbrauch, zur Diskriminierung bis hin zur Fälschung durch KI werden uns alle in den kommenden Jahren vor große Herausforderungen stellen. Die EU hat mit dem „Gesetz über künstliche Intelligenz" (KI-Verordnung) schon früh den Weg für eine umfassende – und notwendige – Regulation von KI vorgelegt. Ich bin sicher, dass wir auch damit einen weltweiten Standard setzen werden.

In der nationalen Beratung und Begleitung von Gesetzentwürfen nahmen 2023 vor allem die Themen Sicherheitsgesetzgebung und die Digitalisierung des Gesundheitswesens eine wichtige Rolle ein.

Dass die Sicherheitsgesetzgebung im Jahr 2023 ein wichtiger Schwerpunkt war, lag an einer Reihe von Urteilen des Bundesverfassungsgerichts (z. B. zum Bayr. Verfassungsschutzgesetz oder zur automatisierten Datenanalyse durch die Polizei), die durch Gesetzesänderungen umgesetzt werden mussten. Hinzu kommen längst überfällige Fortentwicklungen, wie etwa beim Bundespolizeigesetz und Neuregelungen in Bereich der Bekämpfung der Finanzkriminalität.

Auch wenn bei einigen der vorgelegten Gesetzentwürfe Verbesserungen im Vergleich zu den bisher geltenden Regelungen festzustellen waren, galt und gilt in den meisten Fällen: Es fehlen insbesondere Angaben zu Speicherfristen, Bestimmungen zur Zweckbindung und Kennzeichnungspflichten und damit grundsätzliche datenschutzrechtliche Anforderungen. Es ist außerdem unverständlich, dass in den Gesetzentwürfen für gleiche oder ähnlich Sachverhalte unterschiedliche Begriffe genutzt werden, was zu Verwirrung und Fehlinterpretationen führen kann.

Im Bereich des Gesundheitswesens wurde die Digitalisierung 2023 massiv angeschoben. Insbesondere die elektronische Patientenakte (ePA) und die Nutzung der Gesundheitsdaten für die Forschung standen im Mittelpunkt der Beratungen.

Wie ich schon bei der Pressekonferenz zur Vorstellung meines 31. Tätigkeitsberichtes gesagt habe, bin ich ein großer Befürworter der ePA – wenn sie sicher und nutzerfreundlich umgesetzt wird. Wir haben dazu das Bundesgesundheitsministerium und die gematik intensiv beraten (ebenso wie das BSI), sind aber nach wie vor nicht von allen getroffenen Entscheidungen überzeugt und haben alternative Lösungen vorgeschlagen.

Dass die Nutzung der Gesundheitsdaten für die Forschung von großer Bedeutung ist, wird auch von mir so gesehen. Da Gesundheitsdaten aber besonders sensibel sind, muss in jedem Fall die Einwilligung der Patientinnen und Patienten eingeholt werden oder die Daten müssen so anonymisiert oder zumindest pseudonymisiert werden, dass keine Rückverfolgung möglich ist.

Darüber hinaus haben sich meine Behörde und ich über die hier genannten Themen mit einer Vielzahl weiterer Themen, Gesetzentwürfen und Beratungs- und Kontrollbesuchen befasst, wie bereits ein Blick in das Inhaltsverzeichnis des Tätigkeitsberichtes zeigt. Die zunehmende Digitalisierung von Wirtschaft, Verwaltung und privatem Umfeld führt automatisch zum Anfall immer größerer Datenmengen, deren Verwendung geregelt werden muss. Dementsprechend erweitert sich auch das Themenspektrum meiner Behörde zusehends.

Im Jahr 2023 haben wir nicht nur auf fünf Jahre DSGVO zurückgeblickt, sondern auch auf das 45-jährige Bestehen des Bundesdatenschutzbeauftragten. Unser Aufgabenprofil hat sich in diesen Jahren enorm verändert und erheblich erweitert. Die große Zahl von (neuen) Aufgaben und Themen kann ich natürlich nicht allein bearbeiten. Ich bin deshalb sehr froh und dankbar, dass ich mich auf einen Stab von inzwischen über 320 hochmotivierten und engagierten Mitarbeiterinnen und Mitarbeitern verlassen kann. Bei diesen bedanke ich mich für die stets vertrauensvolle, manchmal auch gerne kritische, aber immer gute Zusammenarbeit.

Auch dem Deutschen Bundestag und den für meinen Einzelplan zuständigen Haushaltsberichterstattern möchte ich für die konstruktive und faire Zusammenarbeit danken, ohne die ich mein Amt nicht mit der gesetzlich vorgeschriebenen Unabhängigkeit ausüben könnte.

Prof. Ulrich Kelber

2 Empfehlungen

2.1 Zusammenfassung der Empfehlungen des 32. Tätigkeitsberichts

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 (s. Nr. 3.1.3).

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 (s. Nr. 3.2.1).

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 (s. Nr. 3.2.4)

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 (s. Nr. 3.3.5).

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 (s. Nr. 3.4.1).

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 (s. Nr. 3.4.2).

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 (s. Nr. 4.2.4).

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 (s. Nr. 5.2).

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 (s. Nr. 5.5).

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 (s. Nr. 5.8).

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 (s. Nr. 5.8).

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 (s. Nr. 6.1.1).

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) (s. Nr. 7.1).

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 (s. Nr. 7.3).

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 (s. Nr. 7.6).

Ich empfehle dem Gesetzgeber, Abhilfebefugnisse auch im Bereich der Nachrichtendienste einzuführen (s. Nr. 7.9).

Ich empfehle dem Gesetzgeber, eindeutige und umfassende Regelungen zur Zusammenarbeit der Aufsichtsorgane über die Nachrichtendienste zu schaffen (s. Nr. 7.12).

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 (s. Nr. 8.1).

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 (s. Nr. 8.2).

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 (s. Nr. 8.2).

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 (s. Nr. 8.2).

Ich empfehle der Bundesregierung, sich bei der Diskussion um eine Vorratsdatenspeicherung für eine grundrechtsschonende Balance aus Freiheit und Sicherheit einzusetzen (s. Nr. 8.3).

In Anbetracht der unmittelbar bevorstehenden Aufnahme des Regelbetriebs empfehle ich der Bundesregie-

rung, endlich eine unabhängige Registerstelle für das Implantateregister zu schaffen (s. Nr. 8.14).

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 (s. Nr. 9.2.3).

2.2 Empfehlungen des 31. Tätigkeitsberichts

	Empfehlungen des 31. Tätigkeitsberichts	Stand der Umsetzung
🟡	Ich empfehle der Bundesregierung, ein Beschäftigtendatenschutzgesetz zu erlassen, in dem etwa der Einsatz von KI im Beschäftigungskontext, die Grenzen der Verhaltens- und Leistungskontrolle sowie typische Datenverarbeitungen im Bewerbungs- und Auswahlverfahren klar geregelt werden. (31. TB Nr. 3.2.4)	Die Bundesregierung hat mit den Vorarbeiten zu einem Beschäftigtendatenschutzgesetz begonnen. Zwischenzeitlich haben die federführenden Ressorts Bundesministerium für Arbeit und Soziales (BMAS) und Bundesministerium des Innern und für Heimat (BMI) inhaltliche Vorschläge für einen modernen Beschäftigtendatenschutz vorgestellt. Bislang nicht vorgelegt wurde allerdings ein entsprechender Referentenentwurf.
🔴	Eine datenschutzkonforme Nutzung von Facebook Fanpages ist h. E. weiterhin nicht möglich. Ich empfehle daher, die Fanpages abzuschalten. (31. TB Nr. 4.3.1)	Gegen meinen Bescheid vom Februar 2023 ist mittlerweile ein Verfahren vor dem Verwaltungsgericht anhängig. Solange das Verfahren noch nicht abgeschlossen ist, halte ich meine Empfehlung weiter aufrecht: Eine datenschutzkonforme Nutzung von Facebook Fanpages ist meines Erachtens weiterhin nicht möglich. Die Fanpages sollten abgeschaltet werden.
🔴	Um den Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr rechtlich abzusichern, empfehle ich dem Gesetzgeber, eine umfassende, empirische und interdisziplinäre Bestandsaufnahme durch eine Expertenkommission durchzuführen. (31. TB Nr. 4.4.2)	Der Gesetzgeber hat meine Empfehlung aus dem 31. TB., den Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr rechtlich abzusichern und eine umfassende, empirische und interdisziplinäre Bestandsaufnahme durch eine Expertenkommission durchzuführen, bislang nicht aufgegriffen.
🟡	Ich empfehle der Bundesregierung, auf eine erhebliche, grundrechtskonforme Überarbeitung des VO-Entwurfs zur Chat-Kontrolle im Sinne des EP-Berichts von November 2023 zu drängen und ansonsten den Verordnungsentwurf insgesamt abzulehnen. (31. TB Nr. 4.4.1)	Die bisherige Empfehlung gilt weiter. Zwar hat die Bundesregierung im Rat der EU im April 2023 eine kritische Stellungnahme vorgelegt, die einige meiner Kritikpunkte aufgreift. Da eine Einigung im Rat jedoch noch aussteht und der Rat bisher nur wenige der Kritikpunkte berücksichtigt hat, halte ich an meiner Empfehlung fest. Das EU-Parlament hat im November seinen Bericht verabschiedet, der viele meiner Kritikpunkte enthält.

	Empfehlungen des 31. Tätigkeitsberichts	Stand der Umsetzung
	Ich empfehle die Einführung von Datentreuhändern auf Basis des TTDSG grundsätzlich zu überarbeiten und DSGVO-konform umzusetzen. (31. TB Nr. 5.5)	Es hat sich gezeigt, dass die Einführung von Datentreuhändern auf Basis des TTDSG nicht zielführend möglich ist. Die Rechtsgrundlage dafür sollte deshalb neu gefasst werden. Diesen Standpunkt habe ich gegenüber dem BMDV wiederholt vorgetragen. Gleichzeitig begleite ich konstruktiv die Ressortabstimmung für eine Rechtsverordnung nach § 26 Abs. 2 TTDSG. In diesem Zusammenhang haben meine Kolleginnen und Kollegen aus den Datenschutzaufsichtsbehörden der Länder und ich im Juli 2023 eine gemeinsame Stellungnahme der DSK verabschiedet.[1] In dieser Stellungnahme wird klargestellt, dass die deutschen Datenschutzaufsichtsbehörden die Einführung von „Diensten zur Einwilligungsverwaltung“ zwar grundsätzlich für einen sinnvollen Ansatz halten. Gleichzeitig wird aber auch auf die vielen Unzulänglichkeiten der aktuellen Umsetzungspläne hingewiesen.
	Ich empfehle die Zusammenlegung von Informationsfreiheitsgesetz und Umweltinformationsgesetz (und möglichst auch des Verbraucherinformationsgesetzes) sowie die Weiterentwicklung zu einem Bundestransparenzgesetz mit proaktiven Veröffentlichungspflichten. Der Informationsfreiheitsbeauftragte benötigt in einem Bundestransparenzgesetz Anordnungs- und Durchsetzungsbefugnisse, um im Konfliktfall handlungsfähig zu sein. (31. TB Nr. 6.3)	Ich werde vom federführenden Referat im BMI in die laufenden Planungen und Überlegungen für ein Bundestransparenzgesetz einbezogen, allerdings gibt es noch keinen Gesetzentwurf.
	Ich empfehle dem Gesetzgeber, die anstehende Evaluierung des Sicherheitsüberprüfungsgesetzes (SÜG) zu nutzen, um ein schlüssiges Gesamtkonzept für Personenüberprüfungen auf Bundesebene zu entwickeln. Anstelle einer ausufernden Anwendung der Öffnungsklausel auf ganze Behörden, verschiedene Überprüfungsformate außerhalb des SÜG sowie Mehrfachüberprüfungen aufgrund verschiedener Tätigkeiten sollte der Anwendungsbereich des Gesetzes neu definiert werden. (31. TB Nr. 7.10)	Ein Gesamtkonzept bzw. eine Neudefinition der sicherheitsempfindlichen Stelle war nicht Gegenstand der SÜG-Novelle und wird absehbar auch nicht in der anstehenden Gesetzesnovelle aufgegriffen.
	Ich empfehle dem Gesetzgeber weiterhin, angesichts des festgestellten geringen Nutzwertes von Antiterrordatei und Rechtsextremismusdatei, diese abzuschaffen. (31. TB Nr. 9.2.4)	Bisher keine entsprechende Planung bekannt.

1 Stellungname der DSK vom 11. Juli 2023, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/st/23-07-11_DSK-Stellungnahme_Einwilligungsverwaltung_TTDSG.pdf

	Empfehlungen des 31. Tätigkeitsberichts	Stand der Umsetzung
●	Ich empfehle dem Gesetzgeber, eine gesetzliche Klarstellung hinsichtlich der Zuständigkeit für Reservistinnen und Reservisten zwischen BAMAD und BfV vorzunehmen. (31. TB Nr. 9.2.10)	Die Bundesregierung sieht hier keinen Handlungsbedarf. Es sind daher keine Umsetzungspläne bekannt.
●	Ich empfehle, die Einbindung von Videos auf den Webseiten des Bundes zu überprüfen und datenschutzkonforme Alternativen zur weit verbreiteten Praxis der Einbindung mittels YouTube umzusetzen. (31. TB Nr. 12.2)	Die Einbindung von Videos auf den Webseiten des Bundes sollten überprüft und datenschutzkonforme Alternativen zur weit verbreiteten Praxis der Einbindung mittels YouTube umgesetzt werden. Konkrete Vorgaben sowie praktische datenschutzfreundliche Alternativen habe ich den von mir beaufsichtigten öffentlichen Stellen des Bundes mit einem Rundschreiben im Dezember 2023 aufgezeigt. Insbesondere erfolgte in dem Rundschreiben die Klarstellung, dass aktuell keine der Möglichkeiten zur Einbindung von YouTube Videos auf der eigenen Webseite als datenschutzrechtlich unbedenklich betrachtet werden kann.[2]

2 Rundschreiben an die behördlichen Datenschutzbeauftragten der obersten Bundesbehörden vom 14. Dezember 2023, abrufbar unter: www.bfdi.bund.de/rundschreiben

3 Schwerpunktthemen

3.1 Digitalisierung im Gesundheitsbereich

Im Gesundheitswesen hat es in den vergangenen Jahren einen wahren Digitalisierungsschub gegeben. Um die Digitalisierung im Gesundheitswesen und damit eine Verbesserung der Patientenversorgung und Behandlung erfolgreich umzusetzen, muss Datenschutz von Anfang an mitgedacht werden. Ein effizienter Einsatz von digitalen Angeboten ist nur dann möglich, wenn Standards zum Austausch von Daten geschaffen werden und Interoperabilität gewährleistet ist. Datenschutzkonforme Umsetzungen schaffen bei den Menschen Vertrauen in die Systeme und steigern die Akzeptanz.

Bei der Entwicklung verschiedener Projekte habe ich beraten und mich für eine datenschutzfreundliche Gestaltung eingesetzt.

3.1.1 European Health Data Space

Der Entwurf der EU-Kommission für einen „Rechtsakt über einen europäischen Raum für Gesundheitsdaten" wurde auch im vergangenen Jahr weiterentwickelt. Hierbei wurden einige datenschutzrechtlichen Forderungen berücksichtigt. Dennoch ist der European Health Data Space (EHDS) im Hinblick auf das informationelle Selbstbestimmungsrecht auch weiterhin eine Herausforderung.

Ich habe bereits im 31. Tätigkeitsbericht über den EHDS berichtet (31. TB Nr. 5.1). So sollen die Bürgerinnen und Bürger zum einen über ein digitales interoperables Format die Kontrolle über ihre Daten für ihre Gesundheitsversorgung erhalten. Zum anderen soll auch die elektronische Sekundärnutzung ihrer Gesundheitsdaten für Forschung und Innovation geregelt werden.

Schweden und Spanien haben 2023 im Rahmen ihrer Ratspräsidentschaften eigene Vorschläge zum Verordnungsentwurf vorgelegt. Diese wurden von den Vertretern der Mitgliedstaaten in einer Vielzahl von Sitzungen der Ratsarbeitsgruppe „Öffentliche Gesundheit" diskutiert und modifiziert. Das Bundesministerium für Gesundheit hat mich regelmäßig an den entsprechenden Ressortabstimmungen beteiligt, so dass ich meinen datenschutzrechtlichen Beratungsauftrag in diversen schriftlichen Äußerungen nachkommen konnte.

In einer Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 27. März 2023 spiegelt sich auch meine grundsätzliche Forderung wider, dass die Nutzung von Gesundheitsdaten des Vertrauens der Bürgerinnen und Bürger bedarf und die Rechte aus der DSGVO sowie der Charta der Grundrechte der Europäischen Union gewahrt bleiben müssen[3].

Vorbehaltlich der weiteren Verhandlungen im Europäischen Rat finden sich im aktuellen Kompromisstext der Ratspräsidentschaft Spanien aus datenschutzrechtlicher Sicht diverse Verbesserungen im Vergleich zum ursprünglichen Entwurf der Kommission. So wurden nicht nur eine Reihe von Definitionen und Regelungen in Einklang mit der DSGVO gebracht, sondern auch die Betroffenenrechte gestärkt. Auch wenn dies von verschiedenen Mitgliedstaaten und der Kommission kontrovers diskutiert wird, ist nunmehr vorgesehen, dass die Bürgerinnen und Bürger der elektronischen Verarbeitung ihrer Gesundheitsdaten sowohl in der Primär- als auch Sekundärnutzung widersprechen können. Dies begrüße ich ausdrücklich. Dennoch muss der Verordnungsentwurf insbesondere im Bereich der Governance sowie der Grundsätze der Verhältnismäßigkeit und Datenminimierung erheblich nachgeschärft werden.

3 Stellungnahme der DSK vom 27. März 2023, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf

Die zukünftige Entwicklung im Rechtsetzungsverfahren bleibt abzuwarten. Ich werde auf jeden Fall „am Ball bleiben".

3.1.2 Gesundheitsdatennutzungsgesetz

Wie im Koalitionsvertrag vereinbart, brachte die Bundesregierung in diesem Jahr ein Gesetz auf den Weg, um Gesundheitsdaten – u. a. aus der elektronischen Patientenakte, besser wissenschaftlich nutzen zu können und dies auch Unternehmen der Gesundheitswirtschaft und Pharmaindustrie zu ermöglichen.[4] Gesundheitsdaten sind besonders sensibel und werden über das Arztgeheimnis seit jeher vertraulich gehalten. Kenntnisse Dritter über Erkrankungen ermöglichen Diskriminierung und andere Nachteile. Ein Teil der vorgesehenen Regelungen greift zu weit in die Grundrechte der betroffenen Personen ein und missachtet mögliche Risiken ebenso wie das verfassungsmäßige Recht auf informationelle Selbstbestimmung.

Mit dem Entwurf eines „Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (Gesundheitsdatennutzungsgesetz – GDNG)" soll eine verbesserte Nutzung von Gesundheitsdaten ermöglicht und verschiedene weitere Regelungen insbesondere im Fünften Buch Sozialgesetzbuch (SGB V) geändert werden. Aus Datenschutzsicht besonders bedeutsam waren die folgenden Entwurfsregelungen:

Die Nutzungsberechtigung bezüglich der versichertenbezogenen Abrechnungs-Daten im Forschungsdatenzentrum Gesundheit beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) soll von dem bisherigen Katalog benannter Berechtigter auf eine Berechtigung aller Personen und Unternehmen aufgrund benannter zulässiger Zwecke umgestellt werden

- Die Krankenkassen sollen – auch ohne Einwilligung der Versicherten – eine individuelle, versichertenbezogene Auswertungsbefugnis erhalten.
- Die Gesundheitseinrichtungen, insbesondere Krankenhäuser, sollen eine bundeseinheitliche Grundlage zur Weiterverarbeitung der zu Behandlungszwecken erhobenen Daten zu weiteren Zwecken ohne Beteiligung der betroffenen Patienten erhalten.
- Im Modellvorhaben Genomsequenzierung sollen wesentliche Datenverarbeitungen ohne Einwilligung der betroffenen Personen erlaubt werden.
- Die Weiternutzung der Daten in der elektronischen Patientenakte zu verschiedenen weiteren Zwecken im Forschungsdatenzentrum Gesundheit soll nicht mehr zustimmungsbasiert, sondern automatisiert als Opt-out-Modell gestaltet werden.

Auf Basis der von der DSK in der „Petersberger Erklärung"[5] vom 23. November 2022 benannten Maßgaben für die datenschutzkonforme Nutzung von Gesundheitsdaten zu Forschungszwecken habe ich zu dem Gesetzentwurf mehrfach Stellung genommen.[6] Hinsichtlich der Kabinettfassung waren weitere Empfehlungen angezeigt, die ich mit meiner Stellungnahme[7] vom 22. September 2023 geltend gemacht habe:

- Die Strafbewehrung des Forschungsgeheimnisses – eine langjährige Forderung der DSK – wurde in § 9 GDNG-E geregelt, der wiederum auf besondere, in § 7 GDNG-E festgelegte Pflichten Bezug nimmt. Es fehlen allerdings flankierende strafprozessuale Regelungen zu Beschlagnahmeverboten und Zeugnisverweigerungsrechten. Diese sind noch zu ergänzen.
- Die vorgesehene Befugnis der Krankenkassen, bei ihnen vorliegende Daten versichertenbezogen auszuwerten und den Versicherten darauf basierend Empfehlungen zu geben, wie sie im Entwurf in § 25b SGB V-E vorgesehen wird, verstößt gegen datenschutzrechtliche Grundsätze. Sie verletzt das sozialdatenschutzrechtliche Trennungsgebot und ermöglicht den Krankenkassen die Profilbildung („gläserner Versicherter") und hat daher erhebliches Diskriminierungspotential. Es gibt zudem keinen Nachweis und keine Erfahrung dazu, ob die vorliegenden Daten nach Struktur und Validität überhaupt geeignet sind, die beabsichtigten Ergebnisse zuverlässig zu erbringen. Außerdem greift diese Auswertung in die ärztlichen Kompetenzen ein. Sie ist daher zu streichen.
- Die Änderungen beim Modellvorhaben Genomsequenzierung (§ 64e SGB V) müssen überarbeitet werden, insbesondere sollte die Verarbeitung der Genomdaten aus verfassungsrechtlichen und daten-

4 BT-Drs. 20/9046, abrufbar unter https://dserver.bundestag.de/btd/20/090/2009046.pdf
5 Petersberger Erklärung vom 24. November 2022, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf
6 Stellungnahme der DSK vom 14. August 2023, abrufbar unter: https://datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf
7 Meine Stellungnahme zum Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten vom 28. September 2023, abrufbar unter: www.bfdi.bund.de/stellungnahmen

schutzrechtlichen Gründen aufgrund der besonderen Risiken weiterhin auf die Einwilligung der betroffenen Personen gestützt werden. Durch die neuen gesetzlichen Formulierungen entfiele zudem die bisher vorgesehene Löschfrist von 30 Jahren. Die Zulässigkeit einer unbegrenzten Speicherung von Genomdaten ist in Anbetracht des Grundrechtseingriffs höchst zweifelhaft.

Nach Befassung durch den Bundesrat hat der Bundestag das Gesetz am 15. Dezember 2023. beschlossen. Meine Empfehlungen wurden dabei im Wesentlichen leider nicht berücksichtigt.

3.1.3 Beschleunigung der Digitalisierung im Gesundheitsbereich durch ein Digital-Gesetz

Der Deutsche Bundestag hat am 14. Dezember 2023 das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) beschlossen. Wichtigste Änderung ist die Einführung der widerspruchsbasierten elektronischen Patientenakte (ePA) für alle gesetzlich Versicherten. Zu den Vorschriften bestehen einige datenschutzrechtliche Bedenken.

Nach dem Kabinettbeschluss vom 30. August 2023 wurde von der Bundesregierung das DigiG in das parlamentarische Verfahren eingebracht. Die erste Lesung des Gesetzentwurfs hat im Deutschen Bundestag am 9. November 2023 stattgefunden. Der Deutsche Bundestag hat das Gesetz am 14. Dezember 2023 beschlossen. Am 2. Februar 2024 wird es in zweiter Sitzung im Bundesrat behandelt. Mit Verkündung und Inkrafttreten kann ab Mitte Februar 2024 gerechnet werden. Mit dem Gesetzentwurf soll die digitale Transformation des Gesundheitswesens und der Pflege beschleunigt vorangetrieben werden. Insbesondere sollen mit dem Gesetzentwurf die Potenziale der ePA durch die Umwandlung in eine Widerspruchslösung für alle 74 Mio. gesetzlich Versicherten sowie die Cybersicherheit erhöht werden. Darüber hinaus sollen verschiedene weitere Regelungen insbesondere im Fünften Buch Sozialgesetzbuch geändert werden.

Die Digitalisierung des Gesundheitswesens und der Pflege begrüße ich. Es besteht unbestritten Nachholbedarf. Allerdings muss die Digitalisierung datenschutzkonform erfolgen.

Maßgebliches Instrument für die Digitalisierung des Gesundheitswesens soll nach dem Willen des Gesetzgebers die ePA sein, die den gesetzlich Versicherten überhaupt erst seit dem 1. Januar 2021 zur Verfügung steht. Da der Nutzungsumfang der aktuellen ePA, die auf der Einwilligung der Versicherten basiert, sehr gering ist, soll durch einen Paradigmenwechsel hin zu einer widerspruchsbasierten ePA die Verbreitung und Nutzungsquantität erhöht werden. Dieser Paradigmenwechsel greift erheblich in das Grundrecht auf die informationelle Selbstbestimmung ein. Denn die Gesundheitsdaten der Bürgerinnen und Bürger genießen nach europäischem als auch deutschem Recht besonderen Schutz. Durch die Zusammenführung von bislang bei den Behandlern liegenden Daten entsteht neben der Primärdokumentation bei diesen ein umfassender zusätzlicher Datenbestand, der die Informationen über den Gesundheitszustand der Versicherten in bisher nicht bekannten Ausmaß erschließt und mit den weiteren Planungen die Erstellung eines nahezu vollständigen Gesundheitsprofils ermöglicht, ein Profil mit besonders schutzwürdigen Daten aus der informationellen Intimsphäre der Versicherten.

Bezüglich der geplanten Ausgestaltung der widerspruchbasierten ePA habe ich erhebliche datenschutzrechtliche Bedenken. Der Gesetzentwurf sieht vor, dass allen gesetzlich Versicherten eine elektronische Patientenakte bereitgestellt wird, Behandler auf die ePA zugreifen können und Behandler verpflichtet sind, die ePA mit Informationen zu befüllen, sofern die Versicherten nicht widersprochen haben. Ein Einwilligungsvorbehalt ist nach dem Gesetzentwurf nur für die Befüllung mit Daten aus genetischen Untersuchungen oder Analysen im Sinne des Gendiagnostikgesetzes vorgesehen. Eine meiner Forderungen ist, auch besonders schutzwürdige, höchstpersönliche Daten aus der informationellen Intimsphäre der Versicherten von der Pflichtbefüllung auszunehmen und unter einen Einwilligungsvorbehalt zu stellen. Dies gilt insbesondere für Daten, deren Bekanntwerden zu erheblichen Gefährdungen für die Rechte der Versicherten führen, etwa, weil sie Anlass zu Diskriminierung oder Stigmatisierung geben können, darunter Daten zu HIV-Infektionen, Schwangerschaftsabbrüchen oder psychischen Erkrankungen.

Weiterhin fordere ich, die widerspruchsbasierte Pflichtbefüllung der ePA durch die Behandler nach dem Grundsatz der Verhältnismäßigkeit auf ein notwendiges, dem gesetzlichen Zweck der ePA entsprechendes Mindestmaß zu beschränken. Es darf keine ungeregelte Befüllungserlaubnis für die Behandler geben. Es bestehen Zweifel an der Erforderlichkeit der Befüllung, wenn diese ins Belieben der Behandler gestellt wird.

Darüber hinaus hatte ich während des parlamentarischen Verfahrens kritisiert, dass im Gesetzentwurf datenschutzrechtlich bedeutsame Vorgaben zur Gewährleistung der Betroffenenrechte nach der DSGVO, zu Speicherfristen der ePA an sich sowie deren Inhalte und zu Sonderregelungen für selbst entscheidungsfähige Minderjährige fehlen. Zu den Regelungen für Minderjährige konnte ich letztlich Verbesserungen erreichen. Auch konnte ich den Gesetzgeber davon überzeugen,

Versicherten ohne eigenen Smartphone-Zugang zur ePA eine Möglichkeit zu geben ihre Betroffenenrechte auszuüben. Dazu sollen Ombudsstellen eingerichtet werden, an die Versicherte sich wenden können, um Einblick in ihre ePA zu erlangen. Leider überträgt der Gesetzentwurf entgegen meines ausdrücklichen Rats die Aufgabe der Einrichtung dieser Stellen den Krankenkassen. Nach dem Gebot, dass Krankenkassen keine Gesundheitsdaten verarbeiten sollen, sollten die Ombudsstellen von den Krankenkassen getrennt sein.

Eine weitere wichtige Leitplanke sehe ich in der Gewährleistung der Datensicherheit der im Gesundheitsbereich zu verarbeitenden sehr sensiblen personenbezogenen Daten. Leider lässt der Gesetzentwurf im Gegensatz zu seiner Intention eine Abschwächung der Cybersicherheit erkennen, wenn niedrigschwellige Sicherheitsniveaus im Regelfall und nicht nur in absoluten Ausnahmefällen zugelassen werden sollen, ohne dadurch auch nur zusätzliche Funktionalität oder einfachere Bedienung zu erreichen. Auch sollen durch die Umwandlung der Regelung zum Einvernehmen in ein Benehmen berechtigte Einwände von ausgewiesenen Experten für IT-Sicherheit und Datenschutz keine zwingende Berücksichtigung mehr finden. Dies gilt verstärkt mit Blick auf die Planungen zum ausgeweiteten Einsatz der sogenannten digitalen Identitäten als Zugangsmittel zu Gesundheitsdiensten aller Art – auch über die Telematikinfrastruktur hinaus. Darüber hinaus ist eine wesentliche Bedingung für die Gewährleistung der Datensicherheit, dass alle elektronischen Gesundheitskarten sicher zugestellt werden oder die Besitzer sich sicher nachidentifizieren, bevor sie als Teilzugangsmittel auch ohne Nutzung einer PIN – bspw. zum Nachweis des Behandlungskontexts – genutzt werden. Hierzu sehe ich dringenden Regelungsbedarf. Diesen Regelungsbedarf und meine datenschutzrechtlichen Bedenken zum Entwurf des DigiG habe ich detailliert gegenüber den Parlamentariern sowohl durch Beratungen im Vorfeld als durch umfangreiche Stellungnahmen[8] im parlamentarischen Verfahren geäußert.

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.

3.1.4 Widersprüche gegen opt-out-Regelung der elektronischen Patientenakte im Vorfeld

Bürgerinnen und Bürger haben sich im vergangenen Jahr vermehrt mit der Frage an mich gewendet, ob sie der Anlage einer elektronischen Patientenakte (ePA) widersprechen können. Oftmals wurden die Widersprüche auch unmittelbar an mich adressiert.

Unter der bisherigen Rechtslage war die ePA gemäß § 341 Abs. 1 SGB V eine versichertengeführte elektronische Akte, die den Versicherten von den Krankenkassen auf Antrag zur Verfügung gestellt wird. Das Antragserfordernis sollte sicherstellen, dass die Nutzung für die Versicherten freiwillig ist. Bürgerinnen und Bürger, die eine ePA nutzen wollten, mussten diese aktiv bei ihrer Krankenkasse beantragen und ihr ausdrückliches Einverständnis abgeben („Opt-in“). Ein Widerspruch gegen Anlage und Nutzung der ePA war nicht erforderlich.

Zwischenzeitlich hat der Deutsche Bundestag das Digital-Gesetz (DigiG) verabschiedet. Das Gesetz sieht unter anderem vor, dass die ePA Anfang des Jahres 2025 für alle gesetzlich Versicherten auch ohne deren ausdrückliches Einverständnis eingerichtet wird. Wer die ePA nicht nutzen möchte, kann dem widersprechen („Opt-Out“). Bevor Krankenkassen eine ePA für ihre Versicherten anlegen, müssen sie diese entsprechend informieren und Gelegenheit zum Widerspruch geben (§ 343 Abs. 1a, § 344 Abs. 1 SGB V).

Schon jetzt kontaktieren mich täglich Bürgerinnen und Bürger, die besorgt um ihre Daten sind und der Anlegung einer ePA zuvorkommen möchten. Zwischen den Zeilen nehme ich ein Stück weit Verunsicherung, Ohnmacht und Misstrauen wahr. Beigetragen haben dürfte aus meiner Sicht, dass bei Einführung der ePA vor dem Hintergrund des Selbstbestimmungsrechts der Versicherten und der Patientensouveränität davon gesprochen wurde, dass Verarbeitungen nur auf Basis von Einwilligungen erfolgen würden,[9] nur um jetzt – weniger als vier Jahre später – eine Verarbeitung auch ohne Einwilligung zu ermöglichen.

Gleichwohl rate ich betroffenen Personen davon ab, den Widerspruch gegen die ePA bereits jetzt vorbeugend zu erklären. Das betreffende Gesetz ist gerade erst verabschiedet und die Krankenkassen müssen die gesetzlichen Vorgaben – darunter die Einrichtung einer Ombudsstelle für Anliegen im Zusammenhang mit der ePA (§ 342a SGB V) erst nach und nach umsetzen. Ein Widerspruch zum gegenwärtigen Zeitpunkt, solange

8 Stellungnahme vom 26. September 2023 und Zentrale Forderungen vom 26. September 2023, abrufbar unter: www.bfdi.bund.de/stellungnahmen
9 BT-Drucksache 19/18793, S. 114

dafür keine offiziellen Kommunikationskanäle bei den Krankenkassen eingerichtet sind, erschwert sowohl den Versicherten als auch den Krankenkassen die Bearbeitung. Betroffene Personen sollten sich noch etwas gedulden. Wie geschildert, werden die Krankenkassen informieren, wie der Widerspruch erklärt werden kann. Auch hat der Gesetzgeber eine Widerspruchsmöglichkeit per App vorgesehen (§ 344 Abs. 3 Satz 2 Var. 2 SGB V), die die Krankenkassen erst noch schaffen müssen und wozu sie ebenfalls noch informieren werden.

Hinweisen möchte ich aber darauf, dass der Widerspruch nicht gegenüber meiner Behörde erklärt werden und ich derartige Widersprüche auch nicht weiterleiten kann. Sofern betroffene Personen die Sorge haben, dass ihre Krankenkasse ihren Widerspruch nicht bearbeitet, hilft es nicht, mich bei der Widerspruchsmail in Kopie zu setzen. Ein Nachweis, dass der Widerspruch der Krankenkasse zugegangen ist, kann auf diese Weise nicht geführt werden.

Querverweise:

3.1.3 Beschleunigung der Digitalisierung im Gesundheitsbereich durch ein Digital-Gesetz

3.1.5 Pflegeunterstützungs- und Entlastungsgesetz – Beitragsentlastung für Eltern in der sozialen Pflegeversicherung

Mit dem Pflegeunterstützungs- und Entlastungsgesetz sollen Eltern, die Mitglied in der sozialen Pflegeversicherung sind, beitragsrechtlich entlastet werden. Die Umsetzung gestaltet sich schwieriger als erwartet.

Zum 1. Juli 2023 ist das Pflegeunterstützungs- und -entlastungsgesetz (PUEG) in Kraft getreten. Mit diesem Gesetz wurde unter anderem auch der Beschluss des Bundesverfassungsgerichts[10] umgesetzt, indem der Erziehungsaufwand von Eltern im Beitragsrecht der sozialen Pflegeversicherung berücksichtigt wird. So wird der Beitragszuschlag für Mitglieder ohne Kinder um 0,25 Beitragssatzpunkte auf 0,6 Beitragssatzpunkte angehoben. Mitglieder mit mehreren Kindern werden ab dem zweiten bis zum fünften Kind mit einem Abschlag in Höhe von 0,25 Beitragssatzpunkten für jedes Kind entlastet. Zur Sicherstellung einer einheitlichen Rechtsanwendung sowie zur Gewährleistung eines möglichst effizienten, schnellen und bürgerfreundlichen Verwaltungshandelns sieht § 55 Abs. 3c SGB XI die Verpflichtung des Bundes vor, bis zum 31. März 2025 ein digitales Verfahren zur Erhebung und zum Nachweis der Anzahl der berücksichtigungsfähigen Kinder zu entwickeln.

Die Entwicklung eines derartigen Verfahrens stellte sich als äußerst komplex dar. So galt es zunächst, die erforderliche Datengrundlage (elektronische Lohnsteuerabzugsmerkmale = ELStAM-Datenbank) und die an der Durchführung des Verfahrens beteiligten Stellen (Träger der sozialen Pflegeversicherung, Arbeitgebende als beitragsabführende Stellen, die Datenstelle der Rentenversicherung (DSRV) als Dienstleister bei der Deutschen Rentenversicherung (DRV) Bund, die Zentrale Zulagenstelle für Altersvermögen (ZfA) bei der DRV Bund als zentrale Stelle nach § 81 EStG sowie das Bundeszentralamt für Steuern (BZSt) mit dem Verfahren ELStAM) zu identifizieren. Bei der Erarbeitung der für die Flankierung des Verfahrens erforderlichen gesetzlichen Regelungen habe ich die beteiligten Ressorts beraten und dabei insbesondere auf die datenschutzrechtliche Notwendigkeit der Beachtung des Wesentlichkeitsgebots hingewiesen, wonach der Gesetzgeber ausdrücklich Art, Umfang und Zweck der einzelnen Datenverarbeitungen regeln muss. Außerdem sind Maßnahmen gemäß Art. 32 DSGVO zur Gewährleistung eines technisch sicheren Verfahrens zu treffen sowie die besondere Sensibilität im Hinblick auf die Nutzung der Steuer-Identifikationsnummer (Steuer-ID) zu beachten.

Die Regelungen wurden über das Gesetz zur Stärkung von Wachstumschancen, Investitionen und Innovation sowie Steuervereinfachung und Steuerfairness (Wachstumschancengesetz) in das Gesetzgebungsverfahren eingebracht. Nach Verabschiedung des Gesetzentwurfs durch den Bundestag am 17. November 2023 hat der Bundesrat am 24. November 2023 den Vermittlungsausschuss angerufen. Ein Termin für die Behandlung des Gesetzes im Vermittlungsausschuss steht bislang noch nicht fest.

3.2 Künstliche Intelligenz

Künstliche Intelligenz (KI) ist eine Schlüsseltechnologie, die beeindruckende Möglichkeiten eröffnet. Grundlage der meisten KI-Anwendungen ist ein großer Datenhunger, der nahezu alle Lebensbereiche berührt – einschließlich sehr sensibler Gebiete wie etwa der Gesundheit. Ohne Vertrauen in die Integrität der Technologie und die Wahrung der persönlichen Daten wird eine nachhaltige KI-Entwicklung schwer zu erreichen sein. Es ist deshalb eine zentrale gesamtgesellschaftliche und politische Aufgabe, KI so zu gestalten, dass sie den Men-

10 Beschluss des Ersten Senats des Bundesverfassungsgerichts vom 7. April 2022, Az: 1 BvL 3/18

schen und seine Rechte in den Mittelpunkt stellt und dabei gleichzeitig innovative Entwicklungen und einen breiten Einsatz in vielen Bereichen ermöglicht. Der Datenschutz leistet dazu einen wichtigen Beitrag.

Die öffentlichkeitswirksamen Entwicklungen rund um ChatGPT haben es im vergangenen Jahr gezeigt: Das Tempo, mit dem innerhalb weniger Monate zahllose KI-basierte Innovationen an den Start gegangen sind, hat große Hoffnungen geweckt, aber auch große Ängste ausgelöst. Dass KI tiefgreifende Auswirkungen auf die Gesellschaft haben kann, steht außer Frage. KI-Systeme können bemerkenswert positive Auswirkungen auf unsere Lebensqualität haben, sie können aber auch Freiheiten und Rechte von Bürgerinnen und Bürgern stark beeinträchtigen. Denn die zahlreichen Vorteile basieren in der Regel auf der Auswertung von großen, oft auch personenbezogenen Datenmengen. Je nachdem, wie KI eingesetzt wird, birgt sie damit das Potential für Grundrechtseinschränkungen und Diskriminierungen. Ein hohes Maß an Transparenz und Nachvollziehbarkeit der Ergebnisse und der Prozesse maschinengesteuerter Entscheidungen, der Grundsatz der Datenminimierung, die Einhaltung der Zweckbindung, aber auch die Vermeidung von Diskriminierungen und die klare Zurechnung von Verantwortlichkeiten sind daher Grundsätze, die die Technologiegestaltung begleiten müssen.

Im Rahmen meiner Aufsichts- und Beratungsfunktion bildet dieses Thema aktuell einen Schwerpunkt der Arbeiten meines Hauses. Sei es im Rahmen der klassischen Kontrolltätigkeit, die immer häufiger durch KI-Anwendungen geprägt ist, deren datenschutzkonformer Einsatz sichergestellt werden muss oder als Akteur bei der Gestaltung rechtlicher und gesellschaftlicher Rahmenbedingungen, wenn es etwa um neue Regulierungsansätze oder um gesellschaftliche Debatten geht, die sich mit der Anwendung von KI und den Auswirkungen auf unser aller Zusammenleben auseinandersetzen. Auch die Beratung der Stellen unter unserer datenschutzrechtlichen Aufsicht für deren Einsatz von KI-Systemen ist eine wichtige Aufgabe für meine Behörde.

Datenschutz und Privatsphäre sind Kernelemente, ohne die der sichere Einsatz von KI nicht denkbar ist und durch die Forschung, Anwendung, Auswertung und Regulierung in diesem Bereich zentral geprägt sein müssen.

3.2.1 KI-Verordnung

In der Europäischen Union wird im Trilog über eine Verordnung zur Regulierung von Künstlicher Intelligenz (KI) verhandelt. Die Verordnung soll ein hohes Schutzniveau für die Gesundheit, Sicherheit und Grundrechte der Bürger sicherstellen. Gleichzeitig soll durch sie Innovation im Bereich KI gefördert werden. Dabei ist es wichtig, die Grundsätze der DSGVO zu berücksichtigen.

Die EU-Kommission hat am 21. April 2021 einen Entwurf für eine EU-Verordnung zur Regulierung Künstlicher Intelligenz (KI-Verordnung) oder auch Artificial Intelligence Act (AI Act) vorgelegt. Der EU-Rat hat am 6. Dezember 2022 seinen Kompromissvorschlag angenommen. Im Berichtsjahr hat am 14. Juni 2023 das EU-Parlament seinen Kompromissvorschlag verabschiedet. Aktuell verhandeln die EU-Kommission, der EU-Rat und das EU-Parlament basierend auf diesen Vorschlägen im Trilog die KI-Verordnung. Ich begleite diese Entwicklungen auf europäischer und nationaler Ebene. Über die finale Ausgestaltung der KI-Verordnung wird voraussichtlich Anfang 2024 entschieden.

Der Einsatz von KI-Systemen verspricht in vielen Bereichen einen hohen Nutzen, gleichzeitig nehmen jedoch mit zunehmender Verbreitung von KI-Systemen die Befürchtungen über Intransparenz, Diskriminierung und Missbrauch dieser Technologie zu. Da eine sinnvolle Balance zwischen den potenziellen Gefahren durch KI-Systeme auf der einen und unnötig innovationshemmender Bürokratie auf der anderen Seite gefunden werden muss, sind die Diskussionen über die Details der KI-Verordnung erwartungsgemäß langwierig. Aufgrund der hohen gesellschaftlichen Relevanz wird die KI-Verordnung nicht nur vom Gesetzgeber, sondern auch von Wirtschaft und Zivilgesellschaft kontrovers diskutiert.

Ein risikobasierter Ansatz soll menschenzentrierte und vertrauenswürdige KI fördern und einen hohen Schutz der Gesundheit, Sicherheit und Grundrechte gewährleisten, während gleichzeitig Innovation unterstützt wird. Dabei werden KI-Systeme in vier Risikostufen eingeteilt: minimal, begrenzt, hoch und inakzeptabel. Das entspricht dem Vorschlag, den die deutsche Datenethik-Kommission 2019 unter meiner Beteiligung gemacht hatte.[11] Anwendungen mit minimalem Risiko werden von der KI-Verordnung nicht berührt. Auch für Anwendungen mit begrenztem Risiko werden lediglich Transparenzvorgaben gemacht. Für Anwendungen, die mit einem hohen Risiko einhergehen, werden dagegen

11 Gutachten der Datenethikkommission, abrufbar unter: www.bfdi.bund.de/dek

umfangreichere Vorgaben gemacht, beispielsweise Qualitätsanforderungen an verwendete Datensätze. Dokumentations- und Protokollierungsvorgaben bis hin zu vorgeschriebener menschlicher Aufsicht und Kontrolle der Anwendung dieser KI-Systeme sollen die Sicherheit über den gesamten Lebenszyklus eines Hochrisiko-KI-Systems hinweg sicherstellen. Anwendungen mit inakzeptablem Risiko sind verboten.

Die Aushandlung der Details der KI-Verordnung gestaltet sich erwartungsgemäß schwierig. Politisch besonders kontrovers diskutiert werden ein Verbot biometrischer Fernidentifizierung im öffentlichen Raum in Echtzeit sowie des Einsatzes von KI durch die Polizei zur Vorhersage potenzieller Straftaten („Predictive Policing"). Ich habe mich bereits in der gemeinsamen Stellungnahme des Europäischen Datenschutzausschusses (EDSA) und des Europäischen Datenschutzbeauftragten (EDSB) in 2021 für ein Verbot der Verwendung von KI zur automatischen Erkennung personenbezogener Merkmale in öffentlich zugänglichen Räumen ausgesprochen. Zudem setze ich mich nachdrücklich für ein Verbot der Nutzung von KI für vorhersagende Polizeiarbeit ein. Ich begrüße, dass in dem Kompromissvorschlag des EU-Parlaments diverse Veränderungen enthalten sind, die ich mit meinen europäischen Kolleginnen und Kollegen in der Stellungnahme aus 2021 gefordert habe, unter anderem die obigen Verbote sowie ein Verbot der Nutzung von KI zur Bewertung sozialen Verhaltens („Social Scoring").

Inwiefern generative KI-Systeme letztlich von der KI-Verordnung betroffen sein werden, wird noch verhandelt. Insbesondere in Anbetracht der großen Datenmengen, die bei der Entwicklung solcher KI-Systeme benötigt werden und die auch personenbezogene Daten beinhalten, setze ich mich unermüdlich für die datenschutzkonforme Entwicklung dieser Modelle ein. Dem Datenschutz kommt bei der Entwicklung und Anwendung von KI-Systemen eine herausragende Bedeutung zu, weshalb er über den gesamten Lebenszyklus von KI-Systemen hinweg mitberücksichtigt werden muss.

Die Anwendung und Umsetzung der KI-Verordnung sollen von nationalen KI-Aufsichtsbehörden und Marktüberwachungsbehörden beaufsichtigt werden. Als nationale KI-Aufsichtsbehörden in Deutschland bieten sich die Datenschutzbehörden an. Grundsätzlich haben viele der Hochrisiko-KI-Systeme einen engen Bezug zum Datenschutz. Auch viele der Vorgaben in der KI-Verordnung komplementieren die Vorgaben aus der DSGVO. Der EDSA arbeitet aktuell an Leitlinien zum Zusammenspiel der DSGVO mit der KI-Verordnung und anderen potenziell relevanten Rechtsgrundlagen, woran ich für die deutschen Datenschutzaufsichtsbehörden intensiv beteiligt bin. Datenschutzaufsichtsbehörden haben wegen ihrer Zuständigkeit für die Datenschutzaufsicht über KI-Systeme bereits eine große Expertise in diesem Bereich. Somit bieten sie sich auch für die KI-Aufsicht in vielen der von der KI-Verordnung umfassten Bereiche an und könnten die Aufgaben der in der KI-Verordnung vorgesehenen Marktüberwachungsbehörden übernehmen. Das reduziert den Aufwand für kontrollierte Stellen und bietet den Bürgerinnen und Bürgern einen einheitlichen Ansprechpartner bei Beschwerden oder Auskunftswünschen.

Ich empfehle dem Gesetzgeber, die sich aus der KI-Verordnung der EU ergebende nationale KI-Aufsichtsstruktur zeitnah festzulegen und dabei die 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.

3.2.2 Nationale und internationale Zusammenarbeit zum Thema Künstliche Intelligenz

Die Entwicklung von auf Künstliche Intelligenz (KI) gestützten Verfahren schreitet mit hoher Dynamik voran. Neue Techniken werden heute schneller als je zuvor international verfügbar. Um unter diesen Rahmenbedingungen eine effektive Datenschutzpraxis zu ermöglichen, arbeitet mein Haus intensiv mit den Datenschutzaufsichtsbehörden der Länder sowie auf europäischer und internationaler Ebene zusammen. Hier konnten im Berichtszeitraum klare Positionierungen erreicht und bedeutende Resolutionen verabschiedet werden.

KI-Verfahren stellen mächtige Bausteine zur Lösung technischer Probleme dar, deren Einsatz bislang jedoch ein umfassendes Expertenwissen erforderte und die daher abseits interessierter gesellschaftlicher Gruppen verhältnismäßig wenig Beachtung fanden. Spätestens seit im November 2022 der Dienst ChatGPT vorgestellt und direkt für jedermann zugreifbar wurde, ist KI und insbesondere generative KI aber im Zentrum des gesellschaftlichen Diskurses angekommen. Um den Belangen des Datenschutzes auch in diesem hochdynamischen Umfeld Rechnung zu tragen und den Grundrechten und Grundfreiheiten der betroffenen Personen angemessenes Gewicht zu verleihen, beteiligt sich mein Haus intensiv an der Arbeit in den nationalen und internationalen Datenschutzgremien.

In der deutschen Datenschutzkonferenz (DSK) untersucht die Task Force KI des AK Technik die Datenschutzfragen, die im Zusammenhang mit KI-Systemen auf-

kommen. Die Task Force, in der meine Mitarbeitenden gemeinsam mit den Datenschutzaufsichtsbehörden der Länder bereits 2019 die Hambacher Erklärung zur Künstlichen Intelligenz und ein flankierendes Positionspapier mit empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen erarbeitet haben, setzt sich derzeit intensiv mit Fragestellungen generativer KI-Verfahren auseinander. Darüber hinaus ist die Task Force mit einer Analyse möglicher künftiger Zuständigkeiten aus dem kommenden AI Act der EU beauftragt. Zur 106. DSK im November des Berichtszeitraumes wurde ein entsprechender Sachstandsbericht vorgelegt. Im Ergebnis bin ich überzeugt, dass die Datenschutzaufsichtsbehörden fachlich und strukturell gut geeignet sind, um die KI-Aufsicht in vielen Bereichen zu übernehmen. Auch in anderen Mitgliedsstaaten sind die Datenschutzaufsichtsbehörden für die KI-Aufsicht vorgesehen, insbesondere die CNIL in Frankreich. In Deutschland ist stets der Föderalismus zu berücksichtigen, denn bei einem so bedeutenden Thema sollte es keine Zersplitterung der Aufsicht geben. Meine Behörde bietet sich als nationale KI-Aufsichtsbehörde an, auch da bereits umfangreiche Erfahrung in der Zusammenarbeit mit anderen nationalen Behörden, aber auch auf EU-Ebene vorhanden ist.

Auf europäischer Ebene hat sich mein Haus in der Gremienarbeit ebenfalls intensiv mit Aspekten der generativen KI und hier spezifisch mit den Details des Dienstes ChatGPT auseinandergesetzt. OpenAI, der Betreiber von ChatGPT, verfügt über keine Niederlassung in der EU, weshalb der One-Stop-Shop-Mechanismus der DSGVO nicht greift. Das bedeutet, dass alle europäischen Datenschutzaufsichtsbehörden in ihrem jeweiligen Bereich selbst für die Datenschutzkontrolle des Dienstes zuständig sind. Nachdem die italienische Datenschutzaufsichtsbehörde dem Dienst bis zur Klärung wichtiger Kernfragen in ihrem Zuständigkeitsbereich den Betrieb untersagt hat, hat der Europäische Datenschutzausschuss (EDSA) in seiner Technology Expert Subgroup die Task Force ChatGPT eingerichtet, um das weitere Vorgehen bei der Untersuchung zu harmonisieren, sich über Erkenntnisse auszutauschen und die datenschutzrechtliche Bewertung des Dienstes mit konsolidierten Kräften voranzutreiben. Dieses breite Vorgehen ist also schon deswegen richtig und wichtig, um eine kohärente Anwendung der DSGVO zu gewährleisten. Derzeit erarbeiten meine Mitarbeitenden in der Task Force ChatGPT einen Bericht über Ergebnisse der Untersuchungen, welcher im ersten Quartal 2024 veröffentlicht werden soll.

Im internationalen Gremienbereich konnten meine Mitarbeitenden ebenfalls wichtige Beiträge zu Datenschutzfragen bei generativer KI platzieren. Der G7 DPA Roundtable der Datenschutz- und Privacy-Behörden, dem neben meinem Haus auch die Datenschutzaufsichtsbehörden der G7-Staaten Frankreich, Italien, Japan, Kanada, UK, und die USA sowie der EDSA und der Europäische Datenschutzbeauftragte angehören, hat sein „Statement on Generative AI“ vorgelegt. In diesem werden grundlegende datenschutzrechtliche und -technische Anforderungen an generative KI-Systeme niedergelegt und noch einmal bekräftigt, dass bestehende Datenschutzgesetzgebung auch für die Verarbeitung von personenbezogenen Daten bei Entwicklung, Training und Betrieb von generativen KI-Verfahren anwendbar ist. Darüber hinaus wurde die Bedeutung von Transparenzanforderungen, Betroffenenrechten und Datenminimierung hervorgehoben. Das im Juni verabschiedete Papier ist auf meiner Website zu finden.[12]

Auch in der Global Privacy Assembly (GPA), einem Gremium, dem derzeit mehr als 130 Datenschutzbehörden aus aller Welt angehören, haben meine Mitarbeitenden an einer Resolution zu Generativen KI-Systemen mitgearbeitet. Ich werte es als besonderen Erfolg, dass das Papier auf der 45. Jahresversammlung der GPA durch 20 Sponsor- und Co-Sponsorships (Unterstützer) eingebracht und mit breiter, weit über die EU hinausgehender internationaler Zustimmung beschlossen werden konnte.[13] Die Resolution zeigt dabei auf, wie Datenschutzgrundsätze und hieraus abgeleitete Konzepte, wie sie auch in der DSGVO niedergeschrieben sind, im Kontext generativer KI-Systeme umgesetzt werden sollten. Hierunter fallen die Notwendigkeit des Vorliegens geeigneter Rechtsgrundlagen in allen Lebenszyklusphasen des Systems, Zweckbindung, Datenminimierung, Richtigkeit, Transparenz, Sicherheit, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung, Betroffenenrechte und Verantwortlichkeit. Ich schließe mich dem dort verfassten Appell an Entwickler, Vertreiber und Verwender generativer KI-Systeme an, diese Grundsätze zu verstehen und zu beachten und so weltweit einen die Grund- und Menschenrechte achtenden Umgang mit dieser vielversprechenden Technologie zu etablieren.

Neben generativer KI, die den öffentlichen Diskurs im Berichtszeitraum klar dominiert hat, existieren viele weitere in der Entwicklung befindliche oder bereits etablierte KI-Verfahren. Wie umfassend diese Verfahren

12 Statement des G7-Roundtable zu generativer KI vom 21. Juni 2023, abrufbar unter: www.bfdi.bund.de/g7-en
13 Resolution der GPA zu generativer KI vom 20. Oktober 2023, abrufbar unter: www.bfdi.bund.de/gpa-en

auch im Geschäftsbereich der Bundesregierung zunehmend Anwendung finden, geht etwa aus der Antwort der Bundesregierung auf eine kleine Anfrage zu diesem Thema hervor.[14] Ein wichtiger Baustein, alle Typen von KI-Anwendungen zu regulieren, ist dabei der AI Act, der 2023 in die Trilogphase des Gesetzgebungsprozesses eingetreten ist. Auch vor Beschluss des AI Act und dessen Inkrafttreten ist dabei schon jetzt klar: Meine Behörde wird auch weiterhin für Datenschutzfragen bei KI-Anwendungen zuständig sein, genau wie alle weiteren Datenschutzaufsichtsbehörden für ihren Bereich es ebenfalls sein werden. Um mögliche Unklarheiten, die sich im Zusammenspiel von DSGVO und AI Act ergeben, frühzeitig zu adressieren, erarbeiten meine Mitarbeitenden derzeit zusammen mit weiteren deutschen und europäischen Datenschutzaufsichtsbehörden unter Mandat des EDSA entsprechende Leitlinien. Diese werden Verantwortlichen rechtzeitig eine Orientierungshilfe an der Schnittstelle zwischen beiden Rechtsakten geben, wenn es z. B. um Fragen zur Transparenz, automatischer Entscheidungsunterstützung oder Reallaboren (Regulatory Sandboxes) geht.

Querverweise:

3.2.1 KI-Verordnung, 4.3.2 45. GPA Jahreskonferenz, 4.5.1 G7 DPA Roundtable

3.2.3 GPA-Resolution zu KI und Arbeit

Auf globaler Ebene sind datenschutzrechtliche Leitplanken auch für die Entwicklung und den Einsatz von Künstlicher Intelligenz (KI) im Beschäftigungskontext wichtig. Die Global Privacy Assembly (GPA) hat auf ihrer 45. Sitzung im Oktober 2023 eine Resolution zu Künstlicher Intelligenz und Arbeit beschlossen (Resolution on Artificial Intelligence and Employment).

Die Resolution zu Künstlicher Intelligenz im Beschäftigungskontext,[15] die von der englischen Datenschutzbehörde Information Commissioner's Office (ICO), der italienischen Datenschutzbehörde (Garante per la protezione dei Dati Personali – GPDP) und von mir eingebracht und von zahlreichen Co-Sponsoren unterstützt wurde, basiert auf einer Umfrage zu KI im Beschäftigungskontext, die im Jahr 2022 unter den Mitgliedern der GPA durchgeführt wurde. Der Bericht zu dieser Umfrage ist der Resolution als Annex beigefügt.

Die Resolution unterstreicht die Notwendigkeit der Kooperation auf internationaler Ebene und stellt Grundsätze und Erwägungen hinsichtlich der Entwicklung und des Einsatzes Künstlicher Intelligenz in einem weit verstandenen Beschäftigungskontext zusammen. Umfasst sind beispielsweise die Bewerbungsphase, das Home Office oder auch neue Beschäftigungsformen wie das sogenannte „Gig-Working", das heißt, die meist über digitale Plattformen erfolgende Vermittlung kleinerer Arbeitsaufträge an Solo-Selbstständige, womit ein breiter persönlicher und sachlicher Anwendungsbereich der Resolution einhergeht.

Erwägungen, die der Resolution zufolge bei der Entwicklung und dem Einsatz von KI im Beschäftigungskontext eine Rolle spielen sollen, sind etwa die Vorgabe, dass in allen Phasen des KI-Lebenszyklus Verarbeitungen personenbezogener Daten die Anforderungen geltender Datenschutzgesetze und Datenschutzprinzipien berücksichtigen. Wichtig ist der Resolution zufolge auch, dass es hinreichende Rechtsgrundlagen für alle Verarbeitungen personenbezogener Daten bei KI im Beschäftigungskontext gibt. An erster Stelle verweist die Resolution darauf, dass der Einsatz von KI im Beschäftigungskon-

14 siehe Bundestags-Drucksachen 20/6862 und 20/6401

15 Resolution zu Künstlicher Intelligenz im Beschäftigungskontext, abrufbar unter: https://globalprivacyassembly.org/wp-content/uploads/2023/10/1.-Resolution-on-AI-and-employment-1.pdf

text menschenzentriert sein muss. Als weitere tragende Grundsätze werden unter anderem benannt:

- Erklärbarkeit in allen Phasen des KI-Lebenszyklus,
- Transparenz,
- Informationspflichten der Arbeitgeber gegenüber den Beschäftigten,
- Rechenschafts- und Risikominimierungspflichten derjenigen, die KI im Beschäftigungskontext einsetzen,
- Antidiskriminierungsvorgaben,
- Sensibilisierung von KI-Anwendern sowie
- Datenschutz durch Technikgestaltung (privacy by design).

Neben der Möglichkeit eines unabhängigen Third-Party-Auditing findet insbesondere auch der in Art. 22 DSGVO verankerte Grundsatz, dass Beschäftigte ebenso wie andere betroffene Personen grundsätzlich keiner ausschließlich auf einer automatisierten Verarbeitung einschließlich Profiling beruhenden Entscheidung unterworfen werden dürfen bzw., falls dies ausnahmsweise zulässig ist, über Einwirkungsrechte verfügen sollen, besondere Erwähnung. Auf Grundlage der Ergebnisse der im Annex vorgestellten Umfrage werden Szenarios und Maßstäbe aufgezeigt, die das besonders hohe Risiko der Entwicklung und Verwendung von KI im Beschäftigungskontext begründen.

Insgesamt stellt der Text aufbauend auf zuvor verabschiedete GPA-Papiere übergreifende und allgemeine Prinzipien zusammen, die insbesondere auch bei der Entwicklung und dem Einsatz von KI im Beschäftigungskontext Anwendung finden sollen.

Ich werde mich weiterhin aktiv in die internationale Zusammenarbeit zur Festlegung von Leitlinien für einen sicheren und datenschutzgerechten Einsatz Künstlicher Intelligenz im Beschäftigungskontext einbringen und dabei den sich in diesem Zusammenhang stellenden Herausforderungen – z. B. mit Blick auf das potentielle Machtungleichgewicht zwischen Arbeitgebern und Beschäftigten – in besonderem Maße Rechnung tragen.

Querverweise:

4.3.2 45. GPA Jahreskonferenz

3.2.4 Verordnung zum Auffinden von Material des sexuellen Online-Kindesmissbrauchs

Der europäische Gesetzgeber hat seinen Verordnungsentwurf zum Auffinden von Material des sexuellen Online-Kindesmissbrauchs (Child sexual abuse material – CSAM) auch im Jahr 2023 weiter vorangetrieben. Während das EU-Parlament die datenschutzpolitisch kritischsten Punkte des Entwurfs gestrichen hat, sind diese Punkte im Rat der EU überwiegend noch nicht vom Tisch. Meine Kritik findet zudem immer mehr Unterstützung in Deutschland und der EU.

Bereits in meinem letzten Tätigkeitsbericht hatte ich über die Pläne des Gesetzgebers der Europäischen Union (EU) zur Verabschiedung einer Verordnung zur Prävention und Bekämpfung des sexuellen Online-Kindesmissbrauchs (CSAM-VO) berichtet und hierbei die datenschutzrechtlich höchst problematischen Punkte kritisiert (31. TB Nr. 4.4.1).

Der von der Europäischen Kommission im Mai 2022 vorgelegte Verordnungsentwurf sieht vor, dass Anbietende von Messenger- und Hostingdiensten verpflichtet werden, sämtliche Kommunikationsinhalte und Daten ihrer Nutzenden auf CSAM zu durchleuchten sowie Nachrichten auf Annäherungsversuche von Erwachsenen gegenüber Kindern in sexueller Missbrauchsabsicht (sog. Grooming) zu scannen. Dabei sollen neben Textnachrichten auch Audionachrichten abgehört werden. Das Mitlesen bzw. Mithören von privater Kommunikation soll entweder durch ein Durchbrechen der Ende-zu-Ende-Verschlüsselung oder durch ein Auslesen direkt auf dem jeweiligen Gerät der Nutzenden (sog. Client-Side-Scanning) erfolgen. Ein Durchbrechen der Verschlüsselung würde jede Form vertraulicher Kommunikation faktisch unmöglich machen und zu Sicherheitslücken führen, die auch von Kriminellen genutzt werden könnten. Dies führt im Ergebnis – ebenso wie ein Auslesen auf privaten Geräten – zu eklatanten Verstößen gegen die Achtung des Privatlebens und gegen das Fernmeldegeheimnis.

Das Ziel, den sexuellen Online-Kindesmissbrauch aufzuhalten, ist überaus wichtig und unterstützenswert. Jedoch schießen die Pläne des europäischen Gesetzgebers deutlich über dieses Ziel hinaus, indem sie eine anlasslose und flächendeckende Überwachung der privaten Kommunikation vorsehen. Der EU-Gesetzgeber argumentiert stets, der Verordnungsentwurf würde den Erlass von sog. Aufdeckungsanordnungen nur gegenüber einzelnen Diensteanbietern vorsehen. Innerhalb eines Dienstes wird jedoch sämtliche Kommunikation durchleuchtet, so dass bei einem Diensteanbieter wie WhatsApp von einer solchen Überwachung allein in Deutschland potenziell circa 60 Millionen Bürgerinnen und Bürger betroffen wären.

In einem derartig flächendeckenden Auslesen der privaten Kommunikation sehe ich unverhältnismäßige

Verstöße gegen die Kernvorgaben zum Datenschutz, zur Achtung des Privatlebens, zur Vertraulichkeit der Kommunikation und zum Fernmeldegeheimnis. Diese Grundrechte sind den Bürgerinnen und Bürgern jedoch nach den Art. 7 und 8 der EU-Grundrechte-Charta und nach Art. 10 GG zu gewähren. Durch den flächendeckenden Umfang der geplanten Maßnahmen und die Tiefe der Eingriffe in die genannten Grundrechte sehe ich einen Verstoß gegen den Wesensgehalt dieser Grundrechte, der absolut unverhältnismäßig und nicht zu rechtfertigen ist. Diese scharfe Kritik teilen auch meine europäischen Partner, wie eine gemeinsame Stellungnahme vom Europäischen Datenschutzausschuss (EDSA) und vom Europäischen Datenschutzbeauftragten (EDPS) zum Verordnungsentwurf verdeutlicht,[16] an der ich aktiv mitgewirkt habe.

In diesem Jahr habe ich mich auch zusammen mit meinen Kolleginnen und Kollegen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) kritisch zum geplanten Verordnungsentwurf geäußert: in einer gemeinsamen Entschließung haben die 18 deutschen Datenschutzaufsichtsbehörden scharf kritisiert, dass es sich dabei um eine anlasslose Massenüberwachung handele, die nicht mit den Grundrechten auf Achtung des Privat- und Familienlebens, der Vertraulichkeit der Kommunikation und zum Schutz personenbezogener Daten vereinbar ist und vor den verheerenden Folgen einer Durchbrechung der Ende-zu-Ende-Verschlüsselung gewarnt.[17]

Der Innenausschuss des EU-Parlaments hat sich am 14. November 2023 auf eine vorläufige Position[18] geeinigt, mit der das Parlament in die sog. Trilog-Verhandlungen mit den EU-Mitgliedstaaten und der EU-Kommission gehen möchte. Hierbei wurde die Durchbrechung der Ende-zu-Ende-Verschlüsselung zu meiner großen Zufriedenheit von den EU-Abgeordneten gestrichen. Außerdem sollen Aufdeckungsanordnungen gegenüber Diensteanbietern nur nach Überprüfung durch einen Richter und nur in Bezug auf einzelne Personen oder Gruppen bei begründetem Verdacht ausgesprochen werden. Verhältnismäßige und gezielte Maßnahmen zur Risikominderung durch die Dienstanbieter sollen bevorzugt erfolgen. Um ungewünschte Kontaktaufnahmen von Erwachsenen gegenüber Kindern zu verhindern, sollen betroffene Diensteanbieter die elterliche Kontrolle stärken und die Einwilligung der Nutzenden zur Voraussetzung vor Erhalt von Nachrichten machen.

Im Rat der EU wird bisher lediglich diskutiert, den Anwendungsbereich der Aufdeckungsanordnungen auf bekanntes CSAM zu beschränken (d. h. unbekanntes CSAM und das Aufspüren von Erwachsenen, die sich Kindern annähern – sog. Grooming – auszunehmen). Davon abgesehen sind aber kaum Verbesserungen erkennbar, da z. B. Aufdeckungsanordnungen auch verschlüsselte Dienste umfassen sollen. Insgesamt konnte bisher für keine der im Rat vorgeschlagenen Positionen eine Mehrheit der Mitgliedstaaten erzielt werden.

Die EU-Kommission möchte den Verordnungsentwurf weiterhin unbedingt verabschieden – und greift dabei auch zu ungewöhnlichen Mitteln: es gab Berichte darüber, dass die EU-Kommission vor der geplanten Abstimmung im Rat der EU gezielte Werbung für die Chatkontrolle auf dem Mikrobloggingdienst X (ehemals Twitter) in denjenigen EU-Mitgliedstaaten in der jeweiligen Landessprache in Auftrag gegeben habe, die im Rat der EU noch gegen den Entwurf sind. Hierbei wurden wohl auch politische und religiöse Filter für sog. Mikrotargeting verwendet. Ein derartiges Vorgehen halte ich rechtlich und politisch für äußerst fragwürdig. Der Europäische Datenschutzbeauftragte hat zu diesem Vorfall eine Untersuchung eingeleitet und von der Datenschutzorganisation NOYB eine Beschwerde zu diesem Vorfall erhalten.

Eine Einigung zwischen den EU-Mitgliedstaaten im Rat der EU steht noch aus, so dass die Trilog-Verhandlungen nicht begonnen haben. Die Positionen der Mitgliedstaaten zu dem Verordnungsentwurf liegen zum Teil noch weit auseinander. Ein Vorschlag zum Aufspalten des Verordnungsentwurfs in einen kritischen (inklusive des Durchleuchtens von Kommunikationsinhalten) und einen weniger kritischen Teil ist zunächst gescheitert. Die Bundesregierung hat sich im April 2023 kritisch gegen viele Punkte des Verordnungsentwurfs positioniert und ihre Zustimmung zum aktuellen Ratsentwurf von einer Änderung der wesentlichen Kritikpunkte abhängig gemacht. Viele dieser Kritikpunkte teile ich und freue mich, dass die Bundesregierung meine Kritik aufgegriffen hat.

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

17 Entschließung der DSK vom 17. Oktober 2023, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20231017DSKEntschliessungChatkontrolle.pdf

18 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

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 deutschen und europäischen (Kommunikations-) Grundrechte wahrt und ein flächendeckendes und anlassloses Auslesen privater Kommunikation verbietet oder anderenfalls darauf hinzuwirken, den Verordnungsentwurf insgesamt abzulehnen.

3.2.5 Datenverarbeitung bei der FIU

Ich begrüße zwar den Einsatz von automatisierten Systemen und künstlicher Intelligenz (KI), um der hohen Anzahl von Eingängen von Verdachtsmeldungen bei der Financial Intelligence Unit (FIU) Herr zu werden, aber solche Systeme müssen datenschutzkonform ausgestaltet sein. Dies ist nach derzeitiger Praxis der FIU bei der Bearbeitung von Verdachtsmeldungen nicht der Fall.

Wie in den vergangenen Jahren (29. TB Nr. 6.8 und 30. TB Nr. 8.2.9) stand auch in diesem Jahr die Neugestaltung der IT-Landschaft der FIU im Fokus. Dabei richtete sich mein Augenmerk im Berichtszeitraum auf die Softwarekomponente FIU-Analytics. Diese dient der algorithmenbasierten Analyse von eingehenden Verdachtsmeldungen und unterstützt derzeit die Bearbeitenden bei der manuellen Sichtung mittels verschiedener automatisierter Prognosen. Am 15. März 2023 führten meine Mitarbeiterinnen und Mitarbeiter hierzu einen Informationsbesuch in den Räumlichkeiten der FIU durch, um sich die Funktionsweise dieser KI-Anwendung erläutern zu lassen.

Die FIU erlebte in den vergangenen Jahren steigende Neueingänge von Verdachtsmeldungen. Alleine im Jahr 2021 sind 298.507 neue Verdachtsmeldungen bei der FIU eingegangen.[19] Angesichts dieser Eingangszahlen ist eine manuelle Sichtung jeder einzelnen Verdachtsmeldung nicht leistbar und führte in der Vergangenheit zu erheblichen Speicherzeiten unbearbeiteter Verdachtsmeldungen. Hierunter eine Vielzahl von Bagatellfällen und solchen Transaktionen, die im Ergebnis gar nicht mit einer strafbaren Handlung in Zusammenhang gebracht werden konnten. Dies ist auch aus datenschutzrechtlicher Sicht kein akzeptables Szenario. Daher ist es auch meiner Meinung nach geboten, automatisierte Systeme einzusetzen, um relevante von irrelevanten Verdachtsmeldungen zu trennen. Diese Systeme müssen jedoch datenschutzkonform ausgestaltet sein, wobei insbesondere der Grundsatz der Datenminimierung zu beachten ist, um die Speicherung von Daten unbescholtener Bürger bei der FIU zu vermeiden.

Im Berichtszeitraum und bis heute werden eingehende Verdachtsmeldungen auf Auffälligkeiten durchsucht. Bei einem Treffer werden die Verdachtsmeldungen der manuellen Bearbeitung zugeführt. Unauffällige Meldungen werden im Informationspool gespeichert, verbleiben dort für die nächsten drei Jahre und werden nach Ablauf der Frist pauschal und ohne eine manuelle Prüfung gelöscht. Erhält die FIU innerhalb der Speicherzeit weitere Informationen, die auf einen Zusammenhang mit strafbarem Handeln hindeuten, werden die betroffenen Verdachtsmeldungen erstmalig manuell geprüft.

Die Praxis der pauschalen Speicherung von unauffälligen Verdachtsmeldungen im Informationspool und deren Vorhaltung für einen Zeitraum von mindestens drei Jahren, ohne das jemals eine Bewertung dieser unauffälligen Verdachtsmeldungen erfolgt, ist datenschutzrechtlich unzulässig. Ich habe daher gegenüber der FIU diesbezüglich eine Beanstandung ausgesprochen.

Die FIU ist nach § 29 Abs. 1 GwG nur befugt, personenbezogene Daten zu verarbeiten, soweit diese Daten für ihre Aufgabenerfüllung erforderlich sind. Des Weiteren hat sie nach § 37 Abs. 2 und Abs. 4 GwG die Verpflichtung, personenbezogene Daten zu löschen, wenn diese für ihre Aufgabenerfüllung nicht mehr erforderlich sind. Dies ist bei der Einzelfallbearbeitung und nach regelmäßigen Fristen zu prüfen. Schlussendlich ist sie nach dem Grundsatz der Datenminimierung verpflichtet, nur so viele personenbezogene Daten zu verarbeiten, wie für die konkrete Aufgabenerfüllung erforderlich ist.

Durch die gesetzlichen Regelungen wird die FIU verpflichtet positiv festzustellen, dass die Speicherung der konkreten Verdachtsmeldungen für ihre Aufgabenerfüllung erforderlich sowie eine Speicherung über drei Jahre notwendig ist. Ohne Kenntnisse über den Inhalt der Meldung ist eine solche Feststellung für die FIU unmöglich. Da die FIU Adressat der genannten gesetzlichen Regelung ist, reicht eine Beurteilung des Sachverhalts durch die meldenden Verpflichteten nicht aus.

Auch die Anwendung des sogenannten risikobasierten Ansatzes kann die dargestellte Praxis nicht rechtfertigen. Richtig und datenschutzrechtlich zu befürworten ist, dass sich die FIU auf werthaltige Meldungen konzentriert. Dies kann aber im Gegenzug nur heißen, das un-

19 FIU Jahresbericht 2021, abrufbar unter: https://www.zoll.de/SharedDocs/Downloads/DE/Pressemitteilungen/2022/z89_jahresbericht_fiu_2021.pdf

auffällige Meldungen gelöscht werden müssen. Derzeit tragen rechtstreue Bürger alleine das Risiko, dass ihre Daten bei einer staatlichen Behörde zur Bekämpfung von Straftaten für drei Jahre rechtswidrig gespeichert werden. Unter einem risikobasierten Ansatz verstehe ich ein vorhandenes Risiko zu akzeptieren, dass Bagatellfälle eventuell nicht aufgedeckt werden, um dadurch die Speicherung von Daten rechtstreuer Bürger deutlich zu reduzieren. Eine eingriffsintensive heimliche Datenanalyse durch die FIU ist zur Aufklärung von Bagatelldelikten aus meiner Sicht nicht verhältnismäßig.

3.3 Gesetzgebung im Sicherheitsbereich

Das Jahr 2023 stand ganz im Zeichen neuer Sicherheitsgesetzgebung. Anlass hierfür war zunächst das Grundsatzurteil des Bundesverfassungsgerichts (BVerfG) vom April 2022 zum Bayerischen Verfassungsschutzgesetz, das u. a. gesetzlich festgelegte Schwellen für die Beobachtung von Personen und Gruppierungen forderte und auch der Übermittlung von Informationen der Nachrichtendienste an andere Behörden enge Grenzen setzte. Aber erst die Tatsache, dass das BVerfG in einem Beschluss im September 2022 wesentliche Übermittlungsvorschriften auch im Bundesverfassungsschutzgesetz (BVerfSchG) ab dem 31. Dezember 2023 für nichtig erklärte, veranlasste die Bundesregierung zum Handeln – mit einer sog. ersten Reform des Nachrichtendienste-Rechts.

Im Bereich der Finanzkriminalität und Geldwäsche wurden neue Gesetze geschaffen, um eine effektive Bekämpfung der Finanzkriminalität und auch der Sanktionsdurchsetzung zu erreichen. Bei allem Respekt vor der gestiegenen Notwendigkeit einer effektiven Strafverfolgung und Sanktionsdurchsetzung in diesem Bereich bilden die neuen Vorschriften und deren Umsetzung in einer neuen Behörde unter dem Dach des Bundesfinanzministeriums – der Bundesoberbehörde zur Bekämpfung der Finanzkriminalität – mit zum großen Teil gleichen Ermittlungsbefugnissen wie die Polizeien eine zusätzliche neue Überwachungsdimension.

Längst überfällig ist die immer noch nicht abgeschlossene Fortentwicklung des Bundespolizeigesetzes (BPolG), das den durch höchstrichterliche Rechtsprechung vorgegebenen europäischen und nationalen Rechtsrahmen nicht erfüllt. Wegen der fehlenden Umsetzung der immerhin seit über fünf Jahren gültigen Richtlinie zum Datenschutz bei Polizei und Justiz (JI-Richtlinie) sieht sich die Bundesrepublik Deutschland sogar einem Vertragsverletzungsverfahren der EU ausgesetzt.

Viele der genannten Gesetze wurden – nach langen internen Beratungen der Regierung selbst – zum Ende des Jahres gewissermaßen im Schnelldurchgang durch das parlamentarische Verfahren geschleust. Obwohl meine Beteiligung in einigen Fällen mit Fristen von gerade mal 48 Stunden sehr zu wünschen übrigließ, habe ich in allen Verfahren ausführlich Stellung genommen und dezidiert meine datenschutzrechtlichen Bedenken vorgetragen.

Insgesamt folgt die Sicherheitsgesetzgebung keinem schlüssigen, ineinandergreifendem Konzept. Sie bedeutet eine weitere Ausweitung der Überwachung unserer Bürgerinnen und Bürger mit einer Vielzahl additiver Grundrechtseingriffe durch redundante Ermittlungsbefugnisse.

Die von mir bereits seit Jahren geforderte und im Koalitionsvertrag vereinbarte Überwachungsgesamtrechnung fand bislang nicht statt. Erst im Mai 2023 hat das Bundesministerium des Innern und für Heimat die Überwachungsgesamtrechnung als Projekt über das Beschaffungsamt ausgeschrieben. Über den Stand der Vergabe werde ich nur auf Nachfrage unterrichtet. Immerhin konnte ich nun der Presse entnehmen, dass der Zuschlag erteilt wurde, so dass das Projekt nun starten kann. Dies begrüße ich sehr. Der Schutz von Betroffenenrechten und die Kompensation für von Sicherheitsbehörden oft heimlich vorgenommener Grundrechtseingriffe gehören zu meinen Kernaufgaben. Daher bin ich gerne bereit, mich in das Projekt einzubringen. Im Anschluss daran soll die Bundesregierung nach eigener Aussage eine Freiheitskommission gründen, die den Gesetzgeber bei der Frage beraten soll, ob bestimmte Eingriffsbefugnisse wirklich erforderlich sind.[20] Ich erwarte zumindest bei dieser Einrichtung eine frühzeitige und sachgerechte Einbindung.

3.3.1 Gesetzgebung im Bereich der Nachrichtendienste

Der umfassende Reformbedarf der gesetzlichen Grundlagen für die Arbeit der Nachrichtendienste zeichnete sich bereits durch mehrere wegweisende Entscheidungen des Bundesverfassungsgerichts (BVerfG) ab. Es kam im aktuellen Berichtszeitraum zwar zu den erwarteten Gesetzgebungsverfahren des Bundesverfassungsschutz-

20 Siehe hierzu die Pressemitteilung des BMI vom 10. Januar 2024, abrufbar unter: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/01/evaluation-sicherheitsgesetze.html

gesetz (BVerfSchG), gleichzeitig auch dem des Gesetzes über den Militärischen Abschirmdienst (MADG) sowie des BND-Gesetzes (BNDG). Allerdings verfehlten alle drei Gesetzesänderungen bei weitem das Ziel einer umfassenden Reformierung und werden den Anforderungen des BVerfG erneut nicht gerecht.

In Bezug auf die Nachrichtendienste hat das BVerfG im Jahr 2022 zwei wegweisende Entscheidungen gefällt, die eine grundlegende Anpassung des BVerfSchG, MADG und BNDG erfordern. In dem Urteil des BVerfG[21] zum Bayerischen Verfassungsschutzgesetz wurde bereits die Verfassungswidrigkeit zahlreicher bayerischer Normen festgestellt, die ebenfalls Ausstrahlungswirkungen auf das Bundesrecht haben. Mit dem Beschluss des BVerfG wurde die Verfassungswidrigkeit einzelner Übermittlungsvorschriften des BVerfSchG und die Nachbesserungsmöglichkeit bis zum Ende des Jahres 2023 noch einmal ausdrücklich bestätigt (31. TB Nr. 7.6).[22] Bis zum Jahresende mussten die Vorschriften daher reformiert werden, ansonsten wären sie ungültig geworden und Übermittlungen hätten nicht mehr stattfinden können. Die nun beschlossenen Änderungen beschränken sich, bis auf vereinzelte gesetzliche Anpassungen, ausschließlich auf die Reformierung der in dem Beschluss von September 2022 monierten Übermittlungsvorschriften.

Im Verhältnis zum Vorentwurf der Bundesregierung sind das BNDG, das BVerfSchG und das MADG erst durch Änderungsanträge aus dem Innenausschuss des Bundestages sozusagen auf der Ziellinie so gerade eben in den meisten Punkten noch der (erneuten) Verfassungswidrigkeit entgangen. Die Übermittlungsvorschriften folgen nun in allen Gesetzen grundsätzlich einer gleichen Systematik und einem gleichen Wortlaut und orientieren sich insgesamt deutlich an den Vorgaben des BVerfG. Leider gilt das aber nicht für alle Teile. Gravierend ist die aus meiner Sicht eindeutige Verfassungswidrigkeit von § 65 BNDG, der eine Umgehung der neuen Übermittlungsvorschriften darstellt und darüber hinaus auch gegen die Vorgaben des BVerfG in dessen Urteil vom 19. Mai 2020 zur strategischen Ausland-Fernmeldeaufklärung verstößt. Nach diesem Urteil sollen Daten, die zur politischen Unterrichtung der Bundesregierung ohne nennenswerte Erhebungsschwellen erhoben werden dürfen, ausschließlich zum Zweck der politischen Unterrichtung der Bundesregierung verwendet werden. Die Bundesregierung besteht aus dem Bundeskanzler und den Ministerinnen und Ministern. Weder der den Ministerien nachgeordnete Bereich noch Landesregierungen sind Teile der Bundesregierung. An genau diese sollen solche Daten aber ebenfalls übermittelt werden dürfen.

Unverändert geblieben sind leider die jeweiligen Vorschriften zur Eigensicherung, die sowohl das BNDG als auch das BVerfSchG erstmalig enthalten. Diese divergieren deutlich ohne zwingenden Grund. Es fehlen dort z. B. mit Speicherfristen, Bestimmungen zur Zweckbindung und Kennzeichnungspflichten grundsätzliche datenschutzrechtliche Anforderungen.

Die Änderungen im BVerfSchG, die ich in der Version der Bundesregierung leider umfänglich kritisieren musste,[23] sind durch den Deutschen Bundestag deutlich verbessert worden. Aber auch hier bleiben noch Unsicherheiten und Lücken. Zum Beispiel fehlt aus meiner Sicht in beiden Gesetzen eine spezifische Rechtsgrundlage für das systematische Erfassen und Zusammenführen öffentlich zugänglicher Daten vor deren Übermittlung.

Deutlich kritisieren musste ich im Gesetzgebungsverfahren auch den Ablauf als solchen. Spätestens seit den Entscheidungen vom 26. April 2022 und vom 28. September 2022 war klar, dass die Übermittlungsvorschriften einer umfangreichen Novellierung bedurften. Nachdem eine Bund-Länder-Arbeitsgruppe bereits im September 2022 umfangreiche Auswertungen und Vorschläge vorgelegt hatte, dauerte es trotzdem bis August 2023, bis die Bundesregierung offiziell die Ressortberatungen startete. Weder für mich noch für das Parlament, das sich der Verfallsfrist am 31. Dezember 2023 gegenübersah, sind diese Zeiträume ausreichend, sich vertieft mit diesen Gesetzen auseinanderzusetzen. Ein solches Vorgehen schwächt das parlamentarische Verfahren, das Vertrauen der Bürgerinnen und Bürger und mangels Zeit für einen fachlichen und politischen Diskurs leiden die Vorschriften im Einzelnen. Abgesehen von der sehr kurzen Stellungnahmefrist musste ich auch feststellen, dass jedenfalls mit Blick auf den Gesetzentwurf zur Änderung des BVerfSchG offenbar meine Stellungnahme nicht wirklich gelesen wurde. Denn nicht einmal meine Hinweise auf redaktionelle Fehler wie z. B. Zahlendreher bei Verweisen auf Vorschriften wurden aufgegriffen. Sie fanden sich weitgehend in der Kabinettfassung des Gesetzentwurfs wieder und wurden letztlich erst durch die Änderungsanträge des Bundestages beseitigt.

Dem aus meiner Sicht aber auch schon durch mehrere frühere Gerichtsentscheidungen klaren Auftrag an den Gesetzgeber, das Recht der Nachrichtendienste

21 Urteil des Bundesverfassungsgerichts vom 26. April 2022, Az.: 1 BvR 1619/17
22 Siehe auch Beschluss des Bundesverfassungsgerichts vom 28. September 2022, Az.: 1BvR 2354/13
23 Stellungnahme des BfDI vom 27. Oktober 2023, abrufbar unter: www.bfdi.bund.de/stellungnahmen

in Gänze zu überarbeiten, wird der Gesetzesentwurf zum BVerfSchG in keiner Weise gerecht. Es fehlen z. B. weiterhin die Einführung einer vom BVerfG geforderten unabhängigen Vorabkontrolle besonders eingriffsintensiver Maßnahmen wie einer Observation. Für weitere grundlegende Reformen und auch dafür, dass mir für den Bereich der Nachrichtendienste ebenfalls Abhilfebefugnisse eingeräumt werden, werde ich mich weiter einsetzen.

Querverweise:

9.1.7 Kontrollen beim Bundesamt für den Verfassungsschutz, 9.1.8 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst

3.3.2 Modernisierung des Bundespolizeigesetzes

Das Bundespolizeigesetz (BPolG) soll umfassend modernisiert und neu strukturiert werden. Mein Haus hat sich ausführlich mit den geplanten Änderungen auseinandergesetzt und diese aus datenschutzrechtlicher Sicht bewertet. Während des Gesetzgebungsverfahrens konnte ich durch meine Stellungnahmen an einigen Stellen Verbesserungen erreichen. Leider haben aber auch viele meiner Empfehlungen bislang keinen Eingang in den Gesetzesentwurf gefunden, sodass aus meiner Sicht weiterhin Bedenken verbleiben.

Kurz vor Ende des Jahres ist es der Bundesregierung nach vielen Abstimmungsrunden gelungen, den „Entwurf eines Gesetzes zur Neustrukturierung des Bundespolizeigesetzes (BPolG)“ im Kabinett zu verabschieden. Mit dem Entwurf soll unter anderem endlich die längst überfällige Umsetzung der Richtlinie zum Datenschutz bei Polizei und Justiz (JI-Richtlinie) im Bereich der Bundespolizei erfolgen. Die Frist hierzu lief bereits im Mai 2018 ab, mit Schreiben vom 6. April 2022 hatte die EU-Kommission deshalb ein Vertragsverletzungsverfahren in Bezug auf die fehlende Umsetzung im Bereich der Bundespolizei eingeleitet. Neben einer allgemeinen Neuordnung der BPolG-Vorschriften sieht der aktuell vorliegende Entwurf auch eine Umsetzung der BVerfG-Rechtsprechung zur hypothetischen Datenneuerhebung vor.[24]

Ich habe im Rahmen der Ressortabstimmung mehrfach kritisch Stellung genommen und in diesem Zusammenhang die lange Verzögerung kritisiert. Einige Änderungen im Vergleich zu früheren BPolG-Entwürfen begrüße ich ausdrücklich, etwa den Wegfall der eingriffsintensiven Instrumente der Quellen-TKÜ und der Online-Durchsuchung. An anderen Stellen bestehen weiterhin zum Teil erhebliche datenschutzrechtliche Bedenken.

So enthält der Entwurf zahlreiche, zum Teil neu hinzugekommene grundrechtsintensive Eingriffsbefugnisse (z. B. präventive Telekommunikationsüberwachung, Erhebung von Verkehrs- und Nutzungsdaten), ohne dass deren Erforderlichkeit im Einzelnen immer ausreichend dargelegt wird. Dies ist nicht im Sinne einer „vorausschauenden, evidenzbasierten und grundrechtsorientierten Sicherheits- und Kriminalpolitik“, welche die Regierungsparteien sich im Koalitionsvertrag vorgenommen hatte.[25]

Mit dem Entwurf sollen beispielsweise die Einsatzmöglichkeiten von Bodycams auf Orte ausgedehnt werden, die nicht öffentlich zugänglich sind und für aufenthaltsbeendende und verhindernde Maßnahmen durch die Bundespolizei genutzt werden. Bei Video- und Tonaufnahmen einer Person in eng umgrenzten Räumlichkeiten handelt es sich um einen besonders schweren Grundrechtseingriff, weshalb hier hohe Anforderungen an entsprechende Rechtsgrundlagen gestellt werden müssen. Dem genügen die bisherigen Entwürfe nicht ausreichend.

Gleiches gilt für die vorgesehene Befugnis zum Drohneneinsatz für Überwachungszwecke, der aufgrund der erhöhten Beobachtungsreichweite und der eingeschränkten Möglichkeit, sich einer Überwachung zu entziehen, regelmäßig mit einer hohen Eingriffstiefe einhergeht. Die Schaffung einer Spezialnorm für Bild- und Tonaufnahmen mittels Drohnen ist daher zwar grundsätzlich zu begrüßen, gleichzeitig aber auch an erhöhten verfassungsrechtlichen Anforderungen, insbesondere bei Überwachungsmaßnahmen im Rahmen von Versammlungen, zu messen.

Aus Sicht meines Hauses sind die Einführung von Pflichtkontrollen in Bezug auf eingriffsintensive Maßnahmen sowie die Schaffung einer Anordnungsbefugnis bei Datenschutzverstößen positiv hervorzuheben. Zu kritisieren ist dagegen der Wegfall der sog. Errichtungsanordnungen für automatisierte Dateisysteme der Bundespolizei und meiner damit einhergehenden Anhörungspflicht, die bislang ein wichtiges Kontrollinstrument in der datenschutzrechtlichen Aufsicht darstellt.

Ich werde den Gesetzentwurf 2024 im parlamentarischen Verfahren weiter begleiten und darauf hinwirken,

24 Urteil des Bundesverfassungsgerichts vom 20. April 2016, Az.: 1 BvR 966/09, 1 BvR 1140/09

25 Siehe S. 86 des Koalitionsvertrags zwischen SPD, Bündnis 90/Die Grünen und FDP, abrufbar unter: https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800

dass datenschutzrechtliche Belange noch stärker berücksichtigt werden.

3.3.3 Gesetz zur Verbesserung der Bekämpfung von Finanzkriminalität

Am 14. Dezember 2023 hat der Bundestag das Gesetz zur Verbesserung der Bekämpfung von Finanzkriminalität (Finanzkriminalitätsbekämpfungsgesetz – FKBG) in erster Lesung beraten. Neben der Errichtung einer neuen, eigenständigen Behörde zur Finanzkriminalitätsbekämpfung sieht das Gesetz unter anderem die Einführung eines Immobilientransaktionsregisters vor. Im Rahmen der Ressortabstimmung wurden viele meiner Anregungen und Kritikpunkte bereits berücksichtigt. Dennoch genügen einige Vorschriften noch immer nicht allen datenschutz- und verfassungsrechtlichen Anforderungen.

Der Zustand der Geldwäschebekämpfung in Deutschland stand zuletzt aufgrund bestehender Defizite in der Kritik. Neben zeitweise hohen Bearbeitungsrückständen im Hinblick auf Geldwäscheverdachtsmeldungen bei der Zentralstelle für Finanztransaktionsuntersuchungen (FIU) stellte auch die Financial Action Task Force (FATF) in ihrem Abschlussbericht aus dem Jahr 2022 einen großen Nachholbedarf fest. Die Regierungsfraktionen hatten sich dementsprechend im Koalitionsvertrag auf die Umsetzung der FATF-Empfehlungen und eine Optimierung der Geldwäschebekämpfung verständigt.

Zur nachhaltigen Verbesserung der Bekämpfung von Finanzkriminalität soll mit dem FKBG ein eigenständiges Bundesamt zur Bekämpfung von Finanzkriminalität (BBF) geschaffen werden. Die bisher bei der Generalzolldirektion angesiedelte Zentralstelle für Sanktionsdurchsetzung (ZfS) sowie die FIU werden ab Mitte 2025 in das neue Bundesamt überführt, das mit einem ganzheitlichen Ansatz Datenanalyse, straf- und verwaltungsrechtliche Ermittlungen sowie geldwäscherechtliche Aufsicht in einer Behörde zusammenführen soll.

Im Mittelpunkt des Entwurfs steht das innerhalb des BBF angesiedelte neue Ermittlungszentrum Geldwäsche (EZG), das mit weitgehenden polizeilichen Ermächtigungen und mitunter eingriffsintensiven Datenverarbeitungsbefugnissen ausgestattet wird. Diese zusätzlichen neuen Eingriffsbefugnisse werden ebenfalls eingeführt, ohne dass die im Koalitionsvertrag bis Ende 2023 vereinbarte Evaluierung der Sicherheitsgesetze und eine Überwachungsgesamtrechnung überhaupt begonnen wurde.

Auch werden die Zuständigkeiten des BBF im Bereich der Geldwäschebekämpfung nicht ausreichend von denen des Bundeskriminalamtes (BKA) und der Zollverwaltung abgegrenzt. Bei Überschneidungen sollen Ermittlungen laut der Gesetzesbegründung in „partnerschaftlicher Zusammenarbeit“ erfolgen.

Derartige Doppelzuständigkeiten bergen jedoch die Gefahr mehrfacher, ggf. nicht erforderlicher Datenhaltungen und -übermittlungen und generell ein erhöhtes Risiko für die Rechte und Freiheiten von betroffenen Personen.

Ein weiterer Bestandteil des Gesetzes ist die Einführung eines Immobilientransaktionsregisters. Dieses soll sich aus Angaben speisen, die bereits heute im Transparenzregister, im Grundbuch oder bei der Finanzverwaltung vorhanden sind. Mit dem datenschutzrechtlichen Grundsatz der Vermeidung doppelter Datenhaltung ist dies nicht zu vereinbaren und könnte auch anders gelöst werden. Schließlich kritisiere ich u. a. die fehlende Speicherbegrenzung in Bezug auf die im Register enthaltenen Daten: Diese sollen anstatt einer vollständigen Löschung nach 10 Jahren lediglich auf die im Grundbuch vorgehaltenen Daten – ohne weitere Löschfrist – reduziert werden.

In vorherigen Entwürfen vorgesehene Vorschriften zur automatisierten, auch KI-gestützten Datenanalyse und -auswertung durch das EZG und die Zollfahndung wurden zunächst zurückgestellt und sollen einer weiteren Prüfung unterzogen werden. Dies begrüße ich ausdrücklich, da die bisher geplanten Normen den vom Bundesverfassungsgericht im Frühjahr 2023 gestellten Anforderungen an die Ausgestaltung solcher Rechtsgrundlagen nicht vollumfänglich genügten.[26]

Meinem Haus fällt künftig neben der FIU die datenschutzrechtliche Aufsicht über das EZG zu. Bevor das BBF 2025 seine Arbeit aufnehmen soll, werde ich der im Aufbau befindlichen Behörde im Jahr 2024 beratend zur Verfügung stehen und sie dabei unterstützen, datenschutzrechtliche Belange bereits von Beginn an berücksichtigen zu können.

3.3.4 Gesetz zur Stärkung der risikobasierten Arbeitsweise der Zentralstelle für Finanztransaktionsuntersuchungen

Am 12. Oktober 2023 wurde im Bundestag das Gesetz zur Stärkung der risikobasierten Arbeitsweise der Zentralstelle für Finanztransaktionsuntersuchungen (FIU) beschlossen. Damit gibt es nun auf Bundesebene

26 Urteil des Bundesverfassungsgericht vom 16. Februar 2023, Az.: 1 BvR 1547/19, 1 BvR 2634/20

erstmals eine Befugnis, automatisierte Datenanalysen zur Bekämpfung von Straftaten durchzuführen. Im Verlauf des Gesetzgebungsverfahrens konnte ich einige Verbesserungen beim Datenschutz erreichen.

Die Fokussierung der FIU auf schwere Straftaten im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung ist ein wichtiges Ziel, das ich ausdrücklich unterstütze. Jedoch wurden mit dem Gesetzgebungsverfahren auch Befugnisse zur Durchführung automatisierter Datenanalysen sowie den Einsatz selbstlernender Systeme (Künstliche Intelligenz – KI) geschaffen.

Die FIU setzt bereits jetzt automatisierte Systeme ein, um die immense Anzahl eingehender Geldwäscheverdachtsmeldungen bewältigen zu können. Es verwundert daher nicht, dass nun gerade in diesem Bereich erste Regeln für den Einsatz von KI geschaffen wurden.

Allerdings werden Geldwäscheverdachtsmeldungen heimlich und noch unterhalb der Schwelle eines strafprozessualen Anfangsverdachtes abgegeben und von der FIU verarbeitet. Eine Datenanalyse- und Auswertung durch die FIU begründet deswegen einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung. Der Einsatz automatisierter Systeme kann sich je nach Verwendung gravierend auf die Freiheiten der Bürgerinnen und Bürger auswirken. Zum Beispiel dann, wenn sie die Behörde auf eine falsche Spur führen.

Der Gesetzgeber muss deshalb klare Grenzen vorgeben, um einen verhältnismäßigen Einsatz sicherzustellen. Insbesondere in Form von Eingriffsschwellen, Rechtsgüterschutz und Transparenz. Ziel der Bundesregierung sollte es sein, sich auf die werthaltigen Fälle von Geldwäsche und Terrorismusfinanzierung zu konzentrieren. Dies steht im Gegensatz zur derzeitigen Praxis, massenhaft Daten von Personen auszuwerten, die hierfür gar keinen Anlass gegeben haben.

Aufgrund der Komplexität von KI sind KI-basierte Datenverarbeitungen – wenn überhaupt – nur schwer nachvollziehbar. Je komplexer ein Algorithmus ist, desto größer ist die Fehler- und Diskriminierungsanfälligkeit. Der Einsatz selbstlernender Systeme erhöht daher die Intensität der ohnehin schon schwerwiegenden Eingriffe zusätzlich und sollte nur unter besonderen Schutzvorkehrungen in Betracht kommen. Entsprechende Anforderungen hat auch das Bundesverfassungsgericht in seiner Entscheidung vom 16. Februar 2023 zu polizeilichen Datenanalysen festgelegt.

Im Rahmen des Gesetzgebungsverfahrens konnte ich erreichen, dass mir endlich die Befugnis eingeräumt wird, gegenüber der FIU Maßnahmen zur Beseitigung von Datenschutzverstößen zu ergreifen. Weiterhin sind regelmäßige Pflichtkontrollen der Datenverarbeitung vorgesehen.

Auch begrüße ich, dass der Gesetzgeber entsprechend der Forderungen aus meinen Stellungnahmen die personenbezogenen Daten, die in die Datenanalyse einbezogen werden dürfen, abschließend festgelegt hat. Aus meiner Sicht wäre aber noch eine weitere Ausdifferenzierung der Vorgaben zur Durchführung der Analyse (z. B. Auswertemethode, Art der Analyseergebnisse) nötig gewesen.

Querverweise:

3.2.5 Datenverarbeitung bei der FIU

3.3.5 SÜG-Evaluierung – Verpasste Chancen

Infolge einer Evaluierung des Sicherheitsüberprüfungsgesetzes (SÜG) und getrieben von Forderungen des Parlamentarischen Kontrollgremiums nach Beschleunigung und Modernisierung wird das Gesetz im Moment überarbeitet. Hierbei soll nicht nur einer erhöhten Gefährdungslage, sondern auch dem zunehmenden Ruf nach Digitalisierung Rechnung getragen werden.

Das Bundesministerium des Inneren und für Heimat (BMI) schloss im letzten Berichtsjahr eine Evaluation des SÜG ab. Im Fokus standen die im Jahr 2017 geänderten oder neu hinzugekommenen Vorschriften. Schon mit dieser Einschränkung wurde aus meiner Sicht die Chance vertan, das in die Jahre gekommene Gesetz ganzheitlich in den Blick zu nehmen. An vielen Stellen ist es unübersichtlich und geradezu ein Negativbeispiel, was normenklare, für Betroffene nachvollziehbare Regelungen angeht. Schon die zentrale Bestimmung des § 13 SÜG die bestimmt, welche Daten eine betroffene Person über sich und nahestehende Personen angeben muss, ist ein unübersichtliches Konstrukt aus Festlegungen, Ausnahmen und zusätzlichen Festlegungen, dazu zahlreichen Verweisungen.

Auch bei der Auswahl der an der Evaluierung beteiligten Stellen wurde nicht die Chance genutzt, allen verfügbaren Sachverstand mit einzubeziehen. Die Evaluierung erfolgte ohne meine Beteiligung, obschon hier infolge zahlreicher Kontrollen und Beratungen bei unterschiedlichsten verantwortlichen Stellen erhebliches Erfahrungswissen über bestehende Defizite und praktische Herausforderungen des Gesetzes vorliegt. Gerade auch aus der Begleitung erster Digitalisierungsprozesse hätte ich frühzeitig Impulse und Best-Practice-Beispiele zur Modernisierung des Gesetzes einbringen können. So konnte ich erst im Nachgang der Evaluierung und in den späteren Ressortberatungen Vorschläge einbringen.

Für besonders wichtig halte ich die Entwicklung eines schlüssigen Gesamtkonzepts für alle Überprüfungsverfahren. Durch aktuelle und perspektivische Vorhaben wird der Personenkreis, der sich künftig einer einfachen Sicherheitsüberprüfung nach dem SÜG unterziehen muss, immer mehr ausgeweitet. Begründet wird dies im Wesentlichen mit einer verstärkten Bedrohungslage von innen und außen. Statt immer neue Rechtsnormverweisungen auf den § 1 Abs. 2 Nr. 4 SÜG zu schaffen, regte ich an, die sicherheitsempfindliche Tätigkeit i. S. d. § 1 Abs. 2 SÜG neu zu definieren, der Lebensrealität anzupassen und den Anwendungsbereich des Gesetzes auf ein neues tragfähiges Fundament zu heben. Der Gesetzgeber sollte die verschiedenen Vorschriften über Zuverlässigkeitsüberprüfungen zusammenführen und eine für alle Überprüfungsarten geltende einheitliche gesetzliche Grundlage schaffen. Insbesondere das Verhältnis zwischen personellem Geheimschutz, vorbeugendem personellen Sabotageschutz und Überprüfungen nach anderen Gesetzen sollte hierbei stimmig geregelt werden. In diesem Zusammenhang bietet es sich an, einheitliche gesetzliche Regelungen zum materiellen Verschlusssachenschutz ebenfalls ins SÜG selbst aufzunehmen. Jüngst wurden stattdessen teilweise voneinander abweichende Regelungen im Bundesverfassungsschutzgesetz auf der einen und im Gesetz über den Bundesnachrichtendienst auf der anderen Seite geschaffen.

Auch an eine Neudefinition der sicherheitsempfindlichen Stelle im SÜG wird sich der Gesetzgeber kaum heranwagen. Zumindest gab es hierfür im Berichtszeitraum keinerlei Anzeichen, obwohl ich dies mehrfach angemahnt habe. Vielmehr wurden neue Überprüfungen sowohl für die Bundespolizei als auch für das Bundesamt für Migration und Flüchtlinge eingeführt, jeweils standardmäßig und unabhängig vom konkreten Einsatzbereich. Hiermit wurde das nachvollziehbare Ziel verfolgt, Personen mit extremistischen Bestrebungen generell aus dem öffentlichen Dienst fernzuhalten. Zugleich fand jedoch eine weitere Abkehr von der Verknüpfung der Sicherheitsüberprüfung mit dem Geheim- und Sabotageschutz statt. Dieser schleichende Systemwechsel führt im Ergebnis zu einer erheblichen Ausweitung des betroffenen Personenkreises. Zum Redaktionsschluss war der finale Referentenentwurf des BMI noch nicht veröffentlicht. Allerdings steht schon nach dem Ergebnis der Evaluierung zu befürchten, dass die SÜG-Novelle zu einer Ausweitung von Grundrechtseingriffen führen wird, deren Verhältnismäßigkeit ich trotz einer verschärften Sicherheitslage in Frage stelle.

Insbesondere die standardmäßige und anlasslose Internetrecherche zur mitbetroffenen Person betrachte ich als unverhältnismäßig und lehne sie ab. Nach aktueller Rechtslage ist eine anlassbezogene Internetrecherche zur mitbetroffenen Person bereits möglich (vgl. § 12 Abs. 5 Satz 2 SÜG) und auch ausreichend. Ich werde das weitere Gesetzgebungsverfahren auf jeden Fall kritisch begleiten.

Was ich hingegen unterstütze, ist eine Überarbeitung und Anpassung der Rechtsgrundlagen für eine elektronische Datenverarbeitung. Zuständige Stellen dürfen bisher neben der Akte lediglich Dateien zur Bewirtschaftung des sicherheitsüberprüften Personals führen. Im Gegensatz zu den nichtöffentlichen Stellen ist eine elektronische Vorgangsbearbeitung für den öffentlichen Bereich gar nicht zulässig. Diese Differenzierung ist nicht mehr zeitgemäß und stellt die einzelnen Stellen vor erhebliche Schwierigkeiten, die ich bei meinen Kontrollen feststellen konnte. Daher begrüße ich grundsätzlich jede Initiative, das SÜG auf den aktuellen Stand zu bringen und fit für die Zukunft zu machen.

Ein modernes Gesetz sollte sich hierbei allerdings weniger an den Begrifflichkeiten von Akte und Datei orientieren, sondern zwischen verschiedenen Verarbeitungszwecken wie der Aufgabenerledigung und der Dokumentation unterscheiden, ohne diese zu vermischen. Hier bedarf es differenzierter Regelungen, welche Daten wie lange für welche Zwecke elektronisch verarbeitet werden dürfen. Soweit mehrere Zwecke künftig innerhalb eines Dateisystems bedient werden sollen, ist bei der technischen Ausgestaltung den verschiedenen Zwecken Rechnung zu tragen, insbesondere was Zugriffsrechte und Abgleichmöglichkeiten betrifft.

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.

3.4 Digitale Identitäten

Digitale Identitäten sind wichtige Bausteine bei der Digitalisierung. Sie ermöglichen Zugang und Teilhabe in einer zunehmend digitalisierten Gesellschaft – vom Informationszugang über Bürgerbeteiligungsverfahren bis zur Beantragung von Leistungen. Ihr Einsatz muss aber auf Dienstleistungen beschränkt werden, für die

eine Identifizierung notwendig ist. Wenn sie dann noch die Möglichkeiten datenschutzfreundlicher Technologien nutzen, können digitale Identitäten die Vorteile der Digitalisierung zu den Menschen bringen und ihre Grundrechte schützen.

Eine allgemein anerkannte Definition der häufig überlappend genutzten Begriffe Elektronische Identitäten, digitale Identitäten oder eIDs (von *electronic Identification*) gibt es nicht. Gemeint sind aber meist technische Systeme, die dazu dienen, im digitalen Raum die eigene Identität nachzuweisen. Häufig werden sie auch zur Authentifizierung genutzt. Für die Nutzenden bedeutet das, dass sie sich nicht mehr bei einzelnen Dienstleistern mit deren Zugangsverfahren anmelden, sondern eben ihre digitale Identität nutzen, um sich bei verschiedenen, voneinander unabhängigen Stellen anzumelden.

Beim Ausbau digitaler Identitäten gilt es zahlreiche Risiken für die Grundrechte der Bürgerinnen und Bürger zu bedenken. Dazu gehört zuerst die Einsicht, dass sowohl staatliche als auch private Identifizierungen immer erhebliche Risiken bergen. Insbesondere durch die Möglichkeit des Trackings und des Erstellens von Verhaltens- und Bewegungsprofilen ist das Recht auf informationelle Selbstbestimmung betroffen. Deshalb müssen die digitalen Räume, in denen wir uns pseudonym oder quasi-anonym ohne Angst vor Überwachung bewegen können, erhalten bleiben. Eine digitale Identität sollte nur dann zum Einsatz kommen, wenn eine Identifizierung auch wirklich erforderlich ist. Wenn die digitale Identität als bequemes Zugangsmittel genutzt werden soll, muss sie deshalb auch eine pseudonyme Nutzung unterstützen. Wenn beispielsweise eine digitale Identität zum „log-in", also zur Anmeldung, verwendet wird, darf nicht automatisch der Klarname der Person mitgeliefert werden.

Gut gemachte digitale Identitäten können dann sogar datenschutzfreundlicher als analoge Ausweise sein. So ist es mit „Selective Disclosure", also selektiver Offenlegung von Daten beispielsweise möglich, nur einzelne Datenfelder zu teilen. Wenn nur der Nachweis des Wohnorts benötigt wird, muss nicht der gesamte Ausweisinhalt mitgeschickt werden. Sogenannte „Zero-Knowledge-Proofs" gehen noch einen Schritt weiter und ermöglichen, dass die digitalen Identitäten nur Fragen beantworten, ohne überhaupt ein Datum preiszugeben. Soll kontrolliert werden, ob eine Person volljährig ist, beantwortet die digitale Identität nur genau diese Frage mit „ja" oder „nein", ohne das Geburtsdatum zu nennen. Gute eID-Systeme sollten Selective Disclosure und Zero-Knowledge-Proofs beherrschen.

Tatsächlich steht uns in Deutschland bereits ein datenschutzfreundliches eID-System zur Verfügung. Hierbei handelt es sich um die bekannte Onlineausweisfunktion des Personalausweises, des elektronischen Aufenthaltstitels und der eID-Karte für Bürgerinnen und Bürger aus EU-Mitgliedstaaten (im Nachfolgenden beziehen sich Aussagen zum Ausweis immer auf alle drei technisch identisch ausgestatteten Dokumente). Mit einem geeigneten Smartphone oder einem Kartenleser können die mit einem Chip ausgestatteten Ausweise genutzt werden, um Identitäten online rechtssicher nachzuweisen. Das System ist datenschutzfreundlich und sicher. Leider ist der Einsatz des Ausweises noch nicht flächendeckend verbreitet. Die geringe Verbreitung in der Bevölkerung dürfte vor allem mit den geringen Anwendungsmöglichkeiten, den Kosten für die teilnehmenden Stellen und fehlender Werbung zu tun haben.

3.4.1 Deutsches EUDI-Wallet

Die Europäische Union reformiert die Verordnung für elektronische Identifizierungssysteme (eIDAS). Mitgliedsstaaten sollen ihren Bürgerinnen und Bürgern elektronische Brieftaschen (Wallets) zur Verfügung stellen, mit denen sie Nachweise aus allen Lebensbereichen verwalten können. Ich berate die Bundesregierung bei ihren Planungen zur deutschen EU-Wallet im Sinne einer bürgerrechtsfreundlichen Umsetzung.

Wallets oder digitale Brieftaschen gehen einen Schritt weiter als reine eID-Systeme. Mit ihnen sollen auch Nachweise und Attribute, die über Identitätsdaten hinausgehen, vorgehalten und für Dienstleistungen im Digitalen vorgelegt werden können. Dann sollen in einer App nicht nur der Ausweis, sondern auch beliebige andere Attribute abgelegt werden können: Beispielsweise Fahrerlaubnis, Zugangsberechtigungen und Zeugnisse, aber auch Mitgliedschaften oder Konzerttickets.

Ich berate die Bundesregierung zu einer nationalen Umsetzung der sogenannten European Digital Identity-Wallet (EUDI-Wallet). Bei der EUDI-Wallet handelt es sich um eine digitale Brieftasche, die nach einheitlichen europäischen Vorgaben ausgestaltet werden soll. Nach der Reform der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) müssen die Mitgliedsstaaten solche Digital-Identity-Wallets anbieten, die grenzüberschreitend nutzbar sind.

Ich begrüße, dass die Bundesregierung die für die Wallet notwendige Infrastruktur auf dem vorhandenen eID-System des Personalausweises aufbauen will. Somit kann dessen datenschutzfreundliche Technik auch hier genutzt werden. Gleichzeitig kann über die neue Einbettung in die App die Bekanntheit dieser Technologie gesteigert werden. Auf technisch und regulatorisch Erprobtes zu bauen, ist vor dem Hintergrund, dass eIDs

de facto eine staatliche Basisinfrastruktur darstellen, ein sehr sinnvoller Schritt.

Mit einer Wallet erhalten Nutzende mehr Hoheit über Nachweise und Attribute, da diese an einer Stelle unter ihrer Kontrolle vorgehalten werden. Allerdings führt der Ansatz, dass Betroffene selbst ihre Daten verwalten, allein noch nicht zu einem sicheren System, das die Rechte von Bürgerinnen und Bürgern schützt. Es muss auch sichergestellt sein, dass sie informiert und ohne Nachteile entscheiden können, wem sie welche Daten offenbaren. Technisch muss die Lösung so ausgereift sein, dass sie in der Lage ist, Betrug und Datenabfluss zu verhindern. Für die Wallet als Applikation müssen hohe Standards gelten und die Herausgeber müssen Verantwortung übernehmen, dass sie hinreichend sicher ist. Ein Abwälzen der Verantwortung auf die Nutzenden würde dem Vertrauen in das System schaden.

In meiner Beratung lege ich daher Wert darauf, die Spielräume, die die EU-Verordnung den Mitgliedsstaaten lässt, auszuschöpfen, um den Bürgerinnen und Bürgern Vorteile zu bringen. So muss die Wallet sowohl Selective Disclosure als auch die pseudonyme Nutzung von Anfang an sinnvoll unterstützen. Gleichzeitig müssen die neuen Funktionen von Anfang an so gestaltet werden, dass sie systemischen Schutz bieten. Beispielsweise müssen Bürgerinnen und Bürger vor unberechtigten Anfragen geschützt werden. Akzeptierende Stellen – in der Sprache der Verordnung „Relying Parties“ – geben bei ihrer Registrierung ihren Anwendungsfall und die Daten, die sie abfragen möchten, an. Die Infrastruktur muss technisch sicherstellen, dass die Relying Parties nur die zum Anwendungsfall passenden Daten abfragen. So wäre der Grundsatz der Datenminimierung, als einer der Kerngedanken des Datenschutzrechts, umgesetzt. Warum sollte eine Stelle, die nur einen Altersnachweis braucht, auch nach einem Zeugnis fragen können? Wenn diese Beschränkung nicht durch das System überwacht, sondern auf die Nutzer abgewälzt wird, werden diese regelmäßig große Mengen an irrelevanten Datenfeldern „wegklicken“ müssen. Eine Situation wie bei den Cookie-Bannern, die Nutzerinnen und Nutzer häufig in eine Einwilligung zur Datenverarbeitung drängen, sollte unbedingt vermieden werden.

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

Querverweise:

3.4.3 biometrische Identifizierung

3.4.2 Reform des Pass- und Personalausweisgesetzes

Mit dem Gesetz zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens hat der Gesetzgeber unter anderem die Verarbeitungsbefugnisse der auf dem Chip von Pässen und Personalausweisen gespeicherten Daten erweitert. Darüber hinaus hat er ein neues Verfahren zur Übermittlung von Pass- und Personalausweisfotos für die Ausweisbeantragung eingeführt und die postalische Zustellung von Ausweisdokumenten ermöglicht.

Um die Identität einer Person zu prüfen, dürfen unter anderem Polizeivollzugsbehörden die auf dem Chip eines Passes oder eines Personalausweises gespeicherten Daten auslesen. Werden die Daten anschließend für eine Folgemaßnahme benötigt, werden sie derzeit noch händisch in andere Systeme übertragen. Mit der Gesetzesänderung wurde deshalb eine elektronische Übertragung der ausgelesenen Daten in andere Datenverarbeitungssysteme ermöglicht. Entgegen meiner Empfehlung beschränken die neuen Vorschriften die elektronische Weiterverarbeitung insbesondere hinsichtlich Zweck und Dauer der Verarbeitung aber nicht. Da es sich um eine Öffnungsklausel handelt, ist der Gesetzgeber gefordert, jetzt in den bereichsspezifischen Vorschriften hinreichend wirksame Schranken einzuziehen, um zu verhindern, dass Schattendatenbanken entstehen, in denen Daten aus Identitätsfeststellungen ohne klare Zweckbindung für noch nicht absehbare künftige Verwendungen gespeichert werden.

Darüber hinaus hat der Gesetzgeber eine Vorschrift geschaffen, die es künftig allen öffentlichen Stellen ermöglichen soll, das biometrische Lichtbild aus dem Chip des Passes oder des Personalausweises auszulesen, wenn eine Vorschrift dies erlaubt und der Pass- oder Personalausweisinhaber zustimmt. Auf diese Weise könnten öffentliche Stellen beispielsweise Video-Ident-Verfahren einführen. Bis jetzt können aber nur Polizeibehörden, die Zollverwaltung sowie Pass-, Personalausweis- und Meldebehörden (bei Personalausweisen auch Steuerfahndungsstellen der Länder) das biometrische Lichtbild auslesen. Aus gutem Grund: der Personalausweis verfügt über eine Online-Ausweisfunktion, die eine sichere Identitätsprüfung bei der Abgabe elektronischer Erklärungen ganz ohne Zugriff auf das Lichtbild ermöglicht. Zudem können Live-Videobilder mittlerweile täuschend echt manipuliert werden (so genannte „deep fakes“). Eine Identitätsprüfung durch Abgleich des (vermeintlichen) Live-Videobildes einer Person mit einem Lichtbild

ist nicht zuverlässig. Der Gesetzgeber sollte daher nicht solchen öffentlichen Stellen Zugriff auf die im Chip gespeicherten Daten gewähren, die diese sensiblen Daten gerade nicht zur Erfüllung (besonders wichtiger) Aufgaben wie der Gewährleistung der öffentlichen Sicherheit benötigen.

Wer einen Pass, einen Personalausweis benötigt, hatte bislang oft die Wahl: entweder ein Foto im Bürgerbüro anfertigen zu lassen oder selbst ein Foto aufzunehmen und dieses im Bürgerbüro abzugeben. Um Manipulationen an den Lichtbildern auszuschließen, müssen Fotos, die von einem Fotografen oder an einem Fotoautomaten aufgenommen werden, von diesem künftig über einen „Cloudanbieter" elektronisch direkt an das zuständige Bürgerbüro übersandt werden. Bei den biometrischen Lichtbildern handelt es sich aber um sensible Daten, deren zentrale Speicherung in Cloudinfrastrukturen ein potentielles Angriffsziel bietet. Zu begrüßen ist deshalb, dass der Verordnungsgeber einige Vorkehrungen zum Schutz der Daten getroffen hat. Andererseits geben die Regelungen aber auch Anlass zur Kritik. Beispielsweise müssen sich Fotografen und ihre Beschäftigten künftig etwa mit der elektronischen Identität (eID)-Funktion ihres Personalausweises identifizieren, wenn sie ein Lichtbild an die Behörde übermitteln. Ihre personenbezogenen Daten werden in pseudonymisierter Form mit dem Lichtbild für mehr als 10 Jahre gespeichert. Das halte ich für unverhältnismäßig. Im Begründungstext wird außerdem angedeutet, dass die Verarbeitung der Lichtbilder durch den Cloudanbieter auf Grundlage einer Einwilligung der betroffenen Personen erfolgen soll. Es wäre sinnvoll gewesen, hierzu Regelungen in der Verordnung zu treffen, anstatt die sich daraus ergebenden Fragen der Klärung durch die verantwortlichen Stellen zu überlassen.

Wer einen Pass oder Personalausweis oder eine eID-Karte beantragt hat, musste diese(n) in der Vergangenheit im Bürgerbüro abholen oder durch eine bevollmächtigte Person abholen lassen. Künftig sollen diese Dokumente per Post zugesandt werden. Das ist zwar bürgerfreundlich, jedoch erhöht der Postversand das Risiko, dass Unbefugte in den Besitz eines solchen Ausweises gelangen. Entgegen meiner Empfehlung wurde auf hinreichende Sicherungen verzichtet. So muss sich der Empfänger der Postsendung dem Zusteller gegenüber künftig (nur) durch einen Lichtbildausweis einer Behörde oder einer öffentlich-rechtlichen Körperschaft, zum Beispiel die elektronische Gesundheitskarte oder einen Schülerausweis, ausweisen. Diese Dokumente ermöglichen aber keine sichere Identifizierung einer Person. Offen bleibt zudem, wie zu verfahren ist, wenn die Zustellung fehlschlägt. Sollte sich zeigen, dass es infolge des neuen Verfahrens gehäuft zu Verlust und Fehlzustellungen von Ausweisdokumenten kommt, wird der Verordnungsgeber nachbessern müssen.

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.

3.4.3 Biometrische Identifizierung

Während auf EU-Ebene die Regeln für elektronische Identitäten überarbeitet werden, zeigen Projekte aus dem nicht-öffentlichen Bereich die Notwendigkeit, sich Methoden zur Identifikation genau anzuschauen. Nur weil ein System Technologien nutzt, die angeblich neuartig und modern sind, ist es nicht automatisch auch geeignet, sicher oder gar grundrechtefreundlich.

Ein Beispiel, bei dem in vermeintlich datensparsamer Weise der Nachweis erbracht werden soll, ein „echter" Mensch zu sein, ist das Projekt WorldCoin von OpenAI-Gründer Sam Altman. Gelöst werden soll das vermeintliche Problem, dass die Interaktionen von natürlichen Personen nicht von Interaktionen einer KI oder anderen Bots unterscheidbar sind. Die Lösung soll in der eindeutigen biometrischen Erfassung alle natürlichen Personen der Welt liegen. Der Nachweis, ein echter Mensch zu sein, erfolgt über das Scannen der Iris und einem daraus generierten eindeutigen Code, der gespeichert wird. Dadurch soll sichergestellt werden, dass ein Mensch nur eine „WorldID" ausgestellt bekommt, auch ohne dass der Iriscode selbst Teil der „WorldID" wird. Eine solche große biometrische Datensammlung gefährdet die Grundrechte erheblich, ohne eine geeignete Lösung anzubieten.

Ich sehe die aktuellen Vorstöße zur Entwicklung globaler, biometrischer, digitaler Identitäten vor dem Hintergrund eines effektiven Schutzes der Grundrechte der Bürgerinnen und Bürger kritisch. Durch die Verwendung der besonders schützenswerten biometrischen Daten sind die damit verbundenen Risiken erheblich. Die Euro-

pean Digital Identity-Wallet (EUDI-Wallet) ist hingegen eine geeignete Lösung, die gerade entwickelt wird. Der deutsche elektronische Personalausweis ist schon bereit. Jede kommerzielle Lösung, die nicht an Grundrechten orientiert ist und etablierte Schutzmechanismen für diese unterläuft, sollte abgelehnt werden.

Digitale Identitäten, die auf der Erfassung von biometrischen Daten wie zum Beispiel der Iris oder Gesichtsscans basieren, werfen durchweg zahlreiche grundrechtliche und datenschutzrechtliche Fragen auf. Sie sind buchstäblich die fragwürdigste Lösung aus Sicht der Rechte der Bürgerinnen und Bürger. Körperliche Merkmale sind als Authentisierungsmittel in der Regel nicht besonders sicher. Dass die entsprechenden Scanner verhältnismäßig leicht zu überlisten sind, wurde in der Vergangenheit immer wieder gezeigt. Auf der anderen Seite ist die Verarbeitung von biometrischen Daten aber besonders risikobehaftet: Ein Benutzername mit Passwort kann geändert werden, ein Fingerabdruck bleibt für immer gleich. Wegen dieser lebenslänglichen Unveränderbarkeit genießen biometrische Daten deshalb völlig zu Recht besonderen rechtlichen Schutz. Sie dürfen nur unter besonderen Umständen und mit gesetzlicher Absicherung zu allgemeinen Authentifizierungszwecken eingesetzt werden, etwa im staatlichen Bereich.

Es gibt zahlreiche verfassungs- und datenschutzkonforme Lösungen für digitale Authentifizierung und Identifizierung, die gut funktionieren. Ich setze mich daher auf internationaler Ebene dafür ein, dass die Datenschutzbehörden sich mit der zentralen Frage einer guten und rechtsstaatlichen Authentifizierung in der Digitalisierung befassen und dem pauschalen Einsatz unverhältnismäßiger biometrischer Authentifizierungsverfahren entschieden entgegentreten. Davon unabhängig empfehle ich allen Menschen bei der Preisgabe von biometrischen Daten besonders sorgsam zu sein und die Risiken genau abzuwägen.

Querverweise:

3.4.1 Deutsches EUDI-Wallet

3.5 EU-U.S. Data Privacy Framework – „Privacy Shield“ Nachfolge

Am 10. Juli 2023 nahm die Europäische Kommission den Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework (EU-U.S. DPF)[27] an, der am selben Tag in Kraft trat. Knapp drei Jahre, nachdem der EuGH mit dem sogenannten Schrems II-Urteil den ehemaligen Angemessenheitsbeschluss zum „Privacy Shield“ für unwirksam erklärt hatte, gibt es damit wieder einen neuen Angemessenheitsbeschluss, der als Grundlage für die Übermittlung personenbezogener Daten aus der EU und dem EWR in die USA verwendet werden kann. Voraussetzung ist, dass die Organisationen (zurzeit hauptsächlich Unternehmen, daher im Folgenden: Unternehmen), an welche die Daten übermittelt werden, gemäß dem EU-U.S. DPF zertifiziert und auf der sogenannten „DPF“-Liste veröffentlicht sind.

Bevor der Angemessenheitsbeschluss am 10. Juli 2023 durch die Europäische Kommission angenommen werden konnte, durchlief der Beschlussentwurf seit Dezember 2022 ein formales Annahmeverfahren. Verfahrensbestandteil ist unter anderem die Einholung einer – nicht bindenden – Stellungnahme des Europäischen Datenschutzausschusses (EDSA). Wie bereits in meinem letzten Tätigkeitsbericht angekündigt (31. TB Nr. 3.3.9), habe ich mich intensiv als Berichterstatter[28] in die Erarbeitung der Stellungnahme[29] eingebracht.

Gemeinsam mit den europäischen Kolleginnen und Kollegen habe ich insbesondere überprüft, ob die Maßgaben des EuGH aus dem sogenannten Schrems II-Urteil aus dem Jahre 2020 (Rechtssache C-311/18)[30] durch die Änderungen im US-Recht effektiv umgesetzt wurden und die sonstigen datenschutzrechtlichen Anforderungen erfüllt sind. Während die datenschutzrechtlichen Grundsätze, an die sich die zertifizierten US-Unternehmen halten müssen (sog. commercial part), gegenüber den Grundsätzen, die bereits im Privacy Shield enthalten waren, keine wesentlichen Änderungen enthielten, wurden für die Überwachungstätigkeiten US-amerikani-

27 Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10. Juli 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

28 siehe Pressemitteilung BfDI 7/2023 vom 28. Februar 2023, abrufbar unter: www.bfdi.bund.de/pressemitteilungen

29 Stellungnahme 5/2023 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Schutzes personenbezogener Daten im Rahmen des Datenschutzrahmens EU-USA, angenommen am 28. Februar 2023, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en

30 Urteil des EuGH vom 16. Juli 2020, Data Protection Commissioner gegen Facebook Ireland Ltd, Maximillian Schrems, [C-311/18, ECLI:EU:C:2020:559], 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

scher Nachrichtendienste und dem damit verbundenen staatlichen Zugriff auf in die USA übermittelte Daten („Government Access“) zahlreiche neue Regelungen im US-Recht geschaffen. Diese Vorschriften adressieren die vom EuGH im Schrems II-Urteil aufgezeigten Defizite und bilden damit die wesentliche Grundlage für den Angemessenheitsbeschluss der Europäischen Kommission. Auch die Stellungnahme des EDSA zum Beschlussentwurf hat sich im Bereich Government Access auf diese neuen Regelungen konzentriert und dabei teils erhebliche Verbesserungen im Vergleich zur Vorgängerregelung Privacy Shield festgestellt. So wurde insbesondere ein zweistufiger Rechtsbehelfsmechanismus eingerichtet, über den Beschwerden von EU-Bürgern zu möglichen Überwachungstätigkeiten US-amerikanischer Sicherheitsbehörden eingereicht werden können. Einen Nachweis, dass sie tatsächlich von nachrichtendienstlichen Maßnahmen betroffen sind, müssen Beschwerdeführer dabei nicht führen.

Nach Veröffentlichung des EU-U.S. DPF habe ich zusammen mit meinen Kolleginnen und Kollegen der Datenschutzkonferenz (DSK) Anwendungshinweise zum EU-U.S. DPF[31] erstellt, um Anwendern sowie etwaigen betroffenen Personen die Funktionsweise des Frameworks sowie daraus resultierende Pflichten und Rechte in deutscher Sprache und in übersichtlicher Darstellung näherzubringen.

Funktionsweise des EU-U.S. DPF

Gemäß Kapitel V DSGVO ist die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation nur möglich, wenn die Anforderungen dieses Kapitels erfüllt sind, vorbehaltlich der Einhaltung der sonstigen Bedingungen der DSGVO. Eine Datenübermittlung gemäß Kapitel V kann vor allem auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO) erfolgen.

Bei dem Angemessenheitsbeschluss zum EU-U.S. DPF handelt es sich um einen sektoralen Beschluss. Das bedeutet, dass er nicht für die gesamten USA gilt, sondern nur für Datenübermittlungen an Unternehmen, die gemäß des EU-U.S. DPF zertifiziert sind. Um am EU-U.S. DPF teilnehmen zu können, besteht für US-Unternehmen die Möglichkeit, sich nach den Grundsätzen des EU-U.S. DPF selbst zu zertifizieren und sich damit den dort festgelegten Anforderungen zu unterwerfen. Die Zertifizierungsmöglichkeit steht Unternehmen offen, die der aufsichtsrechtlichen Zuständigkeit der Federal Trade Commission (US-Wettbewerbs- und Verbraucherschutzbehörde) oder des Department of Transportation (US-Verkehrsministerium) unterliegen. Erfolgreich zertifizierte Unternehmen werden über die sog. „DPF“-Liste, die durch das Department of Commerce (US- Wirtschaftsministerium) verwaltet wird, veröffentlicht.[32] Auf Grundlage des EU-U.S. DPF können – mit einer Ausnahme für den Bereich Presse/Medienarchive – alle personenbezogenen Daten im Anwendungsbereich des Angemessenheitsbeschlusses übermittelt werden.

Übermittlungen von personenbezogenen Daten an Unternehmen in den USA, die nicht gemäß des EU-U.S. DPF zertifiziert sind, können nicht auf den Angemessenheitsbeschluss zum EU-U.S. DPF gestützt werden, sondern bedürfen einer anderen Übermittlungsgrundlage gemäß Kapitel V DSGVO (sogenannten geeignete Garantien gemäß Art. 46 DSGVO),[33] wie zum Beispiel Standardvertragsklauseln der Europäischen Kommission.[34] Bei Verwendung dieser geeigneten Garantien ist zudem vor Übermittlung auch weiterhin ein sogenanntes Transfer Impact Assessments (TIA) erforderlich, das heißt, der Datenexporteur hat sich im Zusammenwirken mit dem Importeur davon zu vergewissern, dass durch das Recht oder die Verwaltungspraxis im Drittland die Wirksamkeit des verwendeten Übermittlungsinstrumentes nicht beeinträchtigt wird, beispielsweise durch behördliche Zugriffe auf übermittelte Daten. Für Übermittlungen an Stellen in den USA, die nicht dem Anwendungsbereich des EU-U.S. DPF unterfallen, entfaltet der Angemessenheitsbeschluss zum EU-U.S. DPF allerdings im Hinblick auf das „TIA“ dennoch Wirkung. Denn gemäß der Mitteilung der Europäischen Kommission gelten alle Schutzmaßnahmen, die im Bereich der nationalen Sicherheit in den USA implementiert worden sind, für alle auf der DSGVO basierenden Datenübermittlungen an US-Unternehmen, unabhängig vom verwendeten Übermittlungsinstrument.[35] Das bedeutet, dass – sofern

31 Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

32 Die „DPF-Liste“ ist abrufbar unter: https://www.dataprivacyframework.gov/s/participant-search

33 Erläuterungen des BfDI zur Internationen Datenübermittlung, u. a. geeigneten Garantien gem. Art. 46 DSGVO, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Internationaler_Datentransfer.html

34 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Text von Bedeutung für den EWR), abrufbar unter: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

35 s. hierzu: Questions&Answers: EU-US Data Privacy Framework der Europäischen Kommission, vom 10. Juli 2023, Question 7, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

Übermittlungen aufgrund der Übermittlungsinstrumente gem. Art. 46 DSGVO erfolgen – im Rahmen des durchzuführenden „TIA“ die entsprechende Bewertung der Europäischen Kommission des Rechts und der Behördenpraxis in den USA im Angemessenheitsbeschluss zum EU-U.S. DPF berücksichtigt werden kann.[36]

Ausblick:

Mit dem Inkrafttreten am 10. Juli 2023 handelt es sich bei dem Angemessenheitsbeschluss zum EU-U.S. DPF um geltendes EU-Recht. Der Beschluss wird nach einem Jahr von der Europäischen Kommission überprüft.[37] Diese Überprüfungen sollen unter Beteiligung von Repräsentanten des EDSA erfolgen.[38] Auch hieran werde ich mich intensiv beteiligen.

36 EDSA Information note vom 18. Juli 2023, Question 2, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-transfers-under-gdpr-united-0_en, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, S. 31, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

37 s. hierzu: Questions&Answers: EU-US Data Privacy Framework der Europäischen Kommission, vom 10. Juli 2023, Question 7, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

38 s. Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10. Juli 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), EWG.: 212, abrufbar unter: https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj

4 Gremien

4.1 Die 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 jährlich. 2023 nahm die Landesbeauftragte für Datenschutz Schleswig-Holstein, Frau Dr. Marit Hansen, diese Aufgabe wahr.

Es wurden fünf Entschließungen verabschiedet. Diese betreffen die Themen der Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz, verfassungsrechtlichen Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste, Rahmenbedingungen und Empfehlungen für gesetzliche Regulierung medizinischer Register, die Forderung nach einheitlichen Maßstäben für den Forschungsdatenschutz sowie die geplante Chatkontrolle. Weiterhin wurden vier Beschlüsse gefasst. Diese betreffen die datenschutzrechtliche Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, die Bewertung von Pur-Abo-Modellen auf Webseiten sowie zwei Positionspapiere zu cloudbasierten digitalen Gesundheitsanwendungen und zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten im Straßenverkehr. Darüber hinaus erarbeitete die DSK einen Anwendungshinweis betreffend die Übermittlung personenbezogener Daten aus der Europäischen Union an die USA.

Zu allen von der DSK bearbeiteten Themenfeldern finden Sie weitere Informationen unter www.datenschutzkonferenz-online.de. Die Schwerpunkte meiner Arbeit in der DSK im Jahr 2023 betrafen die Themenfelder Microsoft 365, Kriterien für Souveräne Clouds, die Taskforce Forschungsdaten sowie das Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten. Mein Haus ist in allen Arbeitsgruppen und Task Forces der DSK vertreten und hat mehrere Leitungsfunktionen.

4.1.1 Dialogreihe mit Microsoft zu MS 365

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

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

Bereits im Vorfeld hatte die DSK Mängel an den vertraglichen Grundlagen festgestellt. So räumt sich Microsoft im Vertrag z. B. das Recht ein, Daten der Kunden zusätzlich zur beauftragten Verarbeitung auch für eigene Zwecke, die nicht für den Betrieb notwendig sind, zu verarbeiten. Im Rahmen des Dialoges hat Microsoft dargelegt, wie die Kritikpunkte adressiert werden. Dabei konnten aus Sicht der DSK zwar einige Probleme behoben werden,

die gravierendsten bleiben aber weiterhin bestehen. Der Abschlussbericht der Arbeitsgruppe wurde im Dezember 2022 veröffentlicht und kommt zu dem Schluss, dass ein datenschutzkonformer Einsatz von Microsofts Onlinediensten auf Basis des Datenschutznachtrages vom 15. September 2022 nicht ohne weiteres möglich ist.[39]

Ende des Jahres 2022 habe ich ein Rundschreiben an die obersten Bundesbehörden verschickt. In diesem habe ich den Beschluss der DSK erläutert und auch angekündigt, dass die darin vertretene Rechtsauffassung als Bewertungsgrundlage im Rahmen meiner Aufsichtspraxis herangezogen wird.[40]

Seitdem haben sich die Rahmenbedingungen zwar geändert. Zum einen ist der neue Angemessenheitsbeschluss auf Basis des EU-US Privacy Framework in Kraft getreten. Zum anderen sichert Microsoft in der aktuellen Version des Datenschutznachtrags vom 2. Januar 2024 zu, dass große Teile der Verarbeitung nun innerhalb der EU stattfinden sollen.

An der Gesamtbewertung ändert das allerdings nichts, da die Verarbeitung personenbezogener Daten in den USA nur einer von mehreren Kritikpunkten war. Besonders problematisch ist weiterhin die Nutzung personenbezogener Daten aus der Auftragsverarbeitung für eigene Zwecke von Microsoft. Für diese Nutzung ist eine tragfähige Rechtsgrundlage notwendig. Die Prüfung einer solchen Rechtsgrundlage setzt Kenntnis über die Art der verarbeiteten Daten sowie den korrespondierenden konkreten Zweck der Verarbeitung voraus. Auf Grundlage des aktuellen Datenschutznachtrages vom 1. Januar 2023 lässt sich diese Prüfung auch weiterhin nicht abschließend durchführen.

Verantwortliche, die Microsoft 365 einsetzen wollen, stehen in der Pflicht, die datenschutzkonforme Nutzung nachzuweisen, zum Schutz der nutzenden Mitarbeiter, aber auch zum Schutz der mit MS 365 bearbeiteten Inhalte, die personenbezogene Daten Dritter enthalten können. Solange Microsoft die hierfür notwendige Transparenz nicht herstellt, bleibt unklar, was mit den Daten geschieht. Damit ist eine datenschutzkonforme Nutzung meiner Auffassung nach auch weiterhin nicht regelmäßig möglich.

4.1.2 Kriterien für Souveräne Clouds

Souveräne Clouds sollen die digitale Souveränität von Cloud-Anwendenden stärken und ihre Abhängigkeit von einzelnen Cloud-Anbietenden reduzieren. Letztlich handelt es sich dabei bisher aber primär um einen Marketingbegriff, der – durch die Anbietenden selbst definiert – keine verbindlichen Rückschlüsse auf das eigentliche Angebot zulässt. Eine Task Force der DSK hat daher auf meine Initiative hin ein Positionspapier erarbeitet, in dem der Begriff der Souveränen Cloud anhand von Kriterien betrachtet, die Verantwortlichen und Anwendenden bei der Wahl der genutzten Cloud-Dienste unterstützt.

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

Auf meine Initiative hin wurde auf der 103. DSK im März 2022 die Task Force Souveräne Cloud eingerichtet. Sie hatte zunächst das Ziel, den Begriff der souveränen Cloud aus einer neutralen Position heraus zu definieren, eine Abgrenzung von anderen Cloudangeboten vorzunehmen und Kriterien festzulegen, die eine Cloud erfüllen muss, um als souverän zu gelten. Das Ergebnis ist ein Positionspapier, das Kriterien für souveräne Clouds aus der Sicht des Datenschutzes formuliert und dessen Veröffentlichung auf der 105. DSK im Mai 2023 beschlossen wurde. Zentrale Prämissen sind dabei, dass die Rechte und Freiheiten der betroffenen Personen im Kontext der Verarbeitung ihrer personenbezogenen Daten im Mittelpunkt stehen und dass digitale Souveränität die Befolgung des anwendbaren Datenschutzrechts voraussetzt, wobei die Anforderungen selbst über eine reine Datenschutzkonformität hinausgehen. Aus meiner Sicht besonders wichtig ist dabei die Feststellung, dass in einer souveränen Cloud Verarbeitungen ausgeschlossen sind, die einzig im Interesse der Anbietenden erfolgen. Dies schließt Finanzierungsmodelle aus, in denen letzt-

39 Abschlussbericht zu Microsoft Onlinediensten, abrufbar unter https://datenschutzkonferenz-online.de/beschluesse-dsk.html
40 Rundschreiben vom 21. Dezember 2022, abrufbar unter www.bfdi.bund.de/rundschreiben

lich mit personenbezogenen Daten gezahlt wird. Eine entsprechende Zusicherung muss dabei mindestens so weit in die Zukunft wirken, dass Anwendende die Möglichkeit haben, auf ein ihre Souveränität wahrendes Cloudangebot zu wechseln. Um diese Wechselmöglichkeit überhaupt zu schaffen, ist die Nutzung offener Standards, zumindest aber die Verfügbarkeit dokumentierter Schnittstellen, unabdingbar. Diese Schnittstellen ermöglichen idealerweise auch den Austausch einzelner Komponenten des angebotenen Clouddienstes, sodass Anwendende die für sie am besten geeignete Implementierung wählen können. Möglicherweise ist dies sogar eine, bei der sie dank verfügbarer Quelltexte die Möglichkeit zum eigenen Audit haben.

Mit dem Angemessenheitsbeschluss auf Basis des EU-U.S.-Data Privacy Frameworks haben sich die rechtlichen Rahmenbedingungen für den Transfer von personenbezogenen Daten in die USA in diesem Berichtsjahr geändert. Für die erhöhten Anforderungen an ein souveränes Cloudangebot bleibt das Thema Drittlandübermittlung aber weiterhin relevant. Die Task Force stellt in ihrem Positionspapier fest: Clouds können nur dann als souverän gelten, wenn ein Drittstaateneinfluss gänzlich ausgeschlossen werden kann. Nur so kann eine effektive Rechtsdurchsetzung vertraglich vereinbarter Pflichten ultimativ gewährleistet werden. Hieraus ergeben sich aus u. a. die Anforderungen, dass sowohl alle Serverstandorte als auch der Sitz von Anbietenden souveräner Clouds und ihren Auftragsverarbeitern im Europäischen Wirtschaftsraum (EWR) liegen müssen. Damit Anwendende nicht am Ende doch wieder auf Zusicherungen angewiesen sind, müssen Anbietende ihnen die Möglichkeit zur Überprüfung der Erfüllung dieser Anforderungen bieten und aktiv an solchen mitwirken. Darüber hinaus sehe ich den Nachweis durch Zertifizierung als wirkungsvolle vertrauensbildende Maßnahme an. Mit einer solchen Cloud kann datenschutzkonformer und souveränitätswahrender IT-Betrieb gelingen.

Meine Empfehlung lautet, die im Positionspapier dargelegten Kriterien bei der Auswahl geeigneter Cloud-Angebote zu berücksichtigen. Nicht jede Cloud muss dabei souverän sein, um datenschutzkonform einsetzbar zu sein. Für Verarbeitungstätigkeiten, für die ein höheres Vertrauen in das Cloud-Angebot notwendig ist, z. B. die Verarbeitung sensibler Daten, liefern die definierten Kriterien aber einen hilfreichen Leitfaden bei der Auswahl eines geeigneten Angebotes.[41]

Querverweise:

3.5 EU-U.S. Data Privacy Framework – „Privacy Shield" Nachfolge

4.1.3 Taskforce Forschungsdaten

Die Nutzung von Gesundheitsdaten zu Forschungszwecken und die sich daraus ergebenden Vorteile werden derzeit ebenso lebhaft erörtert, wie die – angeblichen – Hindernisse, die vor allem in Deutschland zu bestehen scheinen. Der Dynamik in Diskussion und Gesetzgebung begegnet die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mit der Taskforce Forschungsdaten, die sich mit anstehenden Projekten und Vorhaben befasst und den Verantwortlichen fachliche Hinweise an die Hand gibt.

Die Taskforce Forschungsdaten wurde im November 2021 als Gremium von der DSK eingerichtet, um vor allem für Verbundvorhaben in der medizinischen Forschung mit Partnern aus verschiedenen Bundesländern als Ansprechpartner zu fungieren (31. TB Nr. 4.1.3). Die Taskforce Forschungsdaten koordiniert unter meinem Co-Vorsitz die Befassung der zuständigen Aufsichtsbehörden und ist um eine abgestimmte Bewertung aller teilnehmenden Datenschutzaufsichtsbehörden bemüht. In diesem Jahr befasste sich die Taskforce Forschungsdaten zudem mit wesentlichen Gesetzesvorhaben, wie dem Gesundheitsdatennutzungsgesetz[42] und dem angekündigten Registergesetz[43] für medizinische Register, und bereitete entsprechende Papiere[44 45 46] für die DSK vor. Die Taskforce Forschungsdaten hat für die jeweiligen Themen Arbeitsgruppen gebildet, die hierzu fachliche Bewertungen abgegeben haben. Weitere Themen der Arbeitsgruppen waren das Modul zum internationalen Datentransfer in der Mustereinwilligung

41 Positionspapier „Kriterien für Souveräne Clouds" der DSK, abrufbar unter https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf

42 BT-Drs. 20/9046, abrufbar unter https://dserver.bundestag.de/btd/20/090/2009046.pdf

43 Siehe S. 65 des Koalitionsvertrags zwischen SPD, Bündnis 90/Die Grünen und FDP, abrufbar unter: https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800

44 Stellungnahme der DSK zum Gesundheitsdatennutzungsgesetz vom 14. August 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf

45 Entschließung zur Harmonisierung der Forschungsklauseln vom 23. November 2023, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf

46 Entschließung zur Regulierung medizinischer Register vom 23. November 2023, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_medRegister.pdf

der Medizininformatik-Initiative, das neue Forschungsdatenportal Gesundheit der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. und der Europäische Gesundheitsdatenraum (EHDS-Verordnungsentwurf[47] [48]).

Querverweise:

3.1.2 Gesundheitsdatennutzungsgesetz

4.1.4 Audiovisuelle Umgebungserfassung im Rahmen von Entwicklungsfahrten

Die Autohersteller und ihre Zulieferer benötigen Rechtssicherheit bei der Entwicklung von hochentwickelten Assistenzsystemen, für die auch eine audiovisuelle Erfassung der Umgebung erforderlich ist. Mit dem DSK-Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten wird der rechtliche Rahmen abgesteckt.

Ein automatisiertes Fahrzeug muss seine Umgebung sehen und hören, um situationsabhängig steuern zu können. Für die Entwicklung zuverlässig verkehrssicherer Fahrzeuge müssen Hersteller und ihre Zulieferer in großem Umfang Entwicklungs- und Testfahrten durchführen, wobei die erfassten Audio-und Videodaten auch gespeichert und in die Entwicklungsabteilungen übertragen werden, um die für das automatisierte Fahren erforderlichen Komponenten entwickeln zu können. Zugleich bedeutet eine detaillierte Erfassung der Umgebung auch einen erheblichen Eingriff in die Grundrechte von Passanten, wenn diese zufällig an Orten oder zu Zeitpunkten erfasst werden, die sie kompromittieren könnten. Auch eine zufällige Erfassung spielender Kinder ist datenschutzrechtlich bedenklich, wenngleich gerade der Schutz dieser vulnerablen Verkehrsteilnehmer ein Grund sein kann, Entwicklungsfahrten insbesondere vor Krankenhäusern und Kinderspielplätzen durchzuführen.

Die DSK hat in einem Positionspapier festgehalten,[49] innerhalb welcher rechtlichen Rahmenbedingungen eine audiovisuelle Umgebungserfassung im Rahmen von Entwicklungsfahrten denkbar ist und dazu auch die im Verband der Automobilindustrie (VdA) vertretenen Hersteller und Zulieferer konsultiert. Aufgrund der erheblichen Eingriffstiefe in die Grundrechte von zufällig erfassten Personen besteht Einigkeit mit den Herstellern und Zulieferern, dass vor Beginn eines Entwicklungsprojekts eine Datenschutzfolgenabschätzung durchzuführen ist. Die Erfassung vulnerabler Personen soll vermieden und möglichst eine Anonymisierung durchgeführt werden, wenn die Beibehaltung des Personenbezuges nicht plausibel begründet werden kann. Eine solche Begründung könnte etwa sein, dass zum Schutz vulnerabler Verkehrsteilnehmer diese zuverlässig erkannt werden müssen bzw. eine Anonymisierung etwa durch Verpixelung oder Schwärzung die Erkennungsleistung beeinträchtigen könnte.

Soweit es allgemein, also über Entwicklungsfahrten hinaus, um eine audiovisuelle Umgebungserfassung durch automatisierte Fahrzeuge geht, setze ich mich dafür ein, dass die erfassten Daten nur unter eng zu fassenden Bedingungen aus Fahrzeugen übertragen werden dürfen und durch geeignete fahrzeugtechnische Vorschriften der Schutz vor zweckfremder Verwendung der erfassten Daten gewährleistet wird. Die Erhöhung der Verkehrssicherheit von Fahrzeugen durch Automatisierung muss mit einem angemessenen Schutz personenbezogener Daten einhergehen.

4.2 Europäischer Datenschutzausschuss

Der europäische Datenschutzausschuss (EDSA) ist eine unabhängige europäische Einrichtung mit dem Ziel, zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beizutragen und die Zusammenarbeit zwischen den EU-Datenschutzbehörden zu fördern. In meinen vorangegangenen Tätigkeitsberichten finden Sie bereits nähere Erläuterungen zu diesen Aufgaben. Meine Behörde ist als gemeinsamer Vertreter aller deutschen Datenschutzbehörden Mitglied des Ausschusses und arbeitet auch in allen Expert Sub Groups und Task Forces des Ausschusses mit. Nähere Ausführungen können über meinen Internetauftritt abgerufen werden.[50] Im Berichtsjahr hat der EDSA mit Frau Anu Talus von der finnischen Datenschutzbehörde „The Office of the Data Protection Ombudsman“ für die kommenden fünf Jahre eine neue Vorsitzende gewählt.

47 EHDS-Verordnungsentwurf, abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197

48 DSK-Stellungnahme zum EHDS-Verordnungsentwurf vom 27. März 2023, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf

49 Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten der DSK vom 27. September 2023, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Positionspapier_audiovisuelle_Umgebungserfassung.pdf

50 Informationen zum EDSA unter: https://www.bfdi.bund.de/edsa

4.2.1 Allgemeiner Bericht

Der Europäische Datenschutzausschuss (EDSA) hat im Berichtsjahr seine Arbeit an einer europaweit einheitlichen Anwendung der Datenschutz-Grundverordnung (DSGVO) weiter verstärkt. Verschiedene Leitlinien wurden angenommen und mehrere Stellungnahmen abgegeben. Auch die grenzüberschreitende Zusammenarbeit wurde weiter intensiviert. Zudem wurden fünf Verfahren der Streitbeilegung entschieden, weitere stehen an. Meine Mitarbeitenden haben sich auch in die Leitung und Koordinierung von EDSA-Gremien eingebracht.

2023 hat der EDSA seine hohe Dichte an Plenarsitzungen weiter verfestigt und insgesamt 15 Mal konferiert, im Wechsel in Form von Videokonferenzen und Präsenzveranstaltungen in Brüssel. Hinzu kommen zahlreiche Sitzungen der Arbeitsgruppen (Expert Subgroups) des EDSA.

Ein Schwerpunkt der Arbeiten lag auch in diesem Berichtsjahr auf der Erarbeitung von Leitlinien bzw. Empfehlungen nach Art. 70 DSGVO zur einheitlichen Umsetzung der DSGVO in Europa. Daneben hat der Ausschuss zahlreiche Stellungnahmen im Kohärenzverfahren (Verfahren zur Gewährleistung einer einheitlichen Anwendung der DSGVO) nach Art. 64 DSGVO angenommen und gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDSB) Stellungnahmen in Rechtsetzungsverfahren abgegeben. In meinen letzten Tätigkeitsberichten (31. TB Nr 3.3.1, 30. TB Nr. 3.2.1, 29. TB Nr. 3.2) habe ich auf erste Entscheidungen gegenüber weltweit führenden Tech-Unternehmen hingewiesen. Auch hier hat es weitere erfreuliche Entwicklungen gegeben, wobei die Geschwindigkeit der Vorlage von Entscheidungs-Entwürfen durch die jeweils federführende nationale Aufsichtsbeschwerde noch deutlich zunehmen muss.

Der EDSA hat zudem seine Strategie für die Jahre 2021 bis 2023 weiter umgesetzt. Einen Schwerpunkt bildete dabei die wirksame Durchsetzung des Datenschutzes auf europäischer Ebene bei grenzüberschreitenden Sachverhalten.

Leitlinien, Empfehlungen und Stellungnahmen/ Kohärenzverfahren

Der EDSA hat im Berichtsjahr zahlreiche Leitlinien und Stellungnahmen verabschiedet,[51] an denen ich regelmäßig als Berichterstatter oder Mitberichterstatter mitgearbeitet habe. Diese wurden im Regelfall zur Wahrung der Transparenz einer öffentlichen Konsultation unterzogen.

- Die **Leitlinien 03/2022 zu täuschenden Gestaltungsmustern in Plattformen sozialer Medien** (Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them) wurden vor allem redaktionell überarbeitet, z. B. wurde der Titel von „dark patterns“ in „deceptive design patterns“ umbenannt. Eine Übersicht mit „best practices“ wurde ergänzt, um Verantwortlichen auch Positivbeispiele zur bewussten Vermeidung von „deceptive design patterns“ mit auf den Weg zu geben.
- Die bereits verabschiedeten **Leitlinien 05/2021 zum Zusammenspiel des räumlichen Anwendungsbereichs nach Art. 3 und den Vorschriften über den internationalen Datentransfer nach dem Kapitel V der DSGVO** (Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR) wurden nach öffentlicher Konsultation mit begrifflichen Klärungen (insb. einer Definition des Begriffs der „Übermittlung“ in Art. 44 DSGVO) und weiteren Beispielen verabschiedet.
- Die bereits verabschiedeten **Leitlinien 07/2022 für Zertifizierungen als Instrument für Drittstaatenübermittlungen** (Guidelines 07/2022 on certification as a tool for transfers) wurden nach öffentlicher Konsultation bestätigt. Eine wesentliche Änderung aus der öffentlichen Konsultation betrifft die Pflichten des Datenexporteurs. Dieser muss das Bestehen einer Zertifizierungsvereinbarung zwischen dem Datenimporteur und der Zertifizierungsstelle nicht prüfen.
- Die **Leitlinien 9/2022 der Leitlinien zu Datenpannenmeldungen** (Guidelines 9/2022 on personal data breach notification under GDPR) wurden dahingehend angepasst, dass die Existenz eines Vertreters in der EU nicht ausreicht, um in den Genuss des One-Stop-Shop-Mechanismus zu kommen. Vielmehr muss ein Verantwortlicher ohne eigene Niederlassung in der EU über seinen Vertreter mit der Aufsichtsbehörde jedes Mitgliedsstaates in Kontakt treten, in dem er Geschäfte betreibt, in Deutschland gegebenenfalls mit allen 16 für den Privatsektor zuständigen Landesdatenschutzbehörden.

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

- Die bereits verabschiedeten **Leitlinien 01/2022 zu den Rechten der betroffenen Personen – Recht auf Auskunft** (Guidelines 01/2022 on data subject rights – Right of access) wurden nach Durchführung einer öffentlichen Konsultation redaktionell überarbeitet.
- Die **Leitlinien 08/2022 zur Identifizierung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragverarbeiters** (Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority) wurden punktuell in Überarbeitung des Dokuments WP244 rev.01 verabschiedet. Die öffentliche Konsultation hat zu keinen Änderungen dieser Leitlinien geführt.
- Die bereits verabschiedeten **Leitlinien 05/2022 für den Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung** (Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement) betreffen inhaltliche Änderungen nach der öffentlichen Konsultation. Aspekte der menschlichen Intervention, der Rechenschaftspflicht und zu Risiken betreffend das Recht auf ein faires Verfahren sowie die Unschuldsvermutung wurden angepasst.
- Die bereits verabschiedeten **Leitlinien 03/2021 zur Anwendung des Art. 65 Abs. 1 lit. a) DSGVO** (Guidelines on the application of Art. 65(1) (a) GDPR) wurden ebenfalls im Anschluss an eine öffentliche Konsultation angenommen. Die Leitlinien zielen darauf ab, die wichtigsten Phasen des Verfahrens nach Art. 65 DSGVO (sog. Streitbeilegungsverfahren) zu beschreiben und die Zuständigkeit des EDSA beim Erlass einer rechtsverbindlichen Entscheidung auf der Grundlage von Art. 65 Abs. 1 lit. a) DSGVO zu erörtern.
- Die **Leitlinien 04/2022 zur Berechnung von Bußgeldern** (Guidelines 4/2022 on the calculation of administrative fines) beinhalten eine fünfstufige Methodik als Ausgangspunkt für die Berechnung einer Geldbuße. Hierbei werden die Anzahl der sanktionierbaren Verhaltensweisen, erschwerende oder mildernde Faktoren, die gesetzlichen Höchstbeträge für Geldbußen sowie die Anforderungen der Wirksamkeit, Abschreckung und Verhältnismäßigkeit berücksichtigt.
- Die **Leitlinien 01/2023 zu Art. 37 JI-Datenschutz-Richtlinie** (Guidelines 01/2023 on Article 37 Law Enforcement Directive) erörtern insbesondere näher die Voraussetzungen „geeigneter Garantien" im Kontext der Drittstaatenübermittlung durch Strafverfolgungsbehörden, wobei das in der EU gewährleistete Schutzniveau durch die Übermittlung personenbezogener Daten in ein Drittland nicht untergraben werden darf. Bei der Erstellung des Entwurfs wurden die Maßstäbe der „Schrems"-Rechtsprechung des EuGH (29. TB Nr. 4.3) für die Bereiche der Polizei und der Justiz entsprechend herangezogen.
- Die **Leitlinien 02/2023 zum technischen Geltungsbereich des Art. 5 Abs. 3 e-Privacy-Richtlinie** (Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive) behandeln eine technische Analyse der Anwendbarkeit von Art. 5 Abs. 3 der ePrivacy Directive, der im nationalen Recht in § 25 Abs. 1 Telekommunikation-Telemedien-Datenschutz-Gesetz umgesetzt wurde. Die Norm reagiert auf neue Tracking-Methoden, die bisherige Tracking-Instrumente (wie etwa das Setzen von Cookies) ablösen und die zugleich neue Geschäftsmodelle schaffen.

Im **Kohärenzverfahren** hat der EDSA – wie in den vergangenen Jahren – zahlreiche Stellungnahmen verfasst.[52] Mit dem Kohärenzverfahren kann der EDSA wie eine Art Clearing-Stelle Stellungnahmen abgeben oder Beschlüsse fällen und so Uneinigkeiten zwischen den Aufsichtsbehörden der Mitgliedstaaten bei der Anwendung der DSGVO im Einzelfall entgegenwirken. Diese betreffen zum großen Teil:

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

Für den Bereich der verbindlichen internen Datenschutzvorschriften hat der EDSA die **Empfehlungen 01/2022 zum Umgang mit Zulassungsanträgen betreffend die verbindlichen Unternehmensregeln von Verantwortlichen sowie zu den dabei zu beachtenden Elementen und Grundsätzen (Art. 47 DSGVO)** (Recommendations 1/2022 on the Application for and on the elements and principles to be found in Controller Binding Corporate Rules [Art. 47 GDPR]) erlassen. Sie dienen dem Ziel, gleiche Wettbewerbsbedingungen für alle Verantwortlichen als BCR-Antragsteller zu gewährleisten.

Im Rahmen der **Konsultation in Rechtsetzungsverfahren** prägen zwei gemeinsame Stellungnahmen des EDSA und des EDSB die Arbeit:

52 Stellungnahmen des EDSA, abrufbar unter: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en

→ Die **Gemeinsame Stellungnahme 01/2023 des EDSA und des EDSB zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensvorschriften für die Durchsetzung der DSGVO** (EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of the GDPR) reagiert auf die wichtige Initiative der Europäischen Kommission, mit welcher das Verfahren der Zusammenarbeit der Aufsichtsbehörden der EU-Mitgliedstaaten und des EWR effektiver und zügiger gestaltet werden soll.

Der EDSA begrüßt in der **Gemeinsamen Stellungnahme mit dem EDPS zum Vorschlag der Europäischen Kommission für eine Verordnung zur Einführung des digitalen Euro** (EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro) im Grundsatz diese Gesetzesinitiative. Er fordert allerdings unter anderem ein, dass die Grundsätze von „Datenschutz durch Technikgestaltung" und durch „datenschutzfreundliche Voreinstellungen" stärker berücksichtigt werden.

Entscheidungen in Streitbeilegungsverfahren/ Dringlichkeitsbeschluss

Der EDSA hat im Berichtsjahr zwei weitere verbindliche Beschlüsse nach Art. 65 Abs. 1 lit. a) DSGVO zu bedeutenden datenschutzrechtlichen (Streit-)Fragen in Bezug auf große soziale Netzwerke erlassen (Beschlüsse 1/2023[53] und 2/2023[54]). Zudem wies der EDSA in einem Dringlichkeitsbeschluss nach Art. 66 Abs. 2 DSGVO eine Aufsichtsbehörde an, endgültige Maßnahmen zu erlassen.[55]

Querverweise:

4.2.3 Umsetzung der EDSA-Strategie 2021–2023, 4.2.4 Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO, Nr. 4.2.7 Streitbeilegungsverfahren im EDSA, Nr. 4.2.8 Verbindliche interne Datenschutzvorschriften – Neues von den Binding Coporate Rules, Nr. 4.2.9 Wichtige Leitlinien des EDSA im Jahr 2023, Nr. 4.2.11. EDSA – neue Taskforces

4.2.2 Leitung und Koordinierung von Gremien des EDSA

Durch meine Mitarbeiterinnen und Mitarbeiter bin ich in allen Gremien des EDSA vertreten. Einige dieser Gremien werden durch meine Mitarbeiterinnen und Mitarbeiter geleitet und koordiniert. Hierbei handelt es sich um die Borders, Travel & Law Enforcement Expert Subgroup (BTLE ESG) des EDSA sowie das an den EDSA angebundene Coordinated Supervision Committee (CSC). Zudem haben meine Mitarbeiterinnen und Mitarbeiter die Koordinierung der Task Forces „Fining" und „International Engagement" übernommen.

Die **BTLE ESG** befasst sich mit datenschutzrechtlichen Themen aus den Bereichen der Grenz- und Migrationskontrolle sowie der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Die europäischen Datenschutzbehörden bündeln in der BTLE ESG ihre Beratungskompetenz zu zentralen Datenschutzfragen aus dem Sicherheits- und Strafverfolgungsbereich. In diesem Zusammenhang ist die BTLE ESG auch zuständig für Fragestellungen rund um das Thema „Government Access", d. h. dem Zugang zu übermittelten Daten durch nationale Sicherheitsbehörden in Drittländern. Die BTLE ESG wird durch zwei meiner Mitarbeitenden gemeinsam koordiniert. Von besonderer Bedeutung war im Berichtsjahr die Stellungnahme des Europäischen Datenschutzausschusses zum Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework. Die BTLE ESG hat im Rahmen dieser Stellungnahme insbesondere geprüft, unter welchen Bedingungen US-amerikanische Nachrichtendienste auf in die USA übermittelte personenbezogene Daten zugreifen können und welche Rechtsschutzmöglichkeiten dabei für betroffene Personen bestehen. Ein weiterer Schwerpunkt der Arbeiten in der BTLE ESG betraf die Leitlinien zur Auslegung von Art. 37 JI-Richtlinie, die im September 2023 verabschiedet wurden. Zudem wurden die Leitlinien 05/2022 für den Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung im Anschluss an ein öffentliches Konsultationsverfahren finalisiert.

Im **CSC** koordinieren die nationalen Aufsichtsbehörden und der EDSB ihre Aufsichtstätigkeit zu den europäischen IT-Großsystemen und bestimmten EU-Institutionen, um ein hohes und einheitliches Datenschutzniveau sicherzustellen. Der Zuständigkeitsbereich des CSC umfasst das Internal Market Information System (IMI),

53 Verbindlicher Beschluss 1/2023 zu Meta Platforms Ireland Limited, abrufbar unter: https://edpb.europa.eu/system/files/2024-01/edpb_bindingdecision_202301_ie_sa_facebooktransfers_de_0.pdf

54 Verbindlicher Beschluss 2/2023 zu TikTok Technology Limited, abrufbar unter: https://edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf

55 Dringlicher Verbindlicher Beschluss zu Meta Ireland Limited, abrufbar unter: https://edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf

Europol, Eurojust, die Europäische Staatsanwaltschaft und seit März 2023 auch das Schengener Informationssystem (SIS). Künftig werden noch etliche weitere Systeme vom CSC abgedeckt werden. Hierzu zählen sowohl bereits bestehende Systeme, etwa das Visa-Informationssystem (VIS), als auch neue Systeme wie zum Beispiel das Einreise-/Ausreisesystem (EES), das Europäische Reiseinformations- und -genehmigungssystem (ETIAS) und das Europäische Strafregisterinformationssystem für Drittstaatsangehörige und Staatenlose (ECRIS-TCN) sowie der EU-Interoperabilitätsrahmen. Der stellvertretende Vorsitz des CSC wird durch einen meiner Mitarbeitenden wahrgenommen. Ein Schwerpunkt der Aktivitäten des CSC im Jahr 2023 lag auf der Übernahme und Fortführung von Aktivitäten der vorherigen Koordinierungsgruppe des SIS II, etwa mit der Verabschiedung der Hilfestellung zur Ausübung von Betroffenenrechten. Ein weiterer Fokus lag darauf, eng abgestimmte Kontrollen und Informationsbesuche z. B. im Bereich von Übermittlungen an Europol oder im Bereich der Europäischen Staatsanwaltschaft zu etablieren. Das CSC hat sich darüber hinaus als wichtiges Forum zum Austausch von Informationen und Erfahrungen sowie zur Diskussion auch von systemübergreifenden Fragestellungen bewährt.

Die **Task Force Fining** berät den EDSA bei der Auslegung der unmittelbar anzuwendenden Bußgeldvorschriften der DSGVO und der Angleichung der Bußgeldpraxis in den einzelnen Mitgliedstaaten. Auf Wunsch unserer Schwesterbehörden aus den anderen Mitgliedsstaaten hat der Sitzungsvertreter des BfDI die Funktion als einer der beiden gemeinsamen Co-Koordinatoren der Task Force übernommen. Für die Datenschutzaufsicht ist bedeutsam, dass in der Bußgeldpraxis keine signifikanten Abweichungen in der Anwendung der DSGVO entstehen, denn diese könnten zu einem sog. „forum-shopping" oder Wettbewerbsverzerrungen führen. Die oben angesprochenen Leitlinien 04/2022 zur Berechnung von Geldbußen konnten 2023 finalisiert und zum Jubiläum der DSGVO vom EDSA beschlossen werden. Sie sind ein wichtiger Schritt hin zu einer unionsweiten Angleichung der Bußgeldpraxis. Zugleich müssen Erfahrungen zu ihrer Anwendung weiterhin ausgetauscht, verbleibende Rechtsfragen geklärt und die Leitlinien zu gegebener Zeit evaluiert werden. Die Task Force wird ihre Arbeit daher über den Erlass der Leitlinien hinaus fortsetzen.

Die **Task Force International Engagement** hat einen verbesserten Austausch im Hinblick auf internationale Angelegenheiten und eine stärkere Kooperation der EDSA-Mitglieder bei der Arbeit in diversen internationalen Gremien und Foren zum Ziel. Meine Behörde hat hier die Co-Koordinatorenschaft übernommen. Grenzüberschreitende Datenflüsse und andere datenschutzrechtliche Fragen sind mittlerweile ein zentrales Thema in den Diskussionen auf Ebene der G7, der G20, der OECD und des Europarates. Nationale Datenschutzbehörden werden allerdings nicht immer durch ihre Regierungen in diese Diskussionen miteinbezogen. Vor diesem Hintergrund und angesichts der Auswirkungen, die Diskussionen in politischen Foren auf internationale Regelungen zum Schutz personenbezogener Daten und der Privatsphäre haben können, ist eine fortwährende Kommunikation zwischen den EDSA-Mitgliedern essentiell, um ihre Stimme in internationalen Gremien und im globalen Diskurs zu verstärken.

Als Vertreter des EDSA sitzt einer meiner Mitarbeiter zudem dem unabhängigen **ETIAS-Beratungsgremium für Grundrechte** vor. Es ist bei Frontex eingerichtet und nimmt wichtige Aufgaben beim Aufbau und Betrieb des Europäischen Reiseinformations- und -genehmigungssystems wahr.

Querverweise:

3.5 EU-U.S. Data Privacy Framework – „Privacy Shield" Nachfolge, 4.2.1 Allgemeiner Bericht,4.2.9 Wichtige Leitlinien des EDSA im Jahr 2023, 4.5.4 ETIAS-Beratungsgremium für Grundrechte, 9.1.11 Europaweit koordinierte Kontrolle – Übermittlungen an Europol zu Minderjährigen im Fokus

4.2.3 Umsetzung der EDSA-Strategie 2021–2023

Neben seinen jährlichen Arbeitsprogrammen hatte der EDSA eine übergreifende Strategie für den Zeitraum von 2021 bis 2023 aufgestellt. Einen Schwerpunkt im dritten und letzten Jahr der gemeinsamen Umsetzung bildeten dabei wiederum koordinierte Mechanismen der Durchsetzung des Datenschutzes auf europäischer Ebene und eine Verstärkung der Zusammenarbeit im internationalen Bereich.

Die vier Säulen der EDSA-Strategie für den Zeitraum 2021–2023[56] sind:

1. Förderung der Harmonisierung und die Erleichterung der Rechtskonformität (Compliance),

56 Strategie des EDSA, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2021-2023_en

2. Unterstützung einer effektiven Durchsetzung und einer effizienten Zusammenarbeit zwischen nationalen Aufsichtsbehörden,
3. ein grundrechtlicher Ansatz für neue Technologien und
4. die globale Dimension.

Über die Umsetzung in den ersten beiden Jahren habe ich in meinen letzten Tätigkeitsberichten informiert (31. TB Nr. 3.3.2, 30. TB Nr. 3.2.1, 29. TB Nr. 3.2). Auch in diesem Berichtsjahr habe ich an der Umsetzung der Strategie auf nationaler wie auf europäischer Ebene mitgewirkt. Nachstehend erläutere ich Beispiele der Umsetzung in der zweiten und der vierten Säule:

Im Bereich der zweiten Säule ist vor allem die Umsetzung der sogenannten „Wishlist" des EDSA hervorzuheben. Bei der Wishlist[57] handelt es sich um eine Liste von zum Teil hinderlichen Aspekten der nationalen Verfahrensrechte, die zur Verbesserung der Durchsetzung der DSGVO auf europäischer Ebene harmonisiert werden sollten (31. TB Nr. 3.3.2) Die Europäische Kommission hat diese Wishlist erfreulicherweise aufgegriffen und einen Entwurf für eine sog. Verfahrens-Verordnung vorgelegt, mit der das Verfahren der Zusammenarbeit der Aufsichtsbehörden der EU-Mitgliedstaaten und des EWR effektiver und zügiger gestaltet werden soll. Hierzu hat der EDSA gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDSB) eine Stellungnahme[58] erarbeitet und veröffentlicht. Insbesondere halten wir mehr Fristen für die federführende nationale Behörde bei großen grenzüberschreitenden Fällen für notwendig, um schnell Entscheidungen zu erhalten.

Der EDSA hat zudem im Berichtszeitraum auf meinen Vorschlag die Umsetzung des Auskunftsrechts durch die für die Verarbeitung Verantwortlichen gemäß Art. 15 DSGVO als Thema für seine dritte koordinierte Durchsetzungsmaßnahme in 2024 beschlossen. Die koordinierten Maßnahmen erfolgen auf Basis des Beschlusses des EDSA aus Oktober 2020, einen koordinierten Durchsetzungsrahmen (Coordinated Enforcement Framework – CEF)[59] einzurichten (31. TB Nr. 3.3.3).

Eine weitere Schlüsselmaßnahme im Rahmen der Strategie für eine verbesserte Rechtsdurchsetzung stellt der im EDSA eingerichtete Expertenpool (Support Pool of Experts)[60] dar. Der unterstützende Expertenpool hat im Berichtszeitraum ein Werkzeug zur Prüfung der Datenschutzkonformität von Webseiten entwickelt (Website Auditing Tool) und hierzu eine Schulung durchgeführt (Bootcamp). Ich habe in diesem Rahmen ein eigenes Projekt initiiert und mit Beteiligung eines Experten aus dem SPE durchgeführt. Dabei wurde ein standardisierter Prüfkatalog zur Überprüfung der Nutzeroberfläche von Messenger Diensten entwickelt (Standardized Messenger Audit – Frontend), der nun als Arbeitsgrundlage für die Kontrolle von Messenger Diensten eingesetzt wird.

Im Rahmen der vierten Säule der Strategie wurde vom EDSA eine neue Taskforce „International Engagement" gegründet mit dem Ziel, den Informationsaustausch, die Diskussion und die Abstimmung im EDSA zu aktuellen Datenschutzthemen in internationalen Foren wie Europarat, GPA, G7 und OECD zu erreichen. Unter anderem soll die Task Force dazu dienen, eine gemeinsame Vorbereitung von internationalen Treffen, an denen EDSA-Mitglieder teilnehmen, zu koordinieren und die Sichtbarkeit der EU-Datenschutzaufsichtsbehörden und die des europäischen Datenschutzmodells auf internationaler Ebene zu stärken. Meine Behörde hat die Co-Koordinatorenschaft der Task Force „International Engagement" übernommen.

Die EDSA-Strategie 2021-2023 läuft zum Ende des Berichtsjahres aus. Meine Mitarbeitenden beteiligen sich aktiv im Reaktionsteam des EDSA an der Entwicklung der künftigen Strategie.

Querverweise:

4.2.4 Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO, 4.2.7 Coordinated Enforcement Action – Benennung und Stellung des Datenschutzbeauftragten, 8.4 Messengerdienste.

4.2.4 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 reagiert die Europäische Kommission auf den Wunsch des Europäischen Datenschutzausschus-

57 Wishlist des EDSA, abrufbar unter: https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf
58 Gemeinsame Pressemitteilung vom 26. September 2023, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2023/15_grenz%C3%BCberschreitende-Sachverhalte-DSGVO.html
59 Beschluss des EDSA vom 20. Oktober 2020, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en
60 Dokument zu Support Pool Experts vom 15. Dezember 2020, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-terms-reference-edpb-support-pool-experts_en

ses (EDSA) nach einer Harmonisierung nationaler Verfahrensregeln und einer Verbesserung der Zusammenarbeit unter den Aufsichtsbehörden in grenzüberschreitenden Fällen. Das Vorhaben ist sehr zu begrüßen, gleichzeitig sind Nachbesserungen am Entwurf nötig, um die Rechte der Bürgerinnen und Bürger aus der DSGVO in grenzüberschreitenden Fällen wirksam zu schützen.

Die Europäische Kommission hat am 4. Juli 2023 ihren Vorschlag für eine „Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679" („VVO") vorgelegt. Dies ist eine unmittelbare Reaktion auf die sogenannte Wiener Erklärung des EDSA, mit der eine Verbesserung der Zusammenarbeit bei der Durchsetzung des Datenschutzes in der EU[61] (31. TB Nr. 3.3.2) bezweckt wird. Der Vorschlag greift dabei viele der vom EDSA identifizierten Aspekte auf, insbesondere die Problematik unterschiedlicher nationaler Verfahrensrechte der Mitgliedsstaaten. Dazu sollen zur Verbesserung der Durchsetzung der DSGVO auf europäischer Ebene einzelne Aspekte des Verfahrensrechts harmonisiert werden.[62]

Die VVO zielt zudem darauf ab, ergänzende Verfahrensregeln zur Verbesserung der Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden bei der Durchführung von Kooperations- und Kohärenzverfahren gemäß Kapitel VII der DSGVO einzuführen. Zudem sollen die Verfahrensrechte der Parteien in grenzüberschreitenden Verfahren festgelegt und harmonisiert sowie Regeln für die Beteiligung der Beschwerdeführenden am Verfahren festgelegt werden.

Das Vorhaben ist von erheblicher Bedeutung für eine bessere und zügigere Durchsetzung der DSGVO bei der Bearbeitung von grenzüberschreitenden Fällen. Dies betrifft insbesondere die vorherrschenden digitalen Geschäftsmodelle globaler Tech-Konzerne, die die Grundrechte einer Vielzahl von Bürgerinnen und Bürgern der EU berühren. Ich habe deshalb intensiv an der Stellungnahme der DSK[63] sowie der gemeinsamen Stellungnahme des EDSA und des EDSB[64] zur VVO mitgearbeitet.

Die VVO bedarf erheblicher Nachbesserung, um die in ihr definierten Ziele zu erreichen und die Rechte der Bürgerinnen und Bürger effektiv zu schützen:

- Die VVO muss der **Verfahrensbeschleunigung** dienen. Teilweise sind Beschwerden von 2018, also aus dem Jahr, als die DSGVO wirksam wurde, noch nicht endgültig entschieden. Zwar sieht der Entwurf eine zu begrüßende frühzeitige Beteiligung der betroffenen Aufsichtsbehörden durch die federführende Aufsichtsbehörde vor. Allerdings fehlt ein verbindlicher Zeitplan mit Vorgaben für die einzelnen Verfahrensschritte der federführenden Aufsichtsbehörde.
- Die VVO sollte den betroffenen Aufsichtsbehörden **mehr Einfluss auf die federführende Aufsichtsbehörde** ermöglichen. Der Entwurf schafft in Bezug auf Fristen und Antragsrechte ein Ungleichgewicht zu Lasten der betroffenen Aufsichtsbehörden. Ich bin der Meinung, dass bereits in einem frühen Verfahrensstadium ein Konsens mit den betroffenen Aufsichtsbehörden auch in Bezug auf rechtliche Bewertungen gefunden werden sollte. Die Erfahrung mit den bisher getroffenen Entscheidungen zu den Datenverarbeitungen der großen Tech-Konzerne zeigt, dass es erst die Zuarbeit und der Druck der betroffenen Aufsichtsbehörden, darunter gerade auch mein Haus, war, die überhaupt zu einer Durchsetzung europäischen Datenschutzrechts geführt hat.
- Die VVO muss **für mehr Rechtssicherheit und Rechtsklarheit** sorgen. Manche Verfahrensschritte, wie z. B. die „gütliche Einigung" oder die Frage der formellen Einlegung der Beschwerde über ein harmonisiertes Formular, sind nur in Ansätzen ausgestaltet und werfen Fragen der praktischen Umsetzung auf oder stellen unnötige Hürden bei der Beschwerde-Einlegung (z. B. Unterschrift) dar. Zur Rechtsklarheit trägt auch **Transparenz** bei.

Nun ist es am Europäischen Parlament und dem Rat der EU, die VVO voranzubringen. Die Europäische Kommission möchte das Gesetzgebungsverfahren noch vor der Europawahl im Juni 2024 abschließen. Ich werde den Gesetzgebungsprozess weiter intensiv beobachten und mich für die nötigen Verbesserungen einsetzen. Nur durch schnelle und verstärkte gemeinsame Rechtsdurchsetzung und Kooperation können die Grundrechte der Bürgerinnen und Bürger effektiv geschützt werden.

---

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

62 Wishlist des EDSA, abrufbar unter: https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf

63 Stellungnahme der DSK vom 1. September 2023, abrufbar unter: https://datenschutzkonferenz-online.de/media/st/2023_09_01_DSK_Stellungnahme_KOM_E_VVO.pdf

64 Pressemitteilung 15/2023, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2023/15_grenz%C3%BCberschreitende-Sachverhalte-DSGVO.html

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.

Querverweise:

4.2.3 Umsetzung der EDSA-Strategie 2021–2023

4.2.5 Simplification Procedure

Im Rahmen eines Verfahrens zur Vereinfachung des Kooperationsverfahrens (Simplification Procedure) verabschiedeten die Aufsichtsbehörden des Europäischen Datenschutzausschusses (EDSA) ein einheitliches Beschwerdeformular und einen neuen „Reviewer-Prozess", um die Zusammenarbeit der Aufsichtsbehörden im Verfahren der Zusammenarbeit und Kohärenz effektiver zu gestalten.

Im April 2022 vereinbarten die Aufsichtsbehörden des EDSA in Wien Absprachen[65] zu einer Verbesserung der Zusammenarbeit bei der Durchsetzung des Datenschutzes auf europäischer Ebene. Auf diese Weise sollte die Durchsetzung der DSGVO einheitlicher, effektiver und konsistenter erfolgen. Einen Teil dieser Absprachen hat der EDSA im Jahr 2023 unter dem Begriff „Simplification Procedure" umgesetzt.

Zur Umsetzung eines Teilziels stimmten sich die Aufsichtsbehörden über die Verwendung eines einheitlichen Beschwerdeformulars und einer einheitlichen Eingangsbestätigung für betroffene Personen ab. Die Dokumente sollen die Einreichung von Beschwerden bei allen Aufsichtsbehörden vereinfachen und diesen den Informationsaustausch erleichtern. Sie können in vielen verschiedenen Szenarien verwendet werden, auch von Vertretern der betroffenen Personen. Zudem haben sie genug Flexibilität, um auf die individuellen Gesetze und rechtlichen Bedürfnisse der einzelnen Mitgliedstaaten einzugehen und entsprechend angepasst zu werden. Ich habe diesen Prozess über die zuständige Unterarbeitsgruppe unterstützt.

Weiterhin wurde ein Prozess vereinbart, der die Bearbeitung grenzüberschreitender Fälle straffen soll. In grenzüberschreitenden Verfahren legt die federführende Aufsichtsbehörde nach Abschluss ihrer Ermittlungen einen Entscheidungsentwurf vor. Gegen diesen kann jede betroffene Aufsichtsbehörde einen maßgeblichen und begründeten Einspruch einlegen. Wenn die federführende Aufsichtsbehörde einen Entscheidungsentwurf bereitstellt, müssen demzufolge alle interessierten Behörden diesen Entwurf eigenständig im Hinblick auf einen möglichen Einspruch prüfen und bewerten. Der neue Prozess sieht die Möglichkeit der vorgelagerten Prüfung und Bewertung des Entwurfes durch „Reviewer-Teams" vor, sodass ein Kreis ausgewählter Behörden auf freiwilliger Basis den Entwurf bearbeitet und ihr Ergebnis den anderen Behörden zur Verfügung stellt. Diese können sich dann, um über einen Einspruch zu entscheiden, an der Ausarbeitung des „Reviewer-Teams" orientieren. Hierzu startete in 2023 eine Pilotphase.

Sowohl das einheitliche Beschwerdeformular als auch der „Reviewer-Prozess" könnten noch durch die von der Europäischen Kommission vorgeschlagene neue sogenannte Verfahrensverordnung verändert werden. In diesem Zusammenhang plant die Europäische Kommission beispielsweise ebenfalls ein harmonisiertes Beschwerdeformular für betroffene Personen. Die genauen Auswirkungen der Ergebnisse auf die Zusammenarbeit der Aufsichtsbehörden des EDSA werden sich erst bei der praktischen Anwendung zeigen. Ich bin zuversichtlich, dass sie uns dabei unterstützen werden, eine effektive und harmonisierte Durchsetzung der DSGVO sicherzustellen.

Querverweise:

4.2.4 Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO

4.2.6 Coordinated Enforcement Action 2023 – Benennung und Stellung des Datenschutzbeauftragten

Auch in diesem Jahr arbeiten die europäischen Datenschutzaufsichtsbehörden gemeinsam bei der Rechtsdurchsetzung im Rahmen des Coordinated Enforcement Framework (CEF). Das Thema ist diesmal „Benennung und Stellung des Datenschutzbeauftragten".

Zur Umsetzung der EDSA-Strategie 2021–2023 führen die Europäischen Aufsichtsbehörden jährlich gemeinsame Durchsetzungsmaßnahmen (Coordinated Enforcement Action – CEA) im Rahmen des Coordinated Enforcement

65 Stellungnahme des EDSA zur Durchsetzungszusammenarbeit vom 28. April 2022, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-enforcement-cooperation_en

Framework (CEF) durch. Im letzten Jahr arbeitete meine Behörde bei der ersten gemeinsamen Durchsetzungsmaßnahme mit, deren Thema die Nutzung cloudbasierter Dienste im öffentlichen Sektor war. In diesem Jahr fand die zweite CEA mit dem Thema „Benennung und Stellung des Datenschutzbeauftragten“ statt.

Mit der DSGVO wurde ein EU-einheitlicher rechtlicher Rahmen für die Institution des Datenschutzbeauftragten in öffentlichen und nichtöffentlichen Stellen geschaffen. Hierdurch ist die herausgehobene kontrollierende und beratende Aufgabe des Datenschutzbeauftragten in einer sich technologisch und medial ständig verändernden Welt europaweit gesetzlich normiert worden.

Für die deutsche Datenschutzpraxis bedeutete dies keine wesentlichen Neuerungen, denn mit dem Rechtsinstrument des Datenschutzbeauftragten stehen den Behörden, den Unternehmen und der interessierten Öffentlichkeit bereits seit Jahrzehnten kompetente und verantwortungsbewusste Ansprechpartner zur Verfügung. Diese wertvollen Erfahrungen hatte Deutschland bereits bei den Beratungen zur DSGVO aktiv eingebracht.

Mit der Vereinheitlichung des europäischen Rechtsrahmens ist auch im Austausch zwischen den europäischen Mitgliedstaaten die Rolle des Datenschutzbeauftragten weiter in den Fokus der Aufmerksamkeit gerückt, so dass es konsequent war, seitens des Europäischen Datenschutzausschusses (EDSA) die Benennung und Stellung des Datenschutzbeauftragten als Thema für eine koordinierte Maßnahme der europäischen Aufsichtsbehörden im Rahmen des CEF (31. TB Nr. 3.3.3) auszuwählen.

Meine Behörde und einzelne Aufsichtsbehörden der Länder haben sich an den Gesprächen im Rahmen des CEF beteiligt und über die guten Erfahrungen im Austausch mit den Datenschutzbeauftragten sowie im Hinblick auf die Bedeutung der Datenschutzbeauftragten in Behörden und Unternehmen informiert.

Im weiteren Verlauf haben die Aufsichtsbehörden der EU-Mitgliedstaaten einen Fragebogen erarbeitet, der auf freiwilliger Basis den Aufsichtsbehörden zugeleitet werden konnte mit dem Auftrag, hierzu Erfahrungen in der praktischen Arbeit zu sammeln, die Ergebnisse auszuwerten und schließlich dem EDSA hierzu zu berichten.

Deutschland hat bereits mit den Regelungen des Bundesdatenschutzgesetzes (§ 38 BDSG) und mit zahlreichen Veröffentlichungen wie der meiner Informationsbroschüre „Info 4 – Die Datenschutzbeauftragten in Behörden und Betrieben“ sowie mit Checklisten zur betrieblichen Umsetzung der Unabhängigkeit der Datenschutzbeauftragten in einigen Bundesländern detaillierte Hintergrundinformationen für die praktische Anwendung der Art. 37 ff. DSGVO erstellt, die auch genutzt werden. Daher ist seitens der deutschen Aufsichtsbehörden darauf verzichtet worden, den Fragebogen des EDSA zur praktischen Anwendung zu zirkulieren.

Ich werde die weiteren Beratungen des CEF zu diesem Thema gleichwohl weiterhin aufmerksam begleiten.

Für die dritte CEA wurde im Übrigen das Thema „Umsetzung des Auskunftsrechts durch Verantwortliche“ gewählt. Auch bei dieser gemeinsamen Maßnahme werde ich mich aktiv einbringen.

4.2.7 Streitbeilegungsverfahren im EDSA

Auch in diesem Jahr verabschiedete der EDSA verbindliche Beschlüsse in Streitbeilegungsverfahren, die Datenschutzfragen großer sozialer Netzwerke zum Gegenstand hatten (zu den Verfahren in Sachen Facebook, Instagram und WhatsApp siehe 31. TB Nr. 3.3.1).

Im Verfahren Facebook/Meta hatte die irische Datenschutzaufsichtsbehörde (DPC) im Jahr 2022 einen Beschlussentwurf vorgelegt und darin Meta Platforms Ireland Limited (Meta Irland) hinsichtlich des sozialen Netzwerkes Facebook die Datenübermittlung in die USA wegen eines Verstoßes gegen Art. 46 Abs. 1 DSGVO für die Zukunft untersagt. Gegen den Beschlussentwurf legten unter anderem die deutschen Aufsichtsbehörden mit meiner Beteiligung Einspruch ein, weil wir ihn für nicht weitreichend genug erachtet hatten.

Ferner hatte die DPC im Jahr 2022 einen Beschlussentwurf in Sachen TikTok vorgelegt, in dem verschiedene Datenschutzverstöße mit Bezug auf Minderjährige geprüft und teilweise festgestellt wurden. Auch gegen diesen Beschlussentwurf legten aus gleichen Gründen wie beim Meta-Fall die italienische Aufsichtsbehörde sowie die deutschen Aufsichtsbehörden Einsprüche ein.

In beiden Verfahren ergingen verbindliche Beschlüsse des EDSA (Verbindliche Beschlüsse 1/2023[66] und 2/2023[67]) nach Art. 65 Abs. 1 lit. a) DSGVO, in denen die DPC angewiesen wurde, weitere Datenschutzverstöße festzustellen bzw. ein Bußgeld zu verhängen.

66 Verbindlicher Beschluss 1/2023 des EDSA, abrufbar unter: https://edpb.europa.eu/system/files/2024-01/edpb_bindingdecision_202301_ie_sa_facebooktransfers_de_0.pdf

67 Verbindlicher Beschluss 2/2023 des EDSA, abrufbar unter: https://edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf

Zudem wies der EDSA in diesem Jahr zum ersten Mal in seiner Geschichte eine Aufsichtsbehörde per Dringlichkeitsbeschluss nach Art. 66 Abs. 2 DSGVO an, endgültige Maßnahmen zu erlassen. Vorausgegangen war eine einstweilige Anordnung der norwegischen Aufsichtsbehörde gegen Meta Irland, keine personenbezogenen Daten zum Zwecke verhaltensbezogener Werbung auf Grundlage von Art. 6 Abs. 1 lit. b) oder lit. f) DSGVO auf seinen sozialen Netzwerken zu verarbeiten. Da die eigentlich zuständige irische Aufsichtsbehörde hier aus Sicht des EDSA selbst nicht ausreichend tätig wurde und aufgrund der Dringlichkeit, die bereits sehr lange andauernde und exzessive rechtswidrige Datenverarbeitung zu beenden, wies der EDSA die DPC an, entsprechende endgültige Maßnahmen gegenüber Meta Irland für den gesamten Europäischen Wirtschaftsraum zu erlassen.

In allen drei Verfahren habe ich aktiv mitgewirkt und erfolgreich die Positionen der deutschen Datenschutzbehörden eingebracht.

Querverweise:

8.7 Streitbeilegung Facebook/TikTok

4.2.8 Verbindliche interne Datenschutzvorschriften – Neues von den Binding Corporate Rules

Die verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules, BCR) sind im Bereich des internationalen Datenverkehrs weiterhin ein wichtiges und gern genutztes Übermittlungsinstrument der DSGVO. Sie können von Einzelunternehmen oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, genutzt werden, um personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums an Verantwortliche oder Auftragsverarbeiter innerhalb derselben Gruppe zu übermitteln (Art. 47 DSGVO). Sie schaffen einklagbare Rechte für betroffene Personen und enthalten Verpflichtungen zur Schaffung eines Datenschutzniveaus, das im Wesentlichen dem der DSGVO entspricht.

Auch im Jahr 2023 hat der EDSA Stellungnahmen zu einer Vielzahl von BCR abgegeben, auf deren Basis diese BCR von den nationalen Aufsichtsbehörden genehmigt wurden. Auch die deutschen Aufsichtsbehörden waren in die Prüfung verschiedener BCR als sogenannter Co-Reviewer eingebunden. Dabei prüft ein i. d. R. aus der in der EU federführenden Aufsichtsbehörde (Lead Supervisory Authority) und zwei oder mehreren Aufsichtsbehörden anderer Mitgliedsstaaten bestehendes Reviewteam, im Vorfeld des EDSA-Stellungnahmeverfahrens gemäß Art. 64 DSGVO, ob die BCR genehmigt werden können. Nach der abschließenden positiven Stellungnahme des EDSA gemäß Art. 64 Abs. 1 lit. f) DSGVO können die nationalen Aufsichtsbehörden die entsprechende BCR genehmigen.

Gemeinsam mit Vertretenden der Aufsichtsbehörden der Länder befasse ich mich innerhalb der Gremien des EDSA auch mit dem BCR-Verfahren als solchem, unter anderem im Hinblick auf dessen Aktualität und Effizienz. Besonders hervorzuheben ist hier der Abschluss der Arbeiten an den sogenannten „BCR-C Referentials“ *(Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR))*[68] zur Überarbeitung der Working Paper WP 256 rev.01[69] und des dazugehörigen Antragsformulars WP 264[70] des EDSA in der finalen Version. Ziel der BCR-C Referentials ist es, Orientierungshilfen zu bieten und die notwendigen Elemente und Inhalte von Controller Binding Corporate Rules (BCR-C) zu erläutern und darzustellen, damit für Unternehmen, die BCR als Verantwortliche nutzen wollen, die Antragstellung vereinfacht wird. Die BCR-C Referentials gelten ab dem Zeitpunkt der Veröffentlichung (20. Juni 2023) für alle BCR-C Inhaber und für Antragsteller, die eine BCR-C neu beantragen wollen. In der Praxis bedeutet das, dass alle BCR-C Inhaber sowie alle BCR-C Antragsteller ihre BCR-C mit den in den Empfehlungen festgelegten Anforderungen in Einklang bringen müssen. Spätestens im Rahmen der jährlichen Aktualisierung für 2024 bei bereits verwendeten BCR-C muss die entsprechende Anpassung durch BCR-C Inhaber erfolgen.

Aktuell überarbeitet der EDSA die sogenannten „BCR-P Referentials“ für Auftragsverarbeiter (Working Document on Binding Corporate Rules for Processors – WP 257 rev.01[71]) und das dazugehörige Antragsformular WP 265[72]).

68 Recommendations 1/2022, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-12022-application-approval-and_en

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

70 Standard application form (WP 264), abrufbar unter: https://ec.europa.eu/newsroom/article29/items/623850/en

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

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

4.2.9 Wichtige Leitlinien des EDSA im Jahr 2023

Auch im Jahr 2023 hat der Europäische Datenschutzausschuss (EDSA) neben zahlreichen umfassenden und wichtigen Stellungnahmen und Empfehlungen auch verschiedene Leitlinien (Guidelines) verabschiedet. Einige davon möchte ich wegen ihres wichtigen Inhaltes sowie meiner aktiven Rolle als federführender oder Co-Berichterstatter in diesem Abschnitt darstellen und erläutern.

Leitlinien 07/2022 – Zertifizierung als Instrument für Drittlandübermittlungen

Der EDSA hat bereits allgemeine Leitlinien für die Zertifizierung die Akkreditierung veröffentlicht.[73] Die vorliegenden Leitlinien konzentrieren sich auf die spezifischen Aspekte der Zertifizierung als Instrument für Drittlandübermittlungen oder Übermittlungen an internationale Organisationen. Ein solches Instrument stellt eine sogenannte „geeignete Garantie" im Sinne des Art. 46 DSGVO dar, die für Datenübermittlungen an Drittländer benötigt wird, wenn kein Angemessenheitsbeschluss der Europäischen Kommission im Sinne des Art. 45 DSGVO vorliegt und keine der (strikt restriktiv) auszulegenden Ausnahme gemäß Art. 49 DSGVO infrage kommt. Dabei berücksichtigen die Leitlinien neben den Anforderungen der DSGVO in Kapitel V auch die Folgen des sogenannten Schrems II-Urteils für Drittlandübermittlungen.[74] Diese Vorgaben geben den Rahmen für den in diesem neuen Übermittlungsinstrument enthaltenen Ansatz einer regulierten Selbstregulierung. Dabei muss eine Balance zwischen den strengen rechtlichen Vorgaben für Übermittlungen an Drittländer und einem möglichst praxistauglichen Einsatz des Instrumentes im Markt gefunden werden. Das Ziel des Datenexporteurs ist es dabei, die Zertifizierung des Datenimporteurs im Drittland als validen Baustein im Rahmen seiner Rechenschaftspflicht für Drittlandübermittlungen heranziehen zu können. Auf Seiten des Datenimporteurs sollen geeignete Garantien ein etwaiges fehlendes (oder zumindest nicht festgestelltes) angemessenes Schutzniveau im Drittland kompensieren. Diese geeigneten Garantien müssen dabei durch verbindliche und durchsetzbare Verpflichtungen flankiert werden, die auch die Rechte der betroffenen Personen in Form durchsetzbarer Rechte und wirksamer Rechtsbehelfe sichern. Das mit der DSGVO geschaffene Instrument der Zertifizierung als Instrument für Drittlandtransfers muss sich in der Praxis noch bewähren, bislang gibt es noch keinen entsprechenden EU-weit genehmigten Zertifizierungsmechanismus.

Leitlinien 05/2021 über das Zusammenspiel von Art. 3 und Kapitel V DSGVO[75]

Der EDSA begann im April 2019 damit, das Zusammenspiel zwischen Art. 3 und Kapitel V der DSGVO zu untersuchen. Eine erste Version dieser EDSA-Leitlinie[76] wurde im November 2021 verabschiedet und zur öffentlichen Konsultation gestellt, die am 31. Januar 2022 mit einer Vielzahl von Eingaben[77] endete. Mein Haus hat sich intensiv an der Erarbeitung der endgültigen Fassung dieser Leitlinie im Drafting Team der International Transfer Expert Subgoup (ITS ESG) des EDSA beteiligt.

Grundansatz nach der DSGVO ist, dass nach der Übermittlung von personenbezogenen Daten aus der EU an ein Drittland oder an eine internationale Organisation im Hinblick auf die übermittelten Daten keine Schutzlücke entsteht, Art. 44 Satz 2 DSGVO. Dies gilt auch für Situationen, in denen die Verarbeitung unter Art. 3 Abs. 2 der DSGVO fällt, um zu vermeiden, dass der durch die DSGVO gebotene Schutz durch andere Rechtsvorschriften, denen der Datenimporteur unterliegt, untergraben werden könnte. Denn gemäß Art. 3 Abs. 2 DSGVO findet die DSGVO zwar Anwendung für Stellen (Importeure), die außerhalb der EU niedergelassen sind und Waren oder Dienstleistungen auf dem EU-Markt anbieten oder die das Verhalten von EU-Bürgern beobachten (sog. Marktortprinzip). Allerdings können diese Importeure z. B. Vorschriften ihres (Dritt-)Landes unterliegen, die staatlichen Behörden Zugriff auf diese personenbezogenen Daten ermöglichen. Ein solcher Zugriff kann über das hinausgehen, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist. Das hier entstehende Schutzrisiko für die übermittelten personenbezogenen Daten soll durch die Bestimmungen des Kapitel V

73 Alle Guidelines des EDSA sind abrufbar unter: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

74 EuGH Urteil vom 16. Juli 2020, Az. 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

75 Guidelines 05/2021 Version 2.0, abrufbar unter: https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf

76 Guidelines 05/2021 adopted for public consultation, abrufbar unter: https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf

77 Contributions GL Interplay, abrufbar unter: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en

ausgeglichen werden. Kapitel V soll den territorialen Anwendungsbereich der DSGVO nach Art. 3 insoweit ergänzen. Dieses „Zusammenspiel“ untersuchte der EDSA mit seinen Leitlinien und erläutert anhand verschiedener Beispielsfälle, die im Anhang zur Leitlinie grafisch dargestellt sind, wann Kapitel V der DSGVO zur Anwendung kommt und wann dies nicht der Fall ist, dennoch aber Schutzvorkehrungen getroffen werden müssen.

Die grundlegende Frage, die in den Leitlinien zu beantworten war, ist, wann eine Datenübermittlung an ein Drittland oder eine internationale Organisation im Sinne des Art. 44 DGSVO vorliegt. Im Sinne einer Auslegungshilfe entwickelte der EDSA drei Kriterien, anhand derer ermittelt werden kann, wann eine Übermittlung als Datenübermittlung an ein Drittland oder eine internationale Organisation zu qualifizieren ist.

Leitlinien 02/2023 zu Art. 37 JI-Richtlinie

Im September 2023 hat der EDSA Leitlinien zur Auslegung von Art. 37 JI-Richtlinie verabschiedet (Guidelines 01/2023). Die Notwendigkeit, auf EU-Ebene Orientierungshilfe für die Anwendung von Art. 37 JI-Richtlinie zu geben, wurde auch von den Mitgliedstaaten zuletzt vermehrt geäußert. An der Erstellung der Leitlinien war ich federführend beteiligt.

Art. 37 JI-Richtlinie regelt, dass personenbezogene Daten vorbehaltlich „geeigneter Garantien“ an Drittstaaten und internationale Organisationen zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten übermittelt werden dürfen. „Geeignete Garantien“ können nach der Vorschrift durch ein rechtsverbindliches Instrument geschaffen werden (Art. 37 Abs. 1 lit. a) JI-Richtlinie). Daneben ist eine Übermittlung zulässig, wenn der Verantwortliche nach einer Beurteilung aller Umstände entscheidet, dass im Drittland „geeignete Garantien“ bestehen (Art. 37 Abs. 1 lit. b) JI-Richtlinie). Spezifische Anforderungen an die „geeigneten Garantien“ legt die JI-Richtlinie jedoch nicht fest.

Die Leitlinien befassen sich daher zunächst grundsätzlich mit dem Begriff der „geeigneten Garantien“. In diesem Zusammenhang stellt der EDSA den in Art. 35 Abs. 3 JI-Richtlinie festgelegten Grundsatz heraus, wonach auch für die Drittstaatenübermittlung nach der JI-Richtlinie gilt, dass das in der EU gewährleistete Schutzniveau durch solche Übermittlungen nicht untergraben werden darf. Der EDSA schlussfolgert daraus, dass Art. 37 JI-Richtlinie für die spezifische Übermittlung ein der Sache nach gleichwertiges und damit angemessenes Schutzniveau im Drittland voraussetzt. Ich begrüße, dass damit auch bei Übermittlungen nach Art. 37 JI-Richtlinie hohe Datenschutzstandards gesichert werden.

Vor diesem Hintergrund geben die Leitlinien konkrete Hinweise zur Auslegung und Anwendung der in Art. 37 Abs. 1 JI-Richtlinie geregelten Tatbestandsalternativen. Dabei hält der EDSA rechtsverbindliche Instrumente, d. h. insbesondere bilaterale oder multilaterale Verträge, für grundsätzlich vorzugswürdig gegenüber einer vom Verantwortlichen vorgenommenen Bewertung. Ich teile diese Einschätzung, die sich auch auf die dem Verantwortlichen für eine solche Bewertung auferlegten erhöhten Dokumentations- und Rechenschaftspflichten stützen kann.

Nach der Verabschiedung der Leitlinien wurde ein Konsultationsverfahren eröffnet. Die Ergebnisse dieser Beteiligung der Öffentlichkeit lagen bei Redaktionsschluss noch nicht vor.

Leitlinien 01/2022 zum Auskunftsrecht

Im März 2023 hat der EDSA die finale Fassung der Leitlinien 01/2022 zum Auskunftsrecht angenommen.

Die erste Fassung der Leitlinien war im Januar 2021 angenommen worden (31. TB Nr. 3.3.5). Im Anschluss erfolgte eine öffentliche Konsultation. Im Rahmen der Konsultation gingen über 70 Stellungnahmen ein. Mein Haus hat sich intensiv im Drafting Team der Key Provisions Expert Subgroup (KEYP ESG) eingebracht, welches die Stellungnahmen ausgewertet und die endgültige Fassung vorbereitet hat.

Es erfolgten bei der Überarbeitung der Leitlinien in erster Linie Klarstellungen. Die Grundaussagen der Leitlinien haben sich nicht verändert (31. TB Nr. 3.3.5).

Querverweise:

3.5 EU-U.S. Data Privacy Framework – Privacy Shield Nachfolge

4.2.10 Bericht aus der Technology Expert Subgroup

In der Technology Expert Subgroup des EDSA beteiligen sich meine Mitarbeitenden an der Entwicklung von Leitlinien zu aktuellen Themen wie Child sexual abuse material (CSAM) und e-Privacy, sowie zu wichtigen Technologiethemen wie Anonymisierung und Pseudonymisierung oder Blockchain. Zusammen mit anderen Aufsichtsbehörden nimmt mein Haus zudem an einem Reallabor zum Thema Blockchain teil.

Die Arbeit der Technology Expert Subgroup des EDSA war in diesem Jahr geprägt von aktuellen Themen wie CSAM und e-Privacy sowie von wichtigen Technologiethemen wie Anonymisierung, Pseudonymisierung und Blockchain. Gerade die Themen Anonymisierung und Pseudonymisierung spielen in vielen Bereichen der For-

schung und Digitalisierung (z. B. im Gesundheitswesen) eine wichtige Rolle. Aus diesem Grunde können entsprechende Leitlinien für alle Beteiligten sehr hilfreich sein. Mein Haus hat sich hier in enger Abstimmung mit der Berliner Beauftragten für den Datenschutz und die Informationsfreiheit, die bei diesem Projekt eine führende Rolle eingenommen hat, intensiv an der Arbeit beteiligt.

Auf Einladung der Europäischen Kommission nimmt mein Haus seit Mitte des Jahres an einem Reallabor zum Thema Blockchain teil (European Blockchain Regulatory Sandbox). In diesem Rahmen 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 dieses Projekts ist es, einen Rahmen für Regulierungsbehörden, Aufsichtsbehörden und Blockchain-Innovatoren bereitzustellen, um in einen regulatorischen Dialog einzutreten und Hindernisse aus rechtlicher und regulatorischer Sicht in einem sicheren und vertraulichen Umfeld zu identifizieren. Die Anwendungsfälle der teilnehmenden Projekte umfassen dabei vor allem Anwendungen der Blockchain-Technologie jenseits von Kryptowährungen oder elektronischen Vermögenswerten. Für die teilnehmenden Aufsichtsbehörden bietet das Reallabor eine Gelegenheit, frühzeitig Einblicke in neue Anwendungsfälle der Blockchain-Technologie zu bekommen, gleichzeitig den beteiligten Firmen ein besseres Verständnis der rechtlichen Anforderungen im Zusammenhang mit ihren Projekten zu vermitteln und dazu beizutragen, dass Aspekte des Datenschutzes im Sinne des Grundsatzes „Data Protection by Design“ in den Projekten von Anfang an berücksichtigt werden.

Querverweise:

3.2.4 Verordnung zum Auffinden von Material des sexuellen Online-Kindesmissbrauchs

4.2.11 EDSA – neue Taskforces

Datenschutz, Wettbewerb und Verbraucherschutz sind in der Digitalwirtschaft eng verknüpft. Um die Zusammenarbeit der jeweiligen Aufsichtsbehörden zu fördern, hat der Europäische Datenschutzausschuss (EDSA) die Taskforce zum Zusammenspiel zwischen Datenschutz, Wettbewerb und Verbraucherschutz (TF C&C) eingerichtet. Zudem hat der EDSA zur Stärkung der internationalen Kooperation der EU-Datenschutzbehörden die neue Taskforce „International Engagement“ (TF INT) ins Leben gerufen. Hier habe ich – gemeinsam mit den französischen Kolleginnen und Kollegen – die Rolle als Co-Koordinator übernommen.

Taskforce „International Engagement“

Die fortschreitende Digitalisierung und damit einhergehende rechtliche und regulatorische Fragen sind weltweit zu einem politischen Schlüsselthema geworden. In diesem Zusammenhang nimmt der Schutz personenbezogener Daten und der Privatsphäre auch in internationalen Gremien und Foren eine immer wichtigere Rolle ein.

Grenzüberschreitende Datenflüsse und andere datenschutzrechtliche Fragen sind insoweit mittlerweile ein zentrales Thema in den Diskussionen auf Ebene der G7, der G20, der OECD und des Europarates. Allerdings werden die nationalen Datenschutzbehörden nicht immer durch ihre Regierungen in diese Diskussionen einbezogen. In einigen der eher wirtschaftsorientierten Gremien ist zudem ein Trend zu beobachten, hohe datenschutzrechtliche Standards als Hindernis für internationale Datenflüsse und damit auch als Hindernis für Innovation und wirtschaftliches Wachstum darzustellen. Diese Darstellung führt zu Herausforderungen für das europäische Datenschutzmodell und seinen globalen Einfluss.

Vor diesem Hintergrund und angesichts der Auswirkungen, die Diskussionen in politischen Foren auf internationale Regelungen zum Schutz personenbezogener Daten und der Privatsphäre haben können, hat der EDSA die neue Taskforce „International Engagement“ (TF INT) gegründet. Ziel der Taskforce ist ein verbesserter Austausch im Hinblick auf internationale Angelegenheiten und stärkere Kooperation der EDSA-Mitglieder bei der Arbeit in diversen internationalen Gremien und Foren.

Eine entsprechend fortwährende Kommunikation ist essentiell, um die Stimme der europäischen Datenschutzbehörden in internationalen Diskussionen zu verstärken. Ich freue mich daher, die Taskforce gemeinsam mit meinen Kolleginnen und Kollegen von der französischen Aufsichtsbehörde (CNIL) als Co-Koordinator zu leiten.

Taskforce zum Zusammenspiel zwischen Datenschutz, Wettbewerb und Verbraucherschutz

Die Regulierung der Digitalwirtschaft mit ihren datengetriebenen Geschäftsmodellen ist nur erfolgreich möglich, wenn Datenschutz- und Kartellbehörden sowie die Verbraucherschutzorganisationen eng zusammenarbeiten. Vor diesem Hintergrund und in Anbetracht der europäischen Rechtsetzung im Rahmen der EU-Digitalstrategie, hier speziell dem Digital Markets Act (DMA), hat der EDSA im März 2023 die Taskforce zum Zusammenspiel zwischen Datenschutz, Wettbewerb und Verbraucherschutz (TF C&C) ins Leben gerufen. Ziel der TF C&C ist es unter anderem, Best Practices für eine

effiziente Zusammenarbeit festzulegen, damit Bürgerinnen und Bürger in Europa besser vor rechtswidrigen und missbräuchlichen Datenverarbeitungen geschützt werden. Dabei kann die TF C&C auf dem Urteil des EuGHs im Verfahren „Meta“[78] aufbauen, das auf einem Verfahren des Bundeskartellamtes beruht, das mein Hamburger Kollege und ich begleitet haben. Darin werden erstmals die Erfordernisse an die Zusammenarbeit zwischen Wettbewerbs- und Datenschutzaufsichtsbehörden in der höchstrichterlichen Rechtsprechung europaweit konkretisiert. Ich freue mich, meine u. a. in diesem Verfahren gewonnenen positiven Erfahrungen in der Zusammenarbeit in Deutschland aktiv in die Arbeit der TF C&C einzubringen.

Durch die weitere Verschränkung von Wettbewerbs- und Datenschutzrecht im DMA wird auch der entsprechende Abstimmungsbedarf auf EU-Ebene einen größeren Raum einnehmen. Hier wurde der TF C&C durch den EDSA das Mandat erteilt, die gemeinsamen Standpunkte des EDSA und des EDSB für das im DMA vorgesehene Abstimmungsgremium, die High Level Group, vorzubereiten und zu konsolidieren.

4.3 Die Global Privacy Assembly

In der Global Privacy Assembly (GPA) versammeln sich über 130 Datenschutzaufsichtsbehörden aus aller Welt. Bei ihrem jährlichen Treffen werden aktuelle Fragen und Herausforderungen für den Datenschutz diskutiert.

Im Jahr 1979 trafen sich Datenschutzbeauftragte aus aller Welt zum ersten Mal in Bonn zu einer gemeinsamen Konferenz. Daraus entwickelte sich die jährlich stattfindende „Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre“, die sich 2019 in „Global Privacy Assembly“ umbenannt hat und mittlerweile mehr als 130 Mitglieder umfasst. Neben meiner Dienststelle gehören – mit Ausnahme von Baden-Württemberg und Saarland – auch alle Landesdatenschutzaufsichtsbehörden der GPA an. In den letzten Jahren gelang es der GPA, immer mehr Mitglieder aus dem „globalen Süden“, z. B. aus Afrika oder Latein-Amerika, zu gewinnen und somit ihren globalen Charakter zu unterstreichen.

Die GPA hat sich mittlerweile zu einem ganzjährig aktiven internationalen Forum weiterentwickelt, um – ihrem Hauptzweck entsprechend – eine führende Stimme in der globalen Datenschutz-Debatte zu sein. Daneben dient die GPA dem Meinungs- und Erfahrungsaustausch sowie der gegenseitigen Unterstützung ihrer Mitglieder.

Seit ihrem Beginn in Bonn habe ich die Internationale Konferenz der Beauftragten für Datenschutz und Privatsphäre bzw. die GPA unterstützt und dabei wiederholt eigene Entschließungsentwürfe eingebracht. Dies geschah auch im Berichtsjahr. Ferner wirke ich im Leitungsgremium der GPA, dem „Executive Committee“ mit.

4.3.1 Mitgliedschaft im „Executive Committee“ der Global Privacy Assembly

Seit Herbst 2020 bin ich gewähltes Mitglied im Leitungsgremium der Global Privacy Assembly (GPA), dem sogenannten „Executive Committee“ (ExCo). Dabei werden wesentliche Entscheidungen der GPA vorbereitet.

Im Herbst 2020 wurde ich auf Vorschlag der damaligen Vorsitzenden des Executive Committee der GPA, Frau Elizabeth Denham, UK Information Commissioner 2016–2021, als eines von fünf Mitgliedern in das ExCo der GPA gewählt. Zwei Jahre später, im Herbst 2022, erhielt ich ein zweites Mandat, das bis Herbst 2024 andauern wird. Gemäß den Regeln, die sich die GPA für ihre Struktur gegeben hat, wird eine weitere Verlängerung dann nicht mehr möglich sein.

Es war mir auch im Berichtsjahr ein besonderes Anliegen, die GPA als globalen Zusammenschluss von Datenschutzbehörden zu unterstützen und zu ihren Aktivitäten beizutragen. Entsprechend habe ich im „Strategic Direction Sub-Committee“ des ExCo mitgewirkt, das sich mit der Umsetzung der GPA Strategie für die Jahre 2021–2023 befasst und darüber hinaus eine neue Strategie für den Zeitraum 2023–2025 erarbeitet hat. Insbesondere bei letzterem Vorhaben habe ich mich mit inhaltlichen und verfahrenstechnischen Beiträgen eingebracht. Zudem habe ich im „Host Selection Sub-Committee“ mitgewirkt, das im Berichtsjahr für die Auswahl des Gastgebers verantwortlich war, der im Herbst 2025 die 47. GPA Jahreskonferenz ausrichten wird.

Während des Berichtsjahres war ich bis zur 45. GPA Jahreskonferenz im Oktober 2023 der einzige Vertreter einer Datenschutzbehörde aus einem G7-Land oder aus einem EU-Mitgliedstaat im ExCo der GPA. Die anderen Mitglieder stammten aus Mexico (Vorsitz), Argentinien, Marokko, Jersey, der Türkei und aus Bermuda. Vor diesem Hintergrund habe ich großen Wert daraufgelegt, EU- oder auch G7-Positionen in das ExCo und in die GPA einzubringen, z. B. im Hinblick auf die neue GPA-Strategie für den Zeitraum 2023–2025, und umgekehrt zur

78 Urteil des Europäischen Gerichtshofs vom 4. Juli 2023, Az.: C-252/21

GPA beim Europäischen Datenschutzausschuss und dessen Arbeitsgruppen zu berichten. Diese Situation hat sich im Herbst 2023 geändert, nachdem mein Kollege aus Bulgarien als neues Mitglied in das ExCo der GPA gewählt wurde.

Ich freue mich auf ein weiteres Jahr der Mitgliedschaft im Leitungsgremium der GPA, dem Executive Committee, und auf die Zusammenarbeit mit den internationalen Kolleginnen und Kollegen in diesem Gremium zur Weiterentwicklung und Stärkung der GPA und ihrer Mitglieder.

4.3.2 45. GPA Jahreskonferenz

Die Privacy Commissioner von Bermuda hat im Herbst 2023 die 45. Jahreskonferenz der Global Privacy Assembly (GPA) veranstaltet. Dabei wurden Grundsatzfragen zum internationalen Datenschutz und zu neuen Technologien besprochen. Die Pixi-Bücher und Videos meiner Dienststelle wurden mit dem „GPA Award" der Kategorie „Education" ausgezeichnet.

Die 45. Jahreskonferenz der GPA wurde vom 15. bis 20. Oktober 2023 vom Bermuda Privacy Commissioner in Hamilton, Bermuda, ausgerichtet. Mehrere hundert Teilnehmende versammelten sich dabei unter dem – vom Veranstaltungsort inspirierten – Motto „Ripples – Waves – Currents" (Riffeln – Wellen – Strömungen). Als neue Mitglieder wurden unter anderem die brasilianische Datenschutzbehörde und die Aufsichtsbehörde für Datenschutz aus Nigeria aufgenommen. Dadurch kann die GPA ihren globalen Charakter unterstreichen. Begleitet von einer kleinen Fachdelegation habe ich an der Konferenz teilgenommen und mich in verschiedenen Formaten eingebracht.

Besonders hat mich gefreut, dass mein Haus mit einem GPA Award ausgezeichnet wurde, der auf Grundlage einer Abstimmung durch die Mitglieder der GPA zuerkannt wird. Für die Pixi-Bücher und Videos meiner Dienststelle durfte ich den GPA Award der Kategorie Education entgegennehmen. Bis Ende 2023 wurden ca. 815.000 Pixi-Bücher durch Bildungseinrichtungen und einzelne Bürgerinnen und Bürger bei uns abgerufen.

Zudem habe ich erstmals ein „Side Event" im Rahmen einer GPA Jahreskonferenz durchgeführt, um auf diese Weise ein breiteres Publikum über Zielsetzung, Aktivitäten und neueste Papiere der „International Working Group on Data Protection in Technology", auch bekannt als „Berlin Group", zu informieren, deren Vorsitzender ich bin. Es hat mich zudem sehr gefreut, dass meine Kolleginnen und Kollegen im Executive Committee dem Vorschlag zugestimmt haben, den Leiter der israelischen

Privacy Protection Authority kurzfristig auf die Rednerliste der GPA Jahreskonferenz zu setzen. Ich war sehr bewegt und beindruckt von der per Videokonferenz übertragenen Rede meines Kollegen aus Israel über die besondere Lage vor Ort und darüber, wie die Behörde auch unter den aktuell erschwerten Umständen ihrem gesetzlichen und datenschutzrechtlichen Auftrag nachkommt.

Die Hauptvorträge und Diskussionsrunden in der für alle Teilnehmer offenen Sitzung konzentrierten sich auf die fortschreitenden technologischen Entwicklungen vor allem im Bereich der Künstlichen Intelligenz. Weitere Schwerpunkte waren Fragen zu grenzüberschreitenden Datentransfers und die Frage, was Datenschutzaufsichtsbehörden von anderen Aufsichtsbehörden, z. B. Wettbewerbsbehörden, lernen können; zu letzterer Frage habe ich an einer Podiumsdiskussion teilgenommen.

Eröffnet wurde die Konferenz mit einer Diskussionsrunde zur „karibischen" Perspektive des Datenschutzes; Datenschutzbeauftragte aus dieser Region, z. B. aus Barbados oder von den Bahamas, haben über ihre jeweilige Situation und ihre Aktivitäten zur Verbesserung des Datenschutzes berichtet.

In der geschlossenen Sitzung der Konferenz, zu der nur die akkreditierten Mitglieder und Beobachter der GPA zugelassen sind, berichteten die Arbeitsgruppen, der Unterausschuss für die strategische Ausrichtung und verschiedene GPA-Mitglieder und -Beobachter über bedeutende Ergebnisse und Tätigkeiten seit der letzten Jahreskonferenz im Herbst 2022. In diesem Zusammenhang konnte ich nochmals über die Arbeiten der International Working Group on Data Protection in Technology sprechen.

Darüber hinaus haben die Mitglieder der GPA folgende Entschließungen angenommen:[79]

- Entschließung zu Gesundheitsdaten und wissenschaftlicher Forschung
- Entschließung zu Künstlicher Intelligenz im Beschäftigungskontext
- Entschließung zur Erreichung globaler Datenschutz-Standards
- Entschließung zu Systemen generativer Künstlicher Intelligenz
- Entschließung zu Datenschutz aus Gender-Perspektive
- Entschließung zu einem „Privacy and Human Rights Award" der GPA
- Entschließung zu einer GPA Bibliothek

Zudem hat die GPA eine neue Strategie, gültig für den Zeitraum von der 45. GPA im Herbst 2023 bis zur 47. GPA im Herbst 2025, beschlossen.

Die nächste Jahreskonferenz der GPA wird vom Jersey Privacy Commissioner im Oktober 2024 ausgerichtet werden.

Querverweise:

4.3.1 Mitgliedschaft im „Executive Committee" der Global Privacy Assembly, 4.4.1 71. Treffen der IWGDPT Berlin Group in Rom, 4.4.3 Arbeitspapiere der Berlin Group zu – „Smart Cities" und Telemetrie veröffentlicht

4.4 International Working Group on Data Protection and Technology bzw. „Berlin Group"

Vor genau vierzig Jahren – im Jahr 1983 – wurde in Berlin die „International Working Group on Data Protection and Technology" (IWGDPT) als unabhängige Gruppe von Expertinnen und Experten gegründet. Wegen ihres Gründungsortes ist sie auch als „Berlin Group" bekannt. In ihrem Fokus steht die datenschutzfreundliche Gestaltung aktueller und zukünftiger Technologien.

Im März 2021 habe ich den Vorsitz der Berlin Group von der Berliner Beauftragten für Datenschutz und Informationsfreiheit übernommen. Nach pandemiebedingter Unterbrechung hat die Arbeitsgruppe 2022 wieder ihren gewohnten Turnus von zwei Treffen pro Jahr aufgenommen und neue Arbeitspapiere verabschiedet.

Eine besondere Eigenschaft der IWGDPT ist ihre vielfältige Zusammensetzung. Die Gruppe umfasst Expertinnen und Experten von Datenschutzbehörden aus aller Welt, aber auch aus Wissenschaft und Forschung oder von Nichtregierungsorganisationen und Denkfabriken („Think-Tanks"). Im Berichtsjahr sind auch neue Mitglieder der IWGDPT beigetreten und haben an deren Treffen und Aktivitäten teilgenommen. Dies betrifft z. B. die 2020 gegründete Datenschutzaufsichtsbehörde Brasiliens oder die Aufsichtsbehörden von Georgien, Albanien, Marokko, Kenia, der Elfenbeinküste, den Philippinen oder (Süd-) Korea. Es ist zudem gelungen, „alte" Mit-

79 Entschließungen der 45. GPA Jahreskonferenz, abrufbar unter https://www.bfdi.bund.de/gpa

glieder der Gruppe für deren Aktivitäten wieder neu zu gewinnen, z. B. aus Kanada, Dänemark oder Schweden.

Aufgrund ihrer Unabhängigkeit kann die Berlin Group ihr Arbeitsprogramm autonom bestimmen und, wenn nötig, neuen Trends oder Technologien anpassen. Der Hauptzweck der Berlin Group besteht darin, auf eine datenschutzfreundliche Ausgestaltung aktueller und künftiger Technologien hinzuwirken, z. B. durch das Prinzip „privacy by design" oder durch die Anwendung datenschutz-fördernder Technologien (Privacy Enhancing Technologies – PETs). Um die praxisorientierten Empfehlungen der Arbeitsgruppe an Unternehmen, Gesetzgeber, Datenschutzbehörden und andere Stakeholder noch gezielter und zeitgerecht vorlegen zu können, hat die Gruppe beschlossen, ihren Fokus auf solche Technologien zu setzen, die gleichzeitig Relevanz für den Massenmarkt haben und in voraussichtlich absehbarer Zeit vor dem Markteintritt stehen werden.

Mein übergeordnetes Ziel als Vorsitzender ist es, die hervorragende Expertise und die Arbeitsergebnisse der Gruppe auf globaler Ebene verstärkt bekannt zu machen sowie die Diversität und Inklusivität der Berlin Group zu stärken, um möglichst viele regionale und professionelle Perspektiven für ihre Arbeiten einzubeziehen.

4.4.1 71. Treffen der IWGDPT Berlin Group in Rom

Am 6./7. Juni 2023 fand das 71. Treffen der International Working Group on Data Protection in Technology (IWGDPT) in Rom statt. Dabei hat die Gruppe ein neues Working Paper angenommen und neue Zukunftsthemen ausgewählt.

Mehr als vierzig Mitglieder der International Working Group on Data Protection in Technology (IWGDPT) versammelten sich aus Anlass des 71. Treffens der Gruppe am 6./7. Juni in Rom auf Einladung der italienischen Datenschutzbehörde „Garante per la protezione dei dati personali", kurz Garante.

Neben der Arbeit an thematischen Papieren stand die Diskussion aktueller Fragen zu neuen Technologien und den Herausforderungen für den Datenschutz im Vordergrund. Aus aktuellem Anlass hatten die Kolleginnen und Kollegen des Garante über ihre jüngsten aufsichtsrechtlichen Aktivitäten in Bezug auf den KI-Dienstleister „ChatGPT" berichtet, insbesondere über die Hintergründe für das zeitweilige Verbot von ChatGPT in Italien.

Im Hinblick auf neue Themen hat die Gruppe nach ausführlicher Diskussion beschlossen, neue Working Papers zu „Neurotechnology" und zu „Artificial Intelligence – Large Language Models" (AI LLMs) zu erarbeiten. Es freut mich zudem, dass die IWGDPT dem von einem Experten meiner Dienststelle vorgelegten Entwurf eines Arbeitspapiers zum Thema „Telemetry/Diagnostic Data" zugestimmt hat.

Um ihren eigenen Auftrag und ihre besonderen Charakteristika zu dokumentieren, hat die Gruppe ein von mir als Vorsitz und Sekretariat erarbeitetes „Vision und Mission"-Dokument, das bereits beim vorhergehenden Treffen in London Gegenstand der Diskussion war, angenommen und verabschiedet. Darin wurde z. B. die Bedeutung der heterogenen Zusammensetzung der Gruppe hervorgehoben und ihre Fokussierung auf praxisrelevante Empfehlungen zur datenschutzfreundlichen Ausgestaltung wichtiger Zukunftstechnologien festgelegt.[80]

Querverweise:

4.4.2 72. Treffen der IWGDPT Berlin Group in Ottawa,
4.4.3 Arbeitspapiere der Berlin Group zu – „Smart Cities" und Telemetrie veröffentlicht

4.4.2 72. Treffen der IWGDPT Berlin Group in Ottawa

Zu ihrem zweiten turnusgemäßen Treffen im Berichtsjahr versammelten sich zahlreiche Mitglieder der International Working Group on Data Protection in Technology (IWGDPT) in Ottawa am 7./8. Dezember 2023. Die Gruppe hat ein Papier zum Thema Digitale Zentralbank-Währungen („Central Bank Digital Currencies") angenommen. Das Treffen in Ottawa wurde ergänzt durch ein „Privacy & Generative AI Symposium" des OPC Canada (Office of the Privacy Commissioner of Canada).

Auf Einladung des Office of the Privacy Commissioner of Canada (OPC Canada) fand das 72. Treffen der International Working Group on Data Protection in Technology (IWGDPT) am 7./8. Dezember 2023 in Ottawa statt. Durch diesen außereuropäischen Tagungsort hat die Gruppe ihren internationalen Charakter betont und neue Teilnehmerkreise erschlossen. Es freut mich, dass neue Mitglieder für die IWGDPT Berlin Group aus den Reihen der regionalen Datenschutzbehörden Kanadas gewonnen werden konnten, z. B. aus Ontario oder Nova Scotia.

In Ergänzung zu diesem Treffen der IWGDPT Berlin Group hat OPC Canada als lokaler Gastgeber ein „Priva-

80 „Vision und Mission" der IWGDPT, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/Weitere/Vision-and-Mission.html

cy & Generative AI Symposium“ organisiert, das auch zusätzlichen Teilnehmenden (Nicht-Mitglieder der IWGDPT) offenstand und auf großes Interesse stieß. In einem Impulsvortrag und drei Podiumsdiskussionen wurden die Herausforderungen, die sich aus dem raschen technologischen Fortschritt der Künstlichen Intelligenz (KI bzw. Artificial Intelligence – AI) für den Datenschutz ergeben, vertieft diskutiert und Möglichkeiten für einen grundrechtswahrenden Umgang mit KI-Anwendungen beleuchtet.

Zum „Kerngeschäft“ der IWGDPT Berlin Group gehört die Erarbeitung thematischer Papiere zu relevanten Zukunftstechnologien mit praxisorientierten Empfehlungen für eine datenschutzfreundliche Ausgestaltung solcher Technologien. Daher freut es mich sehr, dass die Gruppe bei ihrem Treffen in Ottawa in dieser Hinsicht wesentliche Fortschritte erzielen konnte: Die Gruppe hat, nach intensiver Diskussion, ein neues Papier angenommen zum Thema Digitale Zentralbank-Währungen („Central Bank Digital Currencies“), für das nun die abschließende Beratung innerhalb der gesamten IWGDPT Berlin Group im schriftlichen Verfahren („written procedure“) folgen wird. Ziel ist, dieses Papier im Frühjahr 2024 zu veröffentlichen. Ferner arbeitet die IWGDPT Berlin Group weiterhin an Papieren zu den Themen „Data Sharing“, „Neurotechnology“ und „AI Large Language Models (AI LLMs). Letzteres Papier wird dabei aufgrund der hohen Aktualität des Themas beschleunigt bearbeitet mit dem Ziel der Fertigstellung in der ersten Hälfte 2024, so dass die IWGDPT Berlin Group ihre Empfehlungen zeitgerecht abgeben kann.

In Bezug auf mögliche neue Zukunftsthemen haben die IWGDPT Berlin Group Mitglieder aus den Reihen des Europäischen Datenschutzbeauftragten (European Data Protection Supervisor) sowie des UK Information Commissioners und der französischen Datenschutzbehörde (Commission Nationale Informatique et des Libertes) die Ergebnisse ihrer jeweiligen Analysetätigkeiten vorgestellt. Auf dieser Grundlage wird die IWGDPT Berlin Group ihre Liste von Zukunftsthemen erweitern und hat – nach umfassender Diskussion – als unmittelbares nächstes Thema, dem sie sich neu widmen wird, das Thema „Immersive Technologies“ ausgewählt.

Das Sekretariat der IWGDPT Berlin Group hat anlässlich des Treffens in Ottawa die erweiterte Website der Gruppe vorgestellt. Entsprechend den Beschlüssen des vorangegangenen Treffens in Rom sind dort nun das „Vision and Mission“-Dokument der Gruppe sowie eine Liste mit teilnehmenden Delegationen für die Jahre 2014–2023 (Mitglieder-Liste) und die Tagesordnungen der seit November 2021 durchgeführten Treffen (nach meiner Übernahme des Vorsitzes) der IWGDPT Berlin Group abrufbar.[81] Die im Sommer 2023 begonnene Erarbeitung eines Logos und eines eigenen Designs für Dokumente der IWGDPT Berlin Group im Sinne einer besseren Sichtbarkeit der Gruppe wird fortgesetzt mit dem Ziel, erste Vorschläge des Vorsitzes im Sommer 2024 vorzulegen.

Das nächste bzw. 73. Treffen der IWGDPT Berlin Group wird am 18./19. Juni 2024 in Oslo stattfinden.

Querverweise:

4.4.1 71. Treffen der IWGDPT Berlin Group in Rom, 4.4.3 Arbeitspapiere der Berlin Group zu – „Smart Cities“ und Telemetrie veröffentlicht

4.4.3 Arbeitspapiere der Berlin Group zu „Smart Cities“ und Telemetrie veröffentlicht

Unter meinem Vorsitz konnten wir in der Berlin Group Arbeitspapiere zu den Themen „Smart Cities“ und Telemetrie abstimmen und veröffentlichen. Weitere Arbeitspapiere zu den Themen Gesichtserkennungstechnologie, Digitales Zentralbankgeld, Neurotechnologie und Künstliche Intelligenz werden folgen.

Im Berichtsjahr hat die Berlin Group unter meinem Vorsitz Arbeitspapiere zu den Themen „Smart Cities“ und Telemetrie veröffentlicht. Die Arbeitspapiere sind in englischer Sprache verfasst und stehen auf meiner Website zum Download bereit.[82]

In „Smart Cities“ können Bewohner und Besucher von verbesserten Diensten profitieren, wie etwa einer intelligenten Verkehrssteuerung oder einer intelligenten Verwaltung der städtischen Ressourcen. Dies kann das Leben und den Aufenthalt in der Stadt komfortabler machen. Andererseits kann die allgegenwärtige Erfassung und Verarbeitung personenbezogener Daten, beispielsweise durch intelligente Kameras, nachteilige Auswirkungen haben und Risiken für die Privatsphäre mit sich bringen. Für den langfristigen Erfolg von „Smart Cities“ ist das Vertrauen der Menschen unabdingbar. Dafür ist es notwendig, dass die Anbieter der damit verbundenen Dienste die Standards für Datenschutz und Privatsphäre einhalten. Mit dem Arbeitspapier zu diesem Themenkomplex haben wir Städte, Dienstanbieter und Regulierungsbehörden dabei unterstützt, datenschutzfreundliche Lösungen für „Smart Cities“ zu finden. Wir

81 Zur IWGDPT Berlin Group: www.iwgdpt.org

82 Arbeitspapiere der IWGDPT Berlin Group ebenfalls abrufbar unter: www.iwgdpt.org

haben alle beteiligten Akteure dazu aufgerufen, sich der Grundsätze des Datenschutzes bewusst zu sein und diese entsprechend unserer praktischen Empfehlungen umzusetzen.

Unter dem Stichwort Telemetrie sammeln Apps und Betriebssysteme oftmals große Mengen personenbezogener Daten, die rund um die Nutzung erfasst werden. Zum Beispiel Angaben darüber, wie oft Nutzende bestimmte Funktionen einer App verwenden oder zu welchen Zeiten. Auch bei scheinbar harmlosen Szenarien können personenbezogene Daten betroffen sein, beispielsweise wenn Daten über Systemabstürze erhoben werden. Häufig werden Nutzer darüber nicht ausreichend informiert und Datenschutz-Grundsätze wie Zweckbindung und Datenminimierung werden nicht eingehalten. Die Berlin Group hat verschiedene Probleme und Risiken von Telemetrie-Funktionen identifiziert und praktische Empfehlung für eine datenschutzkonforme Umsetzung gegeben. Wir haben alle beteiligten Akteure dazu aufgerufen, sich bewusst zu machen, dass die Grundsätze des Datenschutzes selbstverständlich auch für Telemetrie- und Diagnosedaten gelten. Mit den praktischen Empfehlungen haben wir gezeigt, dass es möglich ist diese, für die Qualitätssicherung wichtigen Funktionen, datenschutzkonform umzusetzen.

Auch Arbeitspapiere zur Gesichtserkennungstechnologie und zum Digitalen Zentralbankgeld wurden erarbeitet und sollen im Jahr 2024 veröffentlich werden. Als neue Themen für zukünftige Arbeitspapiere wurden die Bereiche Neurotechnologie und Künstliche Intelligenz identifiziert und in einem ersten Treffen diskutiert.

4.5 Weitere Gremien

Zu den weiteren europäischen oder internationalen Organisationen, Gruppen, Foren und Gremien, in denen meine Mitarbeiterinnen und Mitarbeiter mitwirken oder die ich selbst besuche, zählen z. B. der Europarat (Council of Europe), die Gruppe der Datenschutzbehörden der G7-Länder (G7 DPA Roundtable), das European Data Innovation Board oder auch die „High-level Expert Group on access to data for effective law enforcement“.

In den hier behandelten Organisationen oder Foren war ich im Berichtsjahr entweder als beratendes oder als ordentliches Mitglied beteiligt. Die Form meiner Beteiligung hängt dabei von den jeweiligen Umständen der betreffenden Gruppe oder Organisation ab. So sind Angehörige meiner Dienststelle als beratende Mitglieder in den deutschen Delegationen beim Datenschutz-Ausschuss des Europarates aktiv. Beim neuen European Data Innovation Board hingegen wirke ich selbst im Auftrag des Europäischen Datenschutzausschusses mit.

Es war mir eine Freude, im Vorjahr (2022) aufgrund der deutschen G7-Präsidentschaft den „G7 DPA Roundtable“, das Treffen der Vorsitzenden der Datenschutzaufsichtsbehörden der G7-Länder in Bonn ausrichten zu dürfen (31. TB Nr. 3.4.). Im Berichtsjahr habe ich gerne am G7-DPA Roundtable teilgenommen, der im Juni 2023 von meinen Kolleginnen und Kollegen der japanischen Datenschutzaufsichtsbehörde (Personal Information Protection Commission Japan – PPC Japan) in Tokio organisiert wurde.

4.5.1 G7 DPA Roundtable

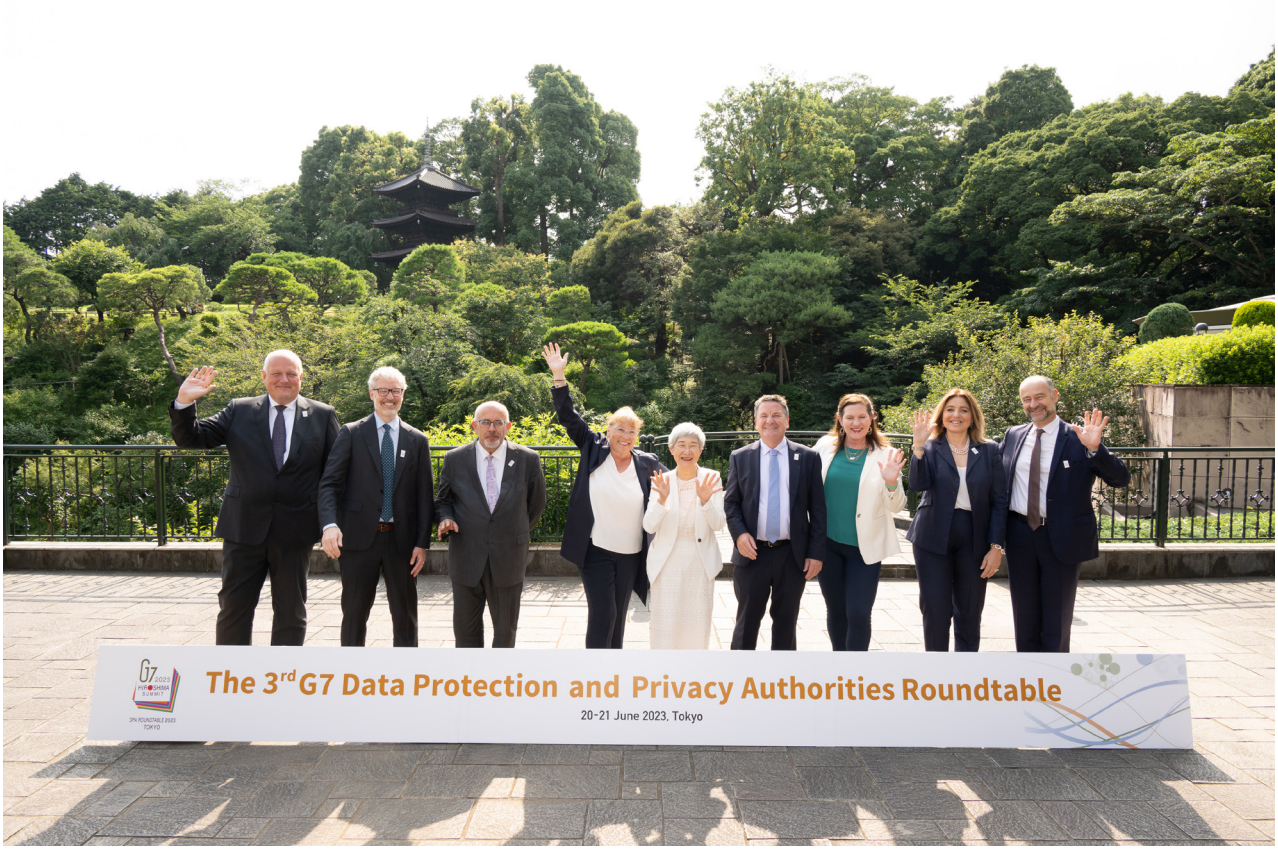
Die Datenschutzbehörden der G7-Staaten sind im Rahmen der japanischen G7-Präsidentschaft im Juni 2023 zur dritten Ausgabe ihres jährlichen Roundtable-Treffens in Tokio zusammengekommen. Im Fokus der Diskussionen standen insbesondere die Themen Data Free Flow with Trust (DFFT), also die Frage vertrauenswürdiger internationaler Datenübermittlung, sowie aktuelle Entwicklungen im Bereich generativer Künstlicher Intelligenz (KI) und die sich hieraus ergebenden Herausforderungen für den Datenschutz.

Nach der konstituierenden (virtuellen) Sitzung der Datenschutzbehörden der G7-Staaten (G7 Data Protection and Privacy Authorities, G7 DPAs) unter der britischen G7-Präsidentschaft 2021 (30. TB Nr. 3.4.1) und dem von mir 2022 organisierten G7 DPA Roundtable unter der deutschen G7-Präsidentschaft (31. TB Nr. 3.4) hat dieses Jahr die japanische Datenschutzbehörde den Vorsitz des G7 DPA Roundtable übernommen. Die Arbeit wurde dabei in drei für den internationalen Datenschutz essentielle Oberthemen untergliedert: Data Free Flow with Trust (DFFT), Emerging Technologies (aktuelle technologische Entwicklungen) und Enforcement Cooperation (internationale regulatorische Kooperation). Jedes dieser Themen wurde durch eine eigens hierfür gegründete Arbeitsgruppe erarbeitet und die Ergebnisse wie schon in den Jahren davor in einem Communiqué[83] zusammengefasst.

Data Free Flow with Trust

Die in den vorherigen G7 DPA Roundtable begonnenen Beratungen zu grundlegenden regulatorischen und technologischen Fragen und Entwicklungen im Zusam-

83 Communiqué 2023 vom 21. Juni 2023, abrufbar unter: www.bfdi.bund.de/g7



menhang mit DFFT wurden weiter vertieft. Das in Tokio verabschiedete Communiqué erkennt die Vorteile an, die sich aus grenzüberschreitenden Datenflüssen ergeben. Gleichzeitig weist der G7 DPA Roundtable jedoch darauf hin, dass entsprechende Datentransfers erhebliche Herausforderungen für den Schutz personenbezogener Daten und die Privatsphäre darstellen können. Vertrauen („Trust“) ist ein wesentlicher Bestandteil des Konzeptes DFFT und hohe Datenschutzstandards stellen eine Grundvoraussetzung für den freien Datenverkehr dar. Zu diesem Zweck bekräftigen die G7 Datenschutzbehörden ihren auch bisher verfolgten Ansatz, auf Gemeinsamkeiten und Elemente der Konvergenz zwischen bestehenden Regulierungsansätzen und Transferinstrumenten (etwa Standardvertragsklauseln, Zertifizierung und genehmigte Verhaltensregeln) hinzuarbeiten, um die Interoperabilität von verschiedenen Rechtssystemen und -instrumenten zu fördern. Der G7 DPA Roundtable selbst erarbeitet hierzu derzeit eine vergleichende Analyse verschiedener internationaler Zertifizierungsmechanismen.

Die G7 Datenschutzbehörden verstehen sich hierbei nicht als exklusives Gremium, vielmehr sollen ausdrücklich auch die in verschiedenen anderen internationalen Foren unternommenen Anstrengungen zu DFFT unterstützt und ergänzt werden, etwa in der Global Privacy Assembly (GPA) oder der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD). Die G7 Datenschutzbehörden haben es sich daher insbesondere zum Ziel gesetzt, den Dialog zwischen relevanten Organisationen und Netzwerken zu fördern. Auch die Digitalminister der G7-Staaten teilen diesen kooperativen Ansatz zur Förderung von DFFT.

Generative KI

Ein technologisches Thema, das aktuell an immer größerer globaler Bedeutung gewinnt und auch die G7 Datenschutzbehörden maßgeblich beschäftigt, sind die Fortschritte und damit einhergehenden rechtlichen und ethischen Herausforderungen der (generativen) KI. Hierbei ist es eine entscheidende Voraussetzung für die weitere Entwicklung und Anwendung von KI-Technologien, dass die Zivilgesellschaft auf die Einhaltung rechtlicher und demokratischer Standards vertrauen kann. Der G7 DPA Roundtable betont daher in seinem Communiqué 2023, dass Entwickler und Anwender entsprechender Technologien dafür Sorge zu tragen haben, bestehende rechtliche Verpflichtungen ein- und Risiken für Betroffene möglichst geringzuhalten.

Die G7 Datenschutzbehörden haben angesichts der großen Relevanz dieser Entwicklungen in Tokio erstmals

auch eine gesonderte Erklärung zu generativer KI (Statement on Generative AI) verabschiedet. Hierin legt die Gruppe sowohl Chancen als auch Herausforderungen dar, die sich aus KI-Technologien ergeben können. Eine der Kernbotschaften ist, dass KI keinesfalls eine rechtsfreie Zone ist: geltende Vorschriften erfassen auch KI-Produkte und -Anwendungen, selbst wenn in verschiedenen Jurisdiktionen derzeit an neuen KI-spezifischen Gesetzen und Richtlinien gearbeitet wird.

Aufbauend auf den wichtigen Erkenntnissen aus diesem Jahr wird der G7 DPA Roundtable seine Arbeit auch unter der italienischen G7-Präsidentschaft 2024 fortsetzen. Ergänzend zu dem in Tokio verabschiedeten Communiqué hat die Gruppe hierzu in einem Aktionsplan konkrete Maßnahmen festgelegt, um die Positionen der G7 Datenschutzbehörden in praktische Ergebnisse umzusetzen.[84]

Querverweise:

3.2.2 Nationale und internationale Zusammenarbeit zum Thema Künstliche Intelligenz

4.5.2 European Data Innovation Board

Der Europäische Datenschutzausschuss (EDSA) hat mich personengebunden als seinen Vertreter im Europäischen Dateninnovationsrat benannt. Im Rahmen meiner Mitgliedschaft werde ich aktiv an der Auslegung und Umsetzung des Data Governance Act sowie perspektivisch des Data Act mitwirken.

Der Europäische Dateninnovationsrat (European Data Innovation Board, kurz EDIB) ist eine Expertengruppe, die auf Grundlage des Data Governance Act (DGA) durch die Europäische Kommission eingerichtet wird. Der EDIB besteht aus Vertreterinnen und Vertretern der Behörden zur Durchsetzung des DGA, der Agentur der Europäischen Union für Cybersicherheit (ENISA), der Europäischen Kommission sowie einzelner Sachverständiger und Interessenträger der Wirtschaft, Forschung, Wissenschaft oder Zivilgesellschaft. Dem EDIB gehört neben einem Vertreter des Europäischen Datenschutzbeauftragten auch ein Vertreter des Europäischen Datenschutzausschusses (EDSA) an.

Der EDIB soll die Europäische Kommission bei der Überwachung und Durchsetzung des DGA und perspektivisch auch des Data Act (DA) beraten und unterstützen. Zu seinen Aufgaben gehört es insbesondere, auf eine EU-weit einheitliche behördliche Praxis im Rahmen der Durchsetzung des DGA bzw. des DA hinzuwirken. Zudem unterstützt der EDIB bei der Entwicklung von Leitlinien zu unterschiedlichen Themen, etwa zur Umsetzung gemeinsamer europäischer Datenräume, zum Schutz zu teilender Daten oder bei der Entwicklung eines Einwilligungsformulars für Datenaltruismus. Ein erstes Treffen des EDIB hat im Dezember 2023 stattgefunden. Ein Fokus für 2024 wird auf dem Thema Standardisierung liegen, die der Interoperabilität der verschiedenen geplanten europäischen Datenräume dienen soll.

Der EDSA hat mich personengebunden als seinen Vertreter im EDIB benannt. Im Rahmen meiner Mitgliedschaft werde ich aktiv an der Auslegung und Umsetzung zweier für das Datenrecht bedeutendsten EU-Digitalrechtsakte mitwirken können. Entsprechend den Positionen des EDSA werde ich mich besonders dafür einsetzen, dass die existierenden Schutzmechanismen – insbesondere der DSGVO – durch die neuen Rechtsakte nicht unterlaufen werden.

Querverweise:

5.3 Nationale Umsetzung der Digitalrechtsakte

4.5.3 Der Datenschutz-Ausschuss des Europarats

Der Datenschutz-Ausschuss (T-PD) des Europarats ist die zentrale Stelle für die Beratung und Bearbeitung datenschutzrelevanter Themen. Aufgrund der hohen Zahl von Vertragsparteien der Datenschutz-Konvention des Europarats hat dies besondere Bedeutung für die Menschen in Europa und darüber hinaus.

Im Berichtsjahr galt die Datenschutz-Konvention des Europarats bzw. das „Übereinkommen des Europarates zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten“ (Konvention 108) von 1981 für 55 Vertragsparteien – für die 46 Mitgliedsländer des Europarats (ohne die 2022 ausgeschiedene Russische Föderation) und für neun außereuropäische Unterzeichner-Staaten, z. B. Mexico, Argentinien, Tunesien oder Marokko.

Das Erweiterungsprotokoll zur Modernisierung der Konvention 108 hatten bis Ende 2023 insgesamt 31 Länder ratifiziert, darunter auch Deutschland.[85] Für das Inkrafttreten der modernisierten Fassung der Konvention 108, der sogenannten „Konvention 108+“, sind 38 Ratifizierungen erforderlich. Ich bin zuversichtlich, dass diese Schwelle im Laufe des Jahres 2024 erreicht werden kann. Dann werden die erweiterten Bestimmungen der Kon-

84 Dokumente des G7 DPA Roundtable sind abrufbar unter: www.bfdi.bund.de/g7

85 Übersicht der Ratifizierungen, abrufbar unter: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223

vention 108+ zum Datenschutz in Europa und darüber hinaus ihre Wirkung entfalten können. Aus meiner Sicht wird dies eine wesentliche Stärkung bedeuten für die Konvention 108+ in ihrer Eigenschaft als einziges verbindliches internationales Vertragswerk zum Datenschutz.

Bereits Art. 18 der Konvention 108 von 1981 sieht vor, einen „Beratenden Ausschuss“ einzurichten, für den häufig die Abkürzung „T-PD“ benutzt wird und der gemäß Art. 19 folgende Aufgaben hat:

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

Jede Vertragspartei ist im Beratenden Ausschuss vertreten. Infolge der Einrichtung meiner Dienststelle als eigenständige oberste Bundesbehörde nehmen Angehörige meiner Dienststelle seit 2016 als beratende Mitglieder der deutschen Delegation an den Sitzungen des T-PD teil. Die Vertretung Deutschlands als Mitglied des Europarats im Beratenden Ausschuss wird durch das Bundesministerium des Innern und für Heimat wahrgenommen. Es freut mich, dass eine Expertin dieses Ressorts im Herbst 2022 erstmals zur Vorsitzenden des T-PD gewählt wurde. Im Laufe der Jahre hat der Beratende Ausschuss zahlreiche wichtige Empfehlungen und Leitlinien beschlossen. Im Berichtsjahr befasste er sich u. a. mit den Themen „Digitale Identität“ oder „Verwendung biometrischer Daten“ (vor allem Fingerabdrücke) bei Wahlen und Abstimmungen. Zudem hat das T-PD Modell-Vertragsklauseln (Model Contractual Clauses) für verschiedene Szenarien von Datenübermittlungen beschlossen (Modul 1 für Übermittlungen zwischen verantwortlichen Stellen; Modul 2 für Übermittlungen zwischen Verantwortlichem und Auftragsverarbeiter). Weitere Themen, an denen der Beratende Ausschuss 2023 gearbeitet hat, sind Neurotechnologie und Art. 11 der Konvention 108+; dieser Artikel berührt das politisch sensible Thema, ob und inwieweit Ausnahmen von Bestimmungen der Konvention 108 für den Bereich der Nachrichtendienste oder Sicherheitsbehörden zulässig sind.

Es war mir auch im zurückliegenden Berichtsjahr ein besonderes Anliegen, durch das Einbringen meiner Expertise die Aktivitäten des Beratenden Ausschusses zu unterstützen.

4.5.4 ETIAS-Beratungsgremium für Grundrechte

Das ETIAS-Beratungsgremium für Grundrechte nimmt seine Arbeit auf. Im Fokus stehen dabei der Aufbau des Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und die Etablierung der Arbeitsbeziehungen zu den künftigen Kooperationspartnern.

Das unabhängige ETIAS-Beratungsgremium für Grundrechte ist im November 2022 neu eingesetzt worden (31. TB Nr. 3.5.3). Es nimmt Beurteilungen vor und gibt Empfehlungen zu den grundrechtlichen Auswirkungen der Bearbeitung von Anträgen auf Erteilung von Reisegenehmigungen im ETIAS. Gleiches gilt für die Anwendung der sog. ETIAS-Überprüfungsregeln, mit denen geprüft werden soll, ob die Einreise von Drittstaatsangehörigen ein Risiko für die Sicherheit in der EU, ein Risiko der illegalen Einwanderung oder ein hohes Epidemierisiko darstellt.

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 Vorsitzender des ETIAS-Beratungsgremiums für Grundrechte ist.

Im Berichtsjahr 2023 lag der Schwerpunkt der Tätigkeit des Beratungsgremiums auf der Begleitung des Aufbaus des ETIAS und auf der Etablierung der Arbeitsbeziehungen zu anderen ETIAS-Einrichtungen. Dazu gehören insbesondere der ETIAS-Überprüfungsausschuss und die ETIAS-Zentralstelle. Diese Einrichtungen werden zentrale Kooperationspartner für das ETIAS-Beratungsgremium für Grundrechte sein. Das Beratungsgremium hatte im Berichtsjahr 2023 insgesamt sechs reguläre Sitzungen. Vertreter des Gremiums haben zudem an zahlreichen weiteren Sitzungen teilgenommen, so etwa zum Aufbau der nationalen ETIAS-Stellen, des ETIAS-Überprüfungsausschusses und verschiedener zentraler Prozesse.

4.5.5 Die „High Level Group on access to data for effective law enforcement“ – neue Empfehlungen zur Vorratsdatenspeicherung?

Die neue EU-Arbeitsgruppe soll Empfehlungen zum Zugriff von Strafverfolgungsbehörden auf Daten im Netz entwickeln. Neue Vorschläge müssen die Rechtsprechung des 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.[86] Die HLG untersucht Herausforderungen, denen sich Strafverfolgungsbehörden bei ihrer täglichen Arbeit im Zusammenhang mit dem Zugang zu Telekommunikationsdaten gegenüberstehen. Dabei verfolgt sie 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.

Die HLG tagt auf Ebene eines Plenums sowie in drei Arbeitsgruppen. Der EDSA entsendet Experten auf alle Ebenen. Ich bin vertreten durch einen meiner Mitarbeiter als Experte des EDSA in der Arbeitsgruppe, die sich mit dem Zugang von Strafverfolgungsbehörden zu Daten in den Systemen von Dienstanbietern beschäftigt.

Die bisherige Diskussion in der Arbeitsgruppe ist stark geprägt von dem Wunsch der teilnehmenden Vertreterinnen und Vertretern von Strafverfolgungsbehörden aus zahlreichen Mitgliedsstaaten nach einer Ausweitung ihrer Befugnisse, möglichst auf Basis einer europaweit einheitlichen Regelung. Ich werde mich dafür einsetzen, dass Vorschläge aus der HLG die Rechtsprechung des EuGH zur Vorratsdatenspeicherung und die zugrundeliegenden Grundrechte beachten. Bei allem Verständnis für die Notwendigkeit effektiver Strafverfolgung im Netz muss – auch im Interesse der Akzeptanz jedweder Maßnahme – ein hohes Datenschutzniveau gewährleistet bleiben.

86 Informationen der Europäischen Kommission zur HLG, abrufbar unter: https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en

5 Gesetzgebung

5.1 Erstes Gesetz zur Änderung des Bundesdatenschutzgesetzes

Das Bundesministerium des Inneren und für Heimat (BMI) hat in diesem Jahr den Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Erstes Bundesdatenschutzänderungsgesetz – 1. BDSGÄndG) vorgelegt. Meine Behörde begleitet das laufende Gesetzgebungsverfahren und setzt sich insbesondere für die Umsetzung der im Rahmen der Evaluierung des Bundesdatenschutzgesetzes (BDSG) durch die Datenschutzkonferenz (DSK) ausgemachten Änderungsbedarfe ein.

Der innerhalb der Bundesregierung noch nicht abgestimmte Gesetzesentwurf für ein 1. BDSGÄndG soll die datenschutzrechtlich relevanten Vereinbarungen des Koalitionsvertrags aufgreifen sowie Ergebnisse umsetzen, die sich aus der Evaluierung des BDSG durch das BMI ergeben haben. Der Gesetzesentwurf enthält einige notwendige Klarstellungen, greift jedoch insbesondere bezüglich der im Rahmen der Evaluierung des BDSG durch die DSK ausgemachten Überarbeitungsbedarfe zu kurz. Er enthält in seinem § 16a eine Regelung zur Institutionalisierung der DSK. Eine Regelung zur rechtlichen Verbindlichkeit ihrer Beschlüsse ist hingegen nicht vorgesehen.

Der Entwurf enthält wichtige Klarstellungen für die Zusammenarbeit der deutschen Aufsichtsbehörden in europäischen Angelegenheiten. Die Aufsichtsbehörden der Länder und meine Behörde sollten auf europäischer Ebene immer mit einer Stimme sprechen, um den deutschen Positionen dort mehr Gewicht beizumessen. Folglich muss aus meiner Sicht bereits im Kooperationsverfahren ein einheitliches Auftreten der deutschen Aufsichtsbehörden gewährleistet sein. Zudem können auch im Dringlichkeitsverfahren Verfahrenshandlungen vorgenommen werden, die zu einem Verfahren vor dem EDSA führen und mithin einen gemeinsamen deutschen Standpunkt bedingen. Daher habe ich mich wiederholt dafür ausgesprochen, im Gesetzestext zu § 18 BDSG klarzustellen, 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. Dieses Petitum ist nun im Gesetzentwurf berücksichtigt worden.

Es bedarf darüber hinaus jedoch einer Änderung von folgenden Regelungen im BDSG:

- 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. Es ist nicht ersichtlich, warum hier nichtöffentliche und öffentliche Stellen ungleich behandelt werden.
- Erweiterung meiner Aufsichtszuständigkeit für Verstöße durch Beschäftigte öffentlicher Stellen des Bundes, die sich selbst zum Verantwortlichen aufschwingen (sog. Mitarbeiterexzess). Liegt ein Mitarbeiterexzess vor, bin nach aktueller Gesetzeslage für die entsprechende Verarbeitung personenbezogener Daten durch die beschäftigte Person nicht ich, sondern nach § 40 BDSG die jeweilige Datenschutzaufsichtsbehörde des Landes zuständig, da die betreffende Person nicht die Voraussetzungen der in § 9 Abs. 1 BDSG genannten Stellen erfüllt. Damit einheit-

liche Lebenssachverhalte bei einer Aufsichtsbehörde gebündelt werden können, halte ich die dargestellte Erweiterung meiner Zuständigkeit, beispielsweise durch eine ergänzende Regelung in § 9 BDSG, für erforderlich.

→ Durch die §§ 32–35 BDSG werden die Betroffenenrechte teilweise in einer nicht den europäischen Vorgaben entsprechenden Weise eingeschränkt. Beispielsweise besteht für eine Einschränkung der Löschverpflichtung, die über Art. 17 Abs. 3 lit. b) DSGVO hinausgeht, weder ein Bedarf noch eine Befugnis, so dass die entsprechende Regelung des § 35 Abs. 3 BDSG zu streichen ist.

Ich werde mich im laufenden Gesetzgebungsverfahren weiterhin insbesondere für die oben dargestellten Änderungsvorschläge einsetzen.

5.2 Beschäftigtendatenschutzgesetz

Der Koalitionsvertrag für die 20. Legislaturperiode sieht die Schaffung von Regelungen zum Beschäftigtendatenschutz vor, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen. Die Bundesregierung hat zwar Vorschläge für einen modernen Beschäftigtendatenschutz erarbeitet, einen Gesetzentwurf bislang aber nicht vorgelegt.

Bereits 2014 hatte die Datenschutzkonferenz (DSK) die Schaffung eines Beschäftigtendatenschutzgesetzes gefordert (vgl. 25. TB Nr. 9.3.1 und Anlage 9). Angesichts der fortschreitenden Digitalisierung der Arbeitswelt sind neue Regelungen nunmehr dringender denn je. Vor dem Hintergrund technischer Entwicklungen, die vielfach auch eine weitgehende Überwachung der Beschäftigten ermöglichen, reicht die geltende Bestimmung des § 26 BDSG nicht aus. Sie ist zu unbestimmt, lässt viel Interpretationsspielraum, ist nicht hinreichend praktikabel, normenklar und sachgerecht. Sie führt zu Unklarheiten über die Zulässigkeit von Verarbeitungen personenbezogener Daten im Beschäftigungskontext für Arbeitgeberinnen und Arbeitgeber, Beschäftigte, Bewerberinnen und Bewerber, Personalvertretungen oder Gerichte.

Der vom BMAS eingesetzte unabhängige Beirat zum Beschäftigtendatenschutz, dessen Mitglied ich war, ist 2022 gleichfalls zu dem Ergebnis gekommen, dass die Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes geboten ist. Zudem liefert ein aktuelles Urteil des Europäischen Gerichtshofs (EuGH)[87] ein weiteres starkes Argument für die überfällige Reform des deutschen Beschäftigtendatenschutzes.

Der EuGH macht in diesem Urteil Vorgaben zur Auslegung des persönlichen und sachlichen Anwendungsbereichs der Öffnungsklausel des Art. 88 DSGVO zu der Frage, unter welchen Voraussetzungen und innerhalb welcher Grenzen nationale Vorschriften „spezifisch“ im Sinne von Abs. 1 dieses Artikels sind sowie zu den Folgen der Feststellung, dass nationale Normen nicht den vom EuGH aufgestellten Vorgaben an „spezifische“ Regelungen genügen. Entscheidend ist dem EuGH zufolge ein zum Beschäftigungskontext passender, über die allgemeinen Regelungen der DSGVO hinausgehender und zugleich mit den Grundsätzen der DSGVO vereinbarer Regelungsgehalt der nationalen Vorschriften, deren Ziel der Schutz der Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext ist und die geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen.

Vor dem Hintergrund des EuGH-Urteils hat die DSK mit ihrer Entschließung vom 11. Mai 2023[88] erneut die Notwendigkeit der Schaffung spezifischer Regelungen bekräftigt. Diese Entschließung knüpft unmittelbar an die vorhergehende Entschließung vom April 2022[89] an. Darin fordert die DSK beschäftigtendatenschutzrechtliche Regelungen im Rahmen eines eigenständigen Gesetzes mindestens in folgenden Bereichen (vgl. 31. TB Nr. 3.2.4):

→ Einsatz algorithmischer Systeme einschließlich Künstlicher Intelligenz (KI)

→ Grenzen der Verhaltens- und Leistungskontrolle

→ Ergänzungen zu den Rahmenbedingungen der Einwilligung

→ Regelungen über Datenverarbeitungen auf Grundlage von Kollektivvereinbarungen

87 Urteil vom 30. März 2023 in der Rechtssache C-34/21

88 Entschließung „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz!“, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Beschaeftigtendatenschutz.pdf

89 Entschließung „Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt‘!“, abrufbar unter: https://datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf

- → Regelungen zum Verhältnis zwischen § 22 und § 26 BDSG sowie zu Art. 6 und 9 DSGVO
- → Beweisverwertungsverbote
- → Datenverarbeitung bei Bewerbungs- und Auswahlverfahren.

Nach Auskunft der Bundesregierung soll ein entsprechender Gesetzentwurf in gemeinsamer Federführung des Bundesministeriums für Arbeit und Soziales (BMAS, technische Federführung) und des Bundesministeriums des Innern und für Heimat (BMI) entsprechend der Koalitionsvereinbarung nunmehr erarbeitet werden (vgl. 31. TB Nr. 3.2.4). Dem vorausgehend haben BMAS und BMI zwischenzeitlich inhaltliche Vorschläge für einen modernen Beschäftigtendatenschutz vorgestellt.

Es bleibt zu hoffen, dass die Chance zur Schaffung eines Beschäftigtendatenschutzgesetzes alsbald genutzt wird. Im Rahmen eines entsprechenden Gesetzgebungsverfahrens werde ich mich für faire Regelungen zum Schutz des Grundrechts auf informationelle Selbstbestimmung der Beschäftigten einsetzen.

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.

5.3 Nationale Umsetzung der Digitalrechtsakte

Meine Behörde berät bei den Verhandlungen zu den europäischen Rechtsakten zur Digitalisierung und ihren nationalen Umsetzungen die Bundesregierung und bringt sich aktiv bei den entsprechenden Initiativen im Europäischen Datenschutzausschuss (EDSA) ein. Zu diesen Rechtsakten gehören u. a. der Data Governance Act (DGA), der Data Act (DA) sowie die Verordnung über die Transparenz und das Targeting von politischer Werbung (Verordnung politische Werbung).

Data Governance Act

Der Data Governance Act (DGA) ist seit dem 24. September 2023 anwendbar. Ziel dieser Europäischen Verordnung ist es, das Vertrauen in die gemeinsame Nutzung von Daten zu stärken. Mit dem DGA sollen in unterschiedlichen Handlungsfeldern die Rahmenbedingungen für eine sog. Datenökonomie geschaffen werden (30. TB Nr. 5.9).

Zum einen beinhaltet der DGA Regelungen für die Weitergabe von u. a. auch personenbezogenen Daten durch öffentliche Stellen zur allgemeinen Nutzung (Open Data). Es bleibt allerdings den Mitgliedstaaten überlassen, die Rechtsgrundlagen für die zulässige Weitergabe zu schaffen, und die DSGVO bleibt insgesamt unberührt. Dies ist aus meiner Sicht zu begrüßen.

Zum anderen definiert der DGA neutrale Vermittlungsdienste für die gemeinsame Datennutzung, die Datenanbieter und Datennutzer zusammenbringen sollen. Darüber hinaus werden Rahmenbedingungen geschaffen, die die Mitgliedstaaten zur Einrichtung sog. datenaltruistischer Organisationen ermutigen sollen. Das Vertrauen in solche Organisationen soll derart gestärkt werden, dass Bürger freiwillig ihre personenbezogenen Daten für gemeinwohlbezogene Ziele, wie etwa zu Forschungszwecken, zur Verfügung stellen.

Aus meiner Sicht problematisch ist, dass zur Durchsetzung des DGA neben der Datenschutzaufsicht eine eigene Aufsichtsstruktur geschaffen wird, obwohl in der Sache überlappende Zuständigkeiten bestehen werden[90] Zum Entwurf des deutschen Durchführungsgesetzes zum DGA, dem Daten-Governance-Gesetz, habe ich daher angeregt, Regelungen zur Kooperation zwischen DGA- und Datenschutzaufsicht aufzunehmen, um eine effektive Durchsetzung sowie Rechtssicherheit für Verantwortliche und Betroffene zu gewährleisten.

Data Act

Mit der Zustimmung zur finalen Fassung des Data Act (DA) durch den Rat der EU Ende November 2023 ist – vorbehaltlich der Unterzeichnung durch die Präsidenten von Rat und EU-Parlament und der Veröffentlichung im Amtsblatt der EU – das europäische Gesetzgebungsverfahren zu Ende gegangen. Ziel des DA ist, neue Vorschriften zu etablieren, wer die in den Wirtschaftssektoren in der EU erzeugten Daten nutzen darf und wer Zugriff darauf hat. Der DA sieht unter anderem vor, Nutzern Zugang zu den von ihren vernetzten Geräten

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

erzeugten Daten zu garantieren, die häufig ausschließlich von Herstellern gesammelt werden. Daneben sollen durch ein Verbot unfairer Klauseln Ungleichgewichte in Verträgen über die gemeinsame Datennutzung verhindert werden. Behörden soll in besonderen Konstellationen Zugang zu und die Nutzung von Daten im Besitz des Privatsektors ermöglicht werden.

Ich habe mich wiederholt dafür eingesetzt, dass die Schutzmechanismen der DSGVO durch den DA nicht unterlaufen werden und die DSGVO vom DA unberührt bleibt. Hierzu sowie zu weiteren kritischen Punkten, wie etwa die vorgesehene Aufsichtsstruktur im Data Act, hatte ich gemeinsam mit meinen europäischen Kolleginnen und Kollegen im EDSA und dem EDSB eine umfängliche Stellungnahme verfasst.[91] In dem nunmehr vorliegenden finalen Text wurden in dieser Hinsicht einige begrüßenswerte Klarstellungen aufgenommen.

Deutlich wird sowohl beim DGA als auch beim DA, dass verbesserte Rahmenbedingungen für digitale Geschäftsmodelle und Verarbeitungsformen im Mittelpunkt der Anstrengungen des EU-Gesetzgebers stehen. Beide Rechtsakte stellen allerdings das bisherige Schutzkonzept des Datenschutzes vor erhebliche Herausforderungen. Umso mehr gilt es, diese Rahmenregelungen für sog. Datenmärkte im Hinblick auf die Risiken in Gestalt eines massenhaften Austausches von auch personenbeziehbaren Daten und deren Auswertung insbesondere zu rein kommerziellen Zwecken sorgfältig im Blick zu behalten. Ziel meiner Beratung ist es daher, auf Problempunkte hinzuweisen und auf eine möglichst datenschutzfreundliche Regulierung hinzuwirken. Hierzu werde ich auch durch meine Mitgliedschaft als Vertreter des EDSA im Europäischen Dateninnovationsrat (EDIB) beitragen, der die Europäische Kommission bei der Überwachung und Durchsetzung des DGA und des DA beraten und unterstützen soll.

Verordnung politische Werbung

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

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

Ich habe mich wiederholt für ein komplettes Verbot der Nutzung jeglicher Form personenbezogener Daten für Targeting, Amplifizieren und Ad Delivery in Bezug zu politischer Werbung eingesetzt. Ein solches Verbot dient dem Schutz der Nutzerinnen und Nutzer von Online-Diensten, aber auch der Integrität von freien Wahlen, und gewährleistet eine offene, plurale Debatte als Säule der europäischen Demokratie.

Zum Ende des Berichtsjahrs wurde im Rahmen der Trilogverhandlungen eine politische Einigung über die wichtigsten politischen Elemente erzielt. In dem nunmehr vorliegenden Entwurf der Verordnung politische Werbung wurden einige Verbesserungen erreicht. So sollen Targeting, Amplifizieren und Ad Delivery in Bezug auf politische Werbung jedenfalls auf Basis der Verarbeitung sensibler personenbezogener Daten insgesamt unzulässig sein. Im Übrigen soll für die Verarbeitung personenbezogener Daten zu diesem Zweck eine ausdrückliche Einwilligung der Nutzer erforderlich sein.

Nach der politischen Einigung sind die Arbeiten am Entwurfstext weit fortgeschritten. Geplant ist eine Anwendbarkeit der Verordnung politische Werbung 18 Monate nach Inkrafttreten, einzelne Regelungen gelten unmittelbar mit Inkrafttreten und damit schon vor der Wahl zum 10. Europäischen Parlament im Juni 2024.

Querverweise:

4.5.4 European Data Innovation Board

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

5.4 NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) soll die IT-Sicherheit in Deutschland gestärkt werden, indem zahlreichen Stellen – ob öffentlich oder nichtöffentlich – Cybersicherheitsmaßnahmen sowie Meldepflichten auferlegt werden. Angesichts der engen Verzahnung zur IT-Sicherheit stellen sich hier zahlreiche Herausforderungen für einen effektiven Datenschutz.

Im Dezember 2022 hat die EU eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS2-Richtlinie) verabschiedet. Diese Richtlinie stellt auf EU-Ebene Regeln für Betreiber kritischer Infrastrukturen und anderer wichtiger Stellen auf und legt ihnen Cybersicherheitsmaßnahmen und Meldepflichten auf. Die EU-Mitgliedstaaten müssen die NIS2-Richtlinie nun bis zum 17. Oktober 2024 in nationales Recht umsetzen.

Das Bundesministerium des Innern und für Heimat (BMI) hat am 18. Juli 2023 seinen Referentenentwurf für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG) zur Ressortabstimmung gestellt. Daran wurde auch ich beteiligt und habe entsprechend dazu Stellung genommen.

Im digitalen Zeitalter kommt der Cyber- und Informationssicherheit eine große Bedeutung zu. Mit dem NIS2-UmsuCG bietet sich die Chance, die Gesellschaft und Wirtschaft im digitalen Raum besser zu schützen. Digitalisierung und Cybersicherheit sind hierbei untrennbar mit dem Thema Datenschutz verbunden. Wird im IT-Bereich eine Bedrohung festgestellt, sind regelmäßig auch die Schutzgüter des Datenschutzes betroffen. Insgesamt lässt sich der Datenschutz nicht ohne eine funktionierende IT-Sicherheit realisieren.

Kern des NIS2UmsuCG ist die Neufassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Dem BSI fällt hier die zentrale Rolle zu, die vorgesehenen Maßnahmen zu kontrollieren, betroffene Stellen zu unterstützen und als zentrale Stelle für Informationssicherheit auf nationaler Ebene zu fungieren.

Aus diesem Grund habe ich in einem Brief an verschiedene Ministerien 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.[92] Schwachstellen sind Sicherheitslücken, durch deren Ausnutzung sich Dritte unbefugt Zugang zu IKT-Produkten oder -Diensten verschaffen bzw. diese beeinflussen können. Die Risiken einer offen gelassenen Schwachstelle überwiegen schlicht die vermeintlichen Vorteile z. B. für die Arbeit von Sicherheitsbehörden, die durch das Offenhalten entstehen könnten.

5.5 Dienste zur Einwilligungsverwaltung

Seit April 2023 liegt der neue Entwurf einer Rechtsverordnung über „Anerkannte Dienste zur Einwilligungsverwaltung“ vor, mit denen Internetnutzende ihre Einwilligungen für nicht unbedingt erforderliche Zugriffe auf ihre Endgeräte nutzerfreundlich verwalten können sollen. Ein – durchaus mögliches – Ende der „Einwilligungs-Banner-Flut“ ist damit aber leider nicht zu erwarten.

Das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) sieht in § 26 Anerkannte Dienste zur Einwilligungsverwaltung vor, mit denen Internetnutzende ihre Einwilligungen für nicht unbedingt erforderliche Zugriffe auf ihre Endgeräte nutzerfreundlich verwalten können sollen. Die Anforderungen an die Dienste, das Verfahren zur Einholung der Einwilligungen und das Anerkennungsverfahren soll nach § 26 Abs. 2 TTDSG eine Rechtsverordnung regeln. Es freut mich, dass seit April dieses Jahres endlich ein überarbeiteter Referentenentwurf für eine Einwilligungsverwaltungsverordnung (EinwVO) vorliegt, nachdem ein erster Entwurf wegen Widersprüche der beteiligten Ressorts und meiner Behörde nicht über die Ressortabstimmung hinausgekommen ist. Über den ersten Entwurf und meine Kritik berichtete ich im letzten Tätigkeitsbericht (31. TB Nr. 5.5).

Die Einwilligungsverwaltungsdienste müssen vorab von einer unabhängigen Stelle nach Maßgabe der EinwVO anerkannt werden. Der aktuelle Entwurf der EinwVO sieht vor, dass ich für das Anerkennungsverfahren zuständig sein soll. Meine Zuständigkeit kann sich dabei allein auf die Prüfung der Anerkennungsfähigkeit erstrecken, die u. a. vorliegt, wenn der Dienst es ermöglicht, wirksame Einwilligungen einzuholen. Eine Prüfung der Wirksamkeit einzelner über den Dienst eingeholter

92 Mein Schreiben vom 18. September 2023 an sechs Ministerien, abrufbar unter: www.bfdi.bund.de/dokumente

Einwilligungen durch mich kann damit nicht einhergehen. Die Prüfung konkreter Einwilligungen im Einzelfall wird weiterhin in der Zuständigkeit der oder des für den Telemedienanbieter jeweils zuständigen Landesdatenschutzbeauftragten liegen. Das gesetzgeberische Ziel, die viel kritisierte „Einwilligungs-Banner-Flut“ zu bekämpfen, begrüße ich. Die konkrete Herangehensweise ist meines Erachtens aber nicht geeignet, dieses Ziel zu erreichen. Denn die angedachten Einwilligungsverwaltungsdienste können allein eine nach TTDSG erforderliche Einwilligung für den Zugriff auf Endgeräte i. S. d. § 25 TTDSG einholen und keine etwaige nach der DSGVO erforderliche Einwilligung in die Verarbeitung personenbezogener Daten. Etwa für eine Datenverarbeitung zu Profiling- oder Marketingzwecken kommt als Rechtsgrundlage regelmäßig nur eine Einwilligung i. S. d. Art. 6 Abs.1 lit. a) DSGVO in Betracht. Es besteht rechtlich auch keine Möglichkeit, DSGVO-Einwilligungen in der Einwilligungsverwaltungsverordnung verbindlich zu regeln.

Zudem kann die Einwilligungsverwaltungsverordnung die Anforderungen an eine freiwillige Einwilligung nicht modifizieren. Diese ergeben sich unmittelbar aus der DSGVO. Insbesondere können über Einwilligungsverwaltungsdienste nicht vorab pauschal Einwilligungen für bestimmte Trackingtechnologien wie Cookies oder für bestimmte Drittanbieter abgefragt und bei Besuch verschiedener Webseiten von den Diensten ungefragt abgegeben werden. Die DSGVO verlangt, dass Einwilligung für den bestimmten Fall erteilt werden. Eine sinnvolle und rechtmäßige Lösung dieses Problem liegt meines Erachtens darin, dass Nutzende in den Einwilligungsverwaltungsdiensten Voreinstellungen vornehmen, die bei dem erstmaligen Besuch einer Webseite abgefragt werden und dann von den Nutzenden bestätigt werden, wobei sie erst in diesem Moment die Einwilligungen tatsächlich abgeben. Schließlich sieht der aktuelle Entwurf vor, dass für Webseitenbetreibende und Drittanbieter die Beachtung der Einwilligungsverwaltungsdienste freiwillig ist. Ohne eine verpflichtende Berücksichtigung der von den Nutzenden in den Verwaltungsdiensten (nicht) erteilten Einwilligungen droht die Einwilligungsverordnung ins Leere zu Laufen, da zu erwarten ist, dass Nutzende weiterhin von Einwilligungsbannern behelligt werden. Einwilligungen, die Nutzende nur abgeben, um mehrfachten Abfragen zu entgehen, sind nicht freiwillig und damit unwirksam.

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.

5.6 Hinweisgeberschutzgesetz

Am 2. Juli 2023 ist das „Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“, in Kraft getreten. Es war zunächst am Widerstand des Bundesrates gescheitert.

Mit dem Gesetz ist die Richtlinie 2019/1937 RL (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Whistleblowing-RL – WBRL) in nationales Recht umgesetzt und damit der bislang lückenhafte und unzureichende Schutz von hinweisgebenden Personen ausgebaut worden. Die Richtlinie schafft erstmals unionsweite Mindeststandards zum individuellen Schutz von Whistleblowern und zum institutionellen Umgang mit den von ihnen weitergegebenen Insider-Informationen.

Ich habe bereits in meinem letzten Tätigkeitsbericht zu der vom Bundestag am 16. Dezember 2022 beschlossenen Gesetzesfassung berichtet. Da der Bundesrat dieser jedoch nicht zugestimmt hatte, wurde der Vermittlungsausschuss einberufen, in dem sich Vertreter des Bundestages und des Bundesrates im Mai dieses Jahres auf die in die finale Gesetzesfassung eingeflossenen Änderungen geeinigt haben.

Zentraler Bestandteil des Gesetzes ist weiterhin das Hinweisgeberschutzgesetz (HinSchG) als neues Stammgesetz für einen besseren Schutz hinweisgebender Personen. Ein wesentliches Element des HinSchG ist die Einrichtung von Meldestellen in Unternehmen und Behörden. Hinweisgebende Personen können sich dorthin wenden, wenn sie Informationen über Verstöße erlangt haben, die sich auf den Beschäftigungsgeber oder eine andere Stelle beziehen, mit der die hinweisgebende Person beruflich im Kontakt stand. Die hinweisgebende Person kann nach dem HinSchG frei wählen, ob sie sich an eine interne oder eine externe Meldestelle wendet, sie soll jedoch die Meldung bevorzugt bei einer internen Meldestelle einreichen, wenn intern wirksam gegen den

Verstoß vorgegangen werden kann und sie keine Repressalien befürchtet.

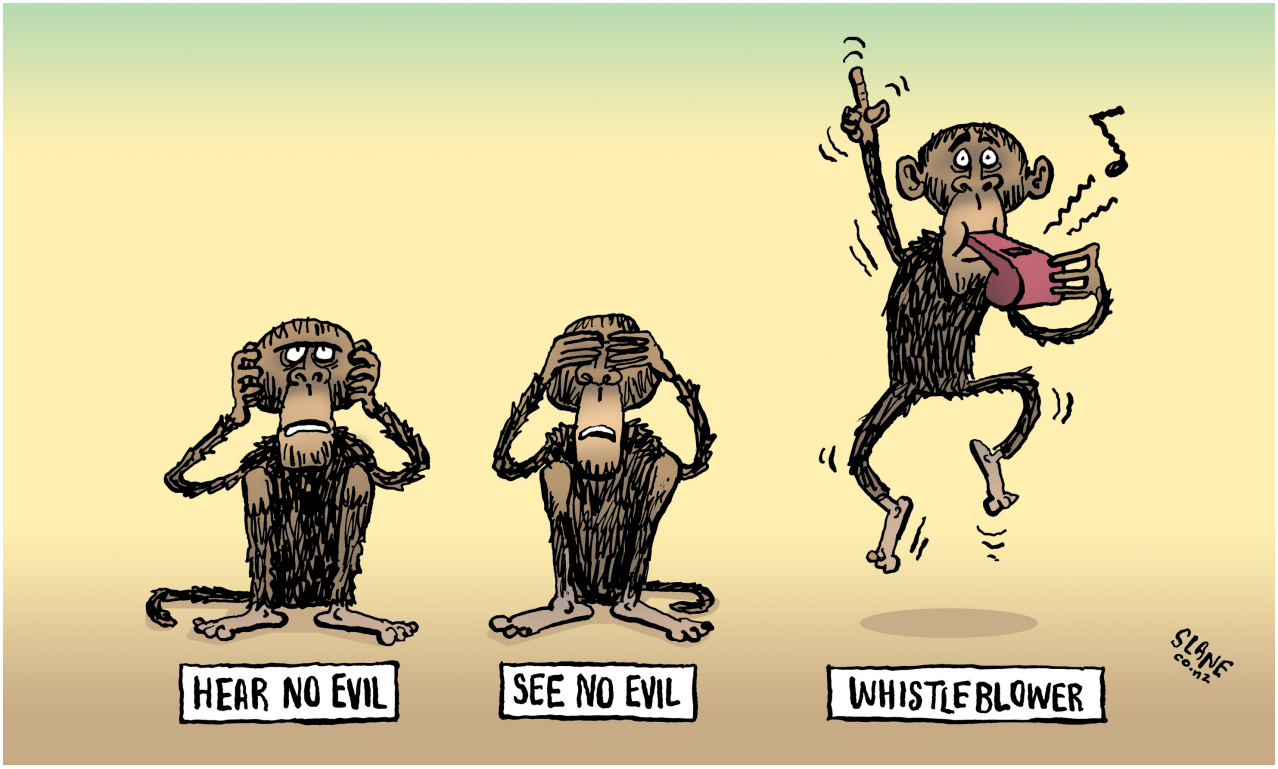
Die auch von mir im Rahmen des Gesetzgebungsverfahrens geforderte und noch in der erstmaligen Beschlussfassung des Gesetzes verankerte Pflicht, auch anonyme Meldungen zu bearbeiten und anonyme Kommunikationskanäle zur Verfügung zu stellen, war einer der umstrittensten Aspekte im Gesetzgebungsverfahren und einer der wesentlichen Gründe für den Bundesrat, der Vorlage nicht zuzustimmen. Diese Pflicht wurde infolge des im Vermittlungsausschuss gefundenen Kompromisses dann leider gestrichen. Enthalten ist in der finalen Fassung des Gesetzes allein der Hinweis, dass anonyme Meldungen zumindest bearbeitet werden „sollen".

Wie ich bereits in meinen Stellungnahmen im Rahmen des Gesetzgebungsverfahren verdeutlicht hatte, wäre die Aufnahme einer Verpflichtung zur Bearbeitung auch anonym eingehender Hinweise ein bedeutendes Vertrauenssignal an potentielle Hinweisgeberinnen und Hinweisgeber gewesen. Die Bereitschaft der Beschäftigten, Verstöße zu melden, wird durch die Bereitstellung anonymer Kommunikationskanäle erhöht und hierdurch ihr Vertrauen in eine diskrete Behandlung gestärkt. Von daher setze ich darauf, dass ein Großteil sowohl der privaten als auch der öffentlichen Beschäftigungsgeber – trotz fehlender gesetzlicher Verpflichtung – anonyme Meldewege bereitstellt, um die Hemmschwelle zur Abgabe von Meldungen möglichst niedrig zu halten.

Obgleich das HinSchG mit dieser „Soll"-Regelung hinter einer meiner wesentlichen Forderungen zurückbleibt, begrüße ich die mit ihm verbundene Umsetzung der WBRL. Denn Hinweisgeberinnen und Hinweisgeber leisten einen Beitrag zu mehr Transparenz und zur Stärkung der Informationsfreiheit in für die Öffentlichkeit weitgehend intransparenten, aber für zentrale gesellschaftliche Ziele und Werte oft außerordentlichen folgenreichen Beschäftigungsbereichen. Sie unterstützen damit in demokratischen rechtsstaatlichen Gesellschaften wichtige öffentliche Interessen.

5.7 Gesetz zur Umsetzung der Richtlinie über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher

Speziell in Massenverfahren und bei oftmals geringen Streitwerten können Verbandsklagen als Durchsetzungsinstrument einen wichtigen Beitrag zum Schutz der Verbraucherinnen und Verbraucher leisten, dies nicht zuletzt bei systematischen Verstößen im Bereich des Datenschutzes. Das Gesetz zur Umsetzung der Richtlinie über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher bietet hierfür die rechtliche Grundlage.



Dem Schutz der Verbraucherinnen und Verbraucher vor rechtswidrigen Geschäftspraktiken widmet sich die sogenannte EU-Verbandsklagenrichtlinie (VKR) sowie das zu deren Umsetzung erlassene Verbandsklagenrichtlinienumsetzungsgesetz, kurz VRUG. Mit den Regelungswerken soll sichergestellt werden, dass den Verbraucherinnen und Verbrauchern in allen Mitgliedstaaten wirksame und effiziente Verbandsklageverfahren auf Unterlassungs- und Abhilfeentscheidungen zur Verfügung stehen. Deshalb und zur Stärkung des Vertrauens in den Binnenmarkt sollen qualifizierte Einrichtungen, welche die Kollektivinteressen der Verbraucherinnen und Verbraucher repräsentieren, in die Lage versetzt werden, entsprechende Verbandsklagen gegen Unternehmen anzustrengen.

Die zentralen Regelungen zum Verbandsklageregister und zum Verfahrensverlauf finden sich im neuen Verbraucherrechtedurchsetzungsgesetz (VDuG). Insbesondere die das Verbandsklageregister sowie das nachgelagerte Umsetzungsverfahren betreffenden Regelungen umfassen verschiedene Datenübermittlungen und -bekanntgaben, deren Erforderlichkeit ich mit dem zuständigen Bundesjustizministerium intensiv diskutiert habe. Zwar befürworte ich die Ziele der VKR sowie des VRUG ausdrücklich als einen wichtigen Beitrag zum Schutz der Verbraucherinnen und Verbraucher, aber nur bei Beachtung der Vorgaben der DSGVO.

In Folge meiner intensiven Bemühungen konnten letztlich entscheidende Verbesserungen beim Datenschutz erreicht werden. Hierzu zählen eine datensparsame Glaubhaftmachung des erforderlichen Verbraucherquorums in der Klageschrift sowie verbesserte Regelungen zur Umsetzung der Informationspflichten der klageberechtigten Stelle bei Anmeldung der Beteiligten zum Verbandsklageregister.

Auch meine weitergehenden Bedenken, die sich insbesondere auf die verschiedenen vorgesehenen Datenübermittlungen aus dem Verbandsklageregister an das für die Verbandsklage zuständige Gericht sowie die dortigen Parteien bezogen, konnten letztlich ausgeräumt werden. Diese Datenübermittlungen sind bedingt durch das geplante gestufte Verfahren zur Geltendmachung der Verbraucheransprüche und stellen die Kehrseite der möglichst einfachen Anspruchsverfolgung im neuen Verbandsklageverfahren dar. Nach dessen Abschluss werden die Ansprüche aller beteiligten Verbraucherinnen und Verbraucher in einem sogenannten Umsetzungsverfahren durch einen bestellten Sachwalter kursorisch geprüft und ausgeglichen. Etwaige einzelfallbezogene Einwendungen können durch den betroffenen Unternehmer nur in einem sich anschließenden Rückforderungsverfahren gegenüber dem einzelnen Verbraucher bzw. der einzelnen Verbraucherin geltend gemacht werden. Zu diesem Zweck werden auch die detaillierten Ergebnisse des durchgeführten Umsetzungsverfahrens samt personenbezogener Daten der teilnehmenden Verbraucherinnen und Verbraucher benötigt. Die Offenlegung ist damit dem vereinfachten und beschleunigten Verfahren geschuldet und datenschutzrechtlich grds. nicht zu beanstanden. Im Ergebnis wird hierdurch auch nur die gleiche Informationslage hergestellt, wie sie im alternativen Individualklageverfahren ohnehin bestehen würde.

Das VRUG ist bereits in Kraft getreten. Ich werde dessen Umsetzung und praktische Anwendung weiter im Blick behalten.

5.8 Gesetz zu Videokonferenzen an Gerichten

Mit dem Gesetz zur Förderung des Einsatzes von Videokonferenztechnik in der Zivilgerichtsbarkeit und den Fachgerichtsbarkeiten sollen die Möglichkeiten zur Durchführung teil- und vollständig virtueller Gerichtsverhandlungen erweitert werden. Dies birgt Chancen für den Ausbau einer effizienteren und leistungsfähigeren Justiz, stellt jedoch auch eine datenschutzrechtliche Herausforderung dar.

Der Einsatz von Videokonferenztechnik in der Gerichtsbarkeit nimmt von Jahr zu Jahr einen höheren Stellenwert ein. Über die vordergründigen Effekte einer effizienteren und damit leistungsfähigeren Justiz hinaus werden hierdurch auch weitere Ziele verfolgt. So wird die angestrebte Digitalisierung vorangetrieben, etwa um die Teilnahme am gerichtlichen Verfahren ressourcenschonend zu ermöglichen und im Falle pandemischer Ausnahmesituationen den Gerichtsbetrieb aufrechtzuerhalten.

Mit dem Gesetz zur Förderung des Einsatzes von Videokonferenztechnik in der Zivilgerichtsbarkeit und den Fachgerichtsbarkeiten sollen insbesondere die Möglichkeiten zur Durchführung von Videokonferenzterminen im gerichtlichen Verfahren erweitert und erleichtert werden. Neben mündlichen Verhandlungen und vorgeschalteten Erörterungsterminen sind hiervon auch Beweisaufnahmen betroffen. Über die schlichte Durchführung von Videokonferenzen hinaus werden nunmehr auch Möglichkeiten zu deren Aufzeichnung und Weiterverarbeitung zur Protokollführung und bei der Gewährung von Akteneinsicht vorgesehen. Diese zentralen Neuregelungen der Zivilprozessordnung werden durch Verweisregeln in diverse weitere Gerichts- und Verfahrensordnungen übernommen. Dabei sieht der

zur Ressortabstimmung vorgelegte Entwurf umfängliche Datenverarbeitungen vor, die in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen eingreifen. Insbesondere geschützte Daten natürlicher Personen sind betroffen, auch solche der nach Art. 9 Abs. 1 DSGVO besonders geschützten Kategorien.

Mit Blick auf den großen Umfang grundgesetzlich geschützter und teilweise höchst sensibler Daten war es mir ein besonderes Anliegen, meine datenschutzrechtlichen Bedenken im Gesetzgebungsverfahren einzubringen. Auch wenn ich die Ziele des Gesetzentwurfs begrüße, so muss deren Umsetzung natürlich die Vorgaben der DSGVO beachten. Dabei habe ich in Folge meiner intensiven Bemühungen bereits einige datenschutzrechtliche Verbesserungen erreichen können. Insbesondere die vorgesehenen Ermessensentscheidungen der zuständigen Gerichte zur Gestattung oder Anordnung von Videokonferenzen bzw. deren Aufzeichnung wurden mit situationsangepassten Hinweisen in der Gesetzesbegründung unterstützt.

Dennoch konnten einige meiner Bedenken nicht bzw. nicht vollständig ausgeräumt werden. So bleibt es auch im zwischenzeitlich in das Parlament eingebrachten Regierungsentwurf grds. beim vorgenannten ermessensbasierten Ansatz. Hier hätte ich mir weitergehende gesetzliche Ausnahmen gewünscht, jedenfalls im Falle der Verhandlung über besonders sensible Daten gemäß Art. 9 Abs. 1 DSGVO. Zudem sieht der Gesetzentwurf weiterhin vor, dass Videoaufzeichnungen auch ohne Zustimmung der Beteiligten angeordnet werden können. Diese sollen zwar grds. nur der vorläufigen Protokollerstellung dienen, verbleiben jedoch letztlich dauerhaft in der Verfahrensakte, wenn ihre Inhalte nicht im absehbaren Ausnahmefall transkribiert und damit im Wortlaut in das Verhandlungsprotokoll übernommen werden. Letztlich bleibt insbesondere die Frage einer belastbaren Identifikation der Beteiligten vor Durchführung einer Videokonferenz unbeantwortet. Hier fehlt es an einer klaren Regelung. Das teilweise vorgesehene Video-Ident-Verfahren birgt hohe Risiken, auf die ich bereits seit Jahren hinweise. Es gibt immer öfter täuschend echt wirkende Audio- und auch Videomanipulationen (sogenannte Deepfakes), mit denen auch Videoidentifizierungen manipuliert werden können. Leider geht der Gesetzentwurf weder auf die Frage der betroffenen Schutzbedarfe noch auf die etwaigen Möglichkeiten einer Senkung der bestehenden Risiken ein. Soweit besonders geschützte Daten der Kategorien des Art. 9 Abs. 1 DSGVO betroffen sind, sollte die Verwendung eines Videoidentverfahrens bereits gesetzlich ausgeschlossen werden.

Sollte das Gesetz in seiner jetzigen Form beschlossen werden, so ist es Aufgabe aller nationaler Datenschutz-Aufsichtsbehörden, dessen praktische Anwendung im Blick zu behalten. Meine Zuständigkeit beschränkt sich insoweit auf die obersten Bundesgerichte; die deutliche Mehrheit aller betroffenen Gerichtsverhandlungen wird im Zuständigkeitsbereich der Landesbeauftragten für Datenschutz durchgeführt. Als Mitglied der Datenschutzkonferenz werde ich die weitere Entwicklung jedoch auch insoweit konstruktiv begleiten.

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.

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.

6 Informationsfreiheit

6.1 Allgemeines

Die Forderung nach einem Bundestransparenzgesetz, und damit die Umsetzung des im Koalitionsvertrag festgelegten Vorhabens, begleitete mich auch in diesem Jahr. Das von mir veranstaltete Symposium zur Informationsfreiheit im September 2023 sowie weitere Tagungen und Konferenzen boten mir eine Gelegenheit, meine Kernforderungen für dessen inhaltliche Ausgestaltung darzustellen und zu erläutern.

Den Schwerpunkt meiner inhaltlichen Arbeit habe ich im Berichtsjahr auf den Auf- und Ausbau von Netzwerken zur Beratung gelegt. Es ist mir ein Anliegen, dass mein Haus als Beratungshaus wahrgenommen und die Expertise meiner Mitarbeitenden schon während der Bearbeitung von Anfragen in Anspruch genommen wird. Deshalb suchen wir in verschiedenen Formaten erfolgreich den Dialog mit den Kolleginnen und Kollegen in der Bundesverwaltung.

Auch in internationale Gremien kann ich mich seit der organisatorischen Eigenständigkeit und dem personellen Aufbau des Referats sowohl auf internationaler als auch auf europäischer Ebene einbringen, um von dem Austausch mit den Kolleginnen und Kollegen zu profitieren.

6.1.1 Zehn Kernforderungen für ein Transparenzgesetz des Bundes

Im Koalitionsvertrag „Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit“ haben die Regierungsparteien vereinbart, ein Transparenzgesetz des Bundes zu verabschieden. Aus meiner Sicht muss ein solches Gesetz folgende Inhalte haben.

1. Ich fordere ein Bundestransparenzgesetz, in dem das geltende Informationsfreiheitsgesetz (IFG) modernisiert und mit dem Umweltinformationsgesetz (UIG) zusammengeführt wird.
2. Ich fordere ein Bundestransparenzgesetz, das umfangreiche proaktive Veröffentlichungspflichten normiert.
3. Ich fordere ein Bundestransparenzgesetz, dessen Kernstück ein elektronisches Transparenzportal bildet. Der Zugang zu diesem Transparenzportal muss für die informationssuchende Person ohne Preisgabe personenbezogener Daten möglich sein.
4. Ich fordere ein Bundestransparenzgesetz ohne Bereichsausnahmen.
5. Ich fordere ein Bundestransparenzgesetz, in dem die Schutzbestimmungen des IFG an die bürgerfreundlichen Schutzbestimmungen des UIG angepasst werden. Dem Informationszugang entgegenstehende Belange müssen grundsätzlich gegen das öffentliche Interesse an der Bekanntgabe abgewogen werden.
6. Ich fordere die Möglichkeit eines Antrags auf Informationszugang ohne zwingende Preisgabe personenbezogener Daten, sofern die informationssuchende Person gegenüber der informationspflichtigen Stelle eine angemessene Empfangsmöglichkeit angibt und der gewählten Form der Bekanntgabe keine zwingende gesetzliche Regelung entgegensteht.
7. Ich fordere ein Bundestransparenzgesetz, das ein klares Bekenntnis enthält, dass Transparenz und Offenheit Leitlinien für das Handeln der Verwaltung sind.
8. Ich fordere ein Bundestransparenzgesetz, das einen behördlichen Transparenzbeauftragten bei den öffentlichen Stellen des Bundes etabliert.
9. Ich fordere ein Bundestransparenzgesetz, das meinem Amt im Bereich Informationsfreiheit weitreichende Anordnungs- und Durchsetzungsbefugnisse gewährt.
10. Ich fordere ein Bundestransparenzgesetz, das von einem umfassenden Schulungsangebot für die Bundesverwaltung begleitet wird, um die Akzeptanz in der Verwaltung zu erhöhen, Vorbehalte abzubauen und eine rasche Umsetzung zu gewährleisten.

Darüber hinaus bin ich der Ansicht, dass die Informationsfreiheit Verfassungsrang erhalten sollte.

6.1.2 Abgrenzung von Umweltinformationen und amtliche Informationen nach IFG bei der Flugsicherung

Wenn die von der Deutschen Flugsicherung herausgegebenen „Nachrichten für Luftfahrer" keine Umweltinformationen sind, stellt sich die Frage, ob diese Informationen nach dem Informationsfreiheitsgesetz (IFG) herauszugeben sind.

Ein Petent rief mich an, da sein Antrag auf Herausgabe der Nachrichten für Luftfahrer (NfL) von der Deutschen Flugsicherung GmbH (DFS) abgelehnt wurde. Bei den NfL handelt es sich um eine aufbereitete Sammlung von rechtlichen Vorgaben sowie aktuellen Informationen im Zusammenhang mit der Luftfahrt, die Piloten kostenpflichtig zugänglich sind.

Die DFS ist der Auffassung, dass die antragsgegenständlichen Informationen keine Umweltinformationen darstellen und somit der Anwendungsbereich des UIG nicht eröffnet sei. Auch ein Anspruch nach dem IFG bestehe nicht, da die DFS lediglich mit der hoheitlichen Erbringung der Flugverkehrskontrolldienste beliehen sei. Die Sammlung und Aufbereitung sowie Verbreitung der NfL sei indes dem Flugberatungsdienst zuzuordnen. Diese Aufgabe werde nicht hoheitlich erbracht, sondern sei eine private Tätigkeit im Wettbewerb, so dass das Sammelwerk NfL keine amtliche Information im Sinne des IFG darstelle und der Antrag auf Übersendung abzulehnen sei.

Der Petent geht davon aus, dass es sich um Umweltinformationen handele, weil die NfL Regelungen und Anweisungen enthielten, die einen Einfluss darauf haben, wie und wo Flugzeuge Emissionen freisetzen. Weiterhin würden sich die Informationen auf die Lärmbelastung im Umfeld des Flughafens auswirken und damit mittelbar auch auf natürliche Lebensräume und die Artenvielfalt.

Ich habe dem Petenten mitgeteilt, dass es sich bei den NfL um flugtechnisch relevante Nachrichten handelt, die für eine sichere und geordnete Durchführung von Flügen notwendig sind. Die NfL stellen keine Datensammlung von Umweltinformationen dar, ebenso wenig ist das Veröffentlichen der NfL selbst – im Gegensatz zum tatsächlichen Flugverkehr – eine Tätigkeit mit Auswirkung auf Umweltbestandteile. Das UIG ist nach meiner Einschätzung nicht anwendbar.

Auch das IFG halte ich für nicht anwendbar, da es sich bei der DFS um eine juristische Person des Privatrechts handelt. Als juristische Person des Privatrechts kann die DFS nur unmittelbare Anspruchsgegnerin sein, wenn ihr die Eigenschaft einer Behörde zukommt. Dies ist dann der Fall, wenn die DFS mit der hoheitlichen Wahrnehmung bestimmter Verwaltungsaufgaben im eigenen Namen betraut ist und damit im Rechtssinne als Beliehene handelt. Ausweislich des § 27c Abs. 2 Satz 2 Luftverkehrsgesetz stellen Flugsicherungsdienste nach den Nummern 2 bis 5 (und damit der Flugberatungsdienst) Unterstützungsdienste für die Flugsicherung dar. Sie sind keine hoheitlichen Aufgaben des Bundes. Die NfL sind vom Flugberatungsdienst umfasst. Damit erbringt die DFS diesen Dienst außerhalb einer Beleihung durch den Bund. Selbst wenn man einen Fall des § 1 Abs. 1 Satz 3 IFG annehmen würde, wonach eine natürliche Person oder juristische Person des Privatrechts einer Behörde im Sinne des § 1 Abs. 1 Satz 1 IFG gleichgestellt wird, soweit sich eine Behörde dieser juristischen Person zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient, wäre ein IFG Antrag nach § 7 Abs. 1 Satz 2 IFG an die jeweilige Behörde zu richten, die sich der natürlichen oder juristischen Person des Privatrechts bedient. Auch bei dieser Konstellation wäre die DFS nicht die Anspruchsgegnerin.

6.1.3 7. Fachsymposium zur Informationsfreiheit

Am 14. und 15. September 2023 habe ich in Berlin das 7. Fachsymposium zur Informationsfreiheit veranstaltet.

Mit vielen interessierten Teilnehmenden aus dem Bundestag, der Justiz und der Rechtswissenschaft, aus den Bundesbehörden und dem Kreis der Landesbeauftragten nimmt das Symposium längst einen festen Platz im Diskurs von Verwaltung, Wissenschaft sowie Zivilgesellschaft ein. Es bietet eine etablierte Plattform für eine Bestandsaufnahme und den Erfahrungsaustausch zu Recht und Praxis der Informationsfreiheit. Nachdem das letzte Symposium im Jahr 2021 pandemiebedingt als digitale Veranstaltung stattfand, konnte die Veranstaltung in diesem Jahr erfreulicherweise wieder in Präsenz in der Landesvertretung Rheinland-Pfalz in Berlin durchgeführt werden.

Der thematische Schwerpunkt des ersten Tages lag auf Transparenzgesetzen. Meine Kollegen aus Hamburg und Rheinland-Pfalz haben ihre Erfahrungen mit diesen moderneren Gesetzen dargestellt, die – neben dem Informationszugang auf Antrag – auch proaktive Veröffentlichungspflichten auf einem staatlich betriebenen Portal für eine große Zahl an Kategorien von Informationen normieren.

Die beiden Informationsfreiheitsbeauftragten berichteten, dass diese Transparenzgesetze eine Erfolgsge-

schichte seien, was sich unter anderem an den beständig hohen Zugriffszahlen auf die Portale und an dem etablierten Bewusstsein für die Bedeutung staatlicher Transparenz bei den verpflichteten Stellen ablesen lässt.

Einen vertieften Einblick in die Pläne des Bundesgesetzgebers für ein Bundestransparenzgesetz ermöglichte ein Vortrag durch das Bundesministerium des Innern und für Heimat. Als wesentliches neues Element soll die proaktive Pflicht zur Veröffentlichung bestimmter Kategorien amtlicher Informationen eingeführt werden. Daneben soll auch ein Rechtsanspruch auf open-data Teil dieses Gesetzes werden. Der Informationszugang auf Antrag bleibt aber wie bisher bestehen.

Den Abschluss des ersten Tages bildete eine Diskussionsrunde, die sich mit der Bedeutung der Verwaltungsdigitalisierung für transparentes Verwaltungshandeln auseinandersetzte.

Am zweiten Tag wurde die Informationsfreiheit aus den verschiedensten Perspektiven beleuchtet. Akteure aus der Wissenschaft, der Anwaltschaft, der Justiz und der Zivilgesellschaft haben ihre Erfahrungen in der Arbeit mit dem Informationsfreiheitsgesetz geschildert.

6.1.4 IFG-Statistik für das Jahr 2023

Statistische Auswertungen für den Berichtszeitraum

In meiner Beratungs- und Kontrollpraxis und im Austausch mit den Behörden des Bundes konnte ich feststellen, dass die Anfragen nach dem IFG und dem UIG deutlich komplexer werden. Dieser Trend ist auch bei den an mich gerichteten Anträgen erkennbar. Dies betrifft sowohl die Tiefe, in der nach Informationen gefragt wird, als auch den Umfang der gestellten Anträge und die Zeiträume, auf die sich Anträge beziehen. Die Anträge hatten beispielsweise politische Vorhaben oder Spezialthemen aus dem medizinischen oder dem technischen Bereich zum Gegenstand. Das Recht auf Informationszugang wird erkennbar auch mehr und mehr von Personen genutzt, die bereits über einen Sachverhalt informiert sind.

Für die Bearbeitung bedeutet das, dass vermehrt Drittbeteiligungsverfahren durchgeführt werden müssen, um Fragen des geistigen Eigentums oder von Betriebs- oder Geschäftsgeheimnissen zu klären. Es erfordert zudem einen erhöhten Koordinierungsaufwand in den Behörden, wenn zahlreiche, an einem Vorgang beteiligte Fachbereiche eingebunden werden müssen. Und schließlich bedeutet dieser Trend für die auskunftspflichtigen Stellen einen größer werdenden Bearbeitungsaufwand

in fachlicher und zeitlicher Hinsicht, auch wenn gleichzeitig die Zahl der Anträge teilweise abnimmt.

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

Mich erreichten im Berichtszeitraum insgesamt 543 Eingaben. Damit ist die Zahl der Eingaben im Vergleich zum Vorjahr leicht gestiegen.

In 372 Fällen riefen mich Petenten nach § 12 Abs. 1 IFG an und rügten eine Verletzung ihres Rechts auf Informationszugang nach dem IFG.

Im Berichtszeitraum erreichten mich elf Bitten um Vermittlung bei Anträgen nach dem UIG. Hierbei entfielen vier Vermittlungsbitten auf das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz und seinen Geschäftsbereich. 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, weil z. B. das IFG der Länder betroffen war.

Bezogen auf die Ressorts und ihrer Geschäftsbereiche verteilen sich die Eingaben wie aus der nachfolgenden Grafik ersichtlich. Die höchste Zahl der Eingaben betraf das Bundesministerium des Inneren und seinen Geschäftsbereich.

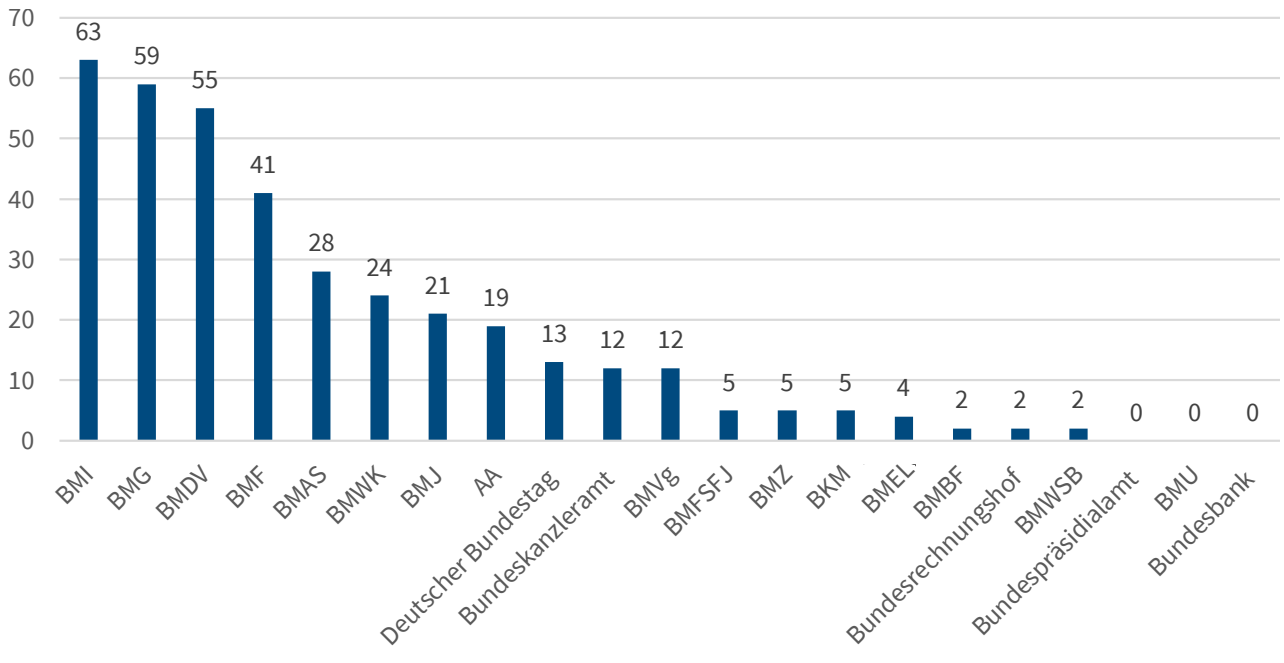
Im Berichtszeitraum musste ich erfreulicherweise keine Beanstandung androhen oder gar aussprechen.

IFG-Anträge an meine Behörde

Im Berichtszeitraum erreichten mich insgesamt 118 Anträge auf Informationszugang. Diese Anträge richteten sich zum einen auf den Zugang zu Informationen in meiner Tätigkeit als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, wie etwa Stellungnahmen in Gesetzesvorhaben auf nationaler oder europäischer Ebene. Zum anderen wurde um Zugang zu Akteninhalten im Rahmen von eigenen, an meine Behörde gerichteten Vermittlungsbitten nach deren Abschluss nachgesucht. In diesem Kontext ist auch zu berücksichtigen, dass ich auf meiner Internetpräsenz den Bereich meiner proaktiven Veröffentlichung ausbaue. Beispielsweise veröffentliche ich Rundschreiben an die von mir beaufsichtigten Stellen und möglichst alle Kontrollberichte. Dies hat zur Folge, dass das Antragsaufkommen nach dem IFG an mein Haus rückläufig ist. Aus meiner Sicht ist die proaktive Veröffentlichung die adäquate Form des Informationsmanagements zwischen interessierten Personen und Bundesbehörden.

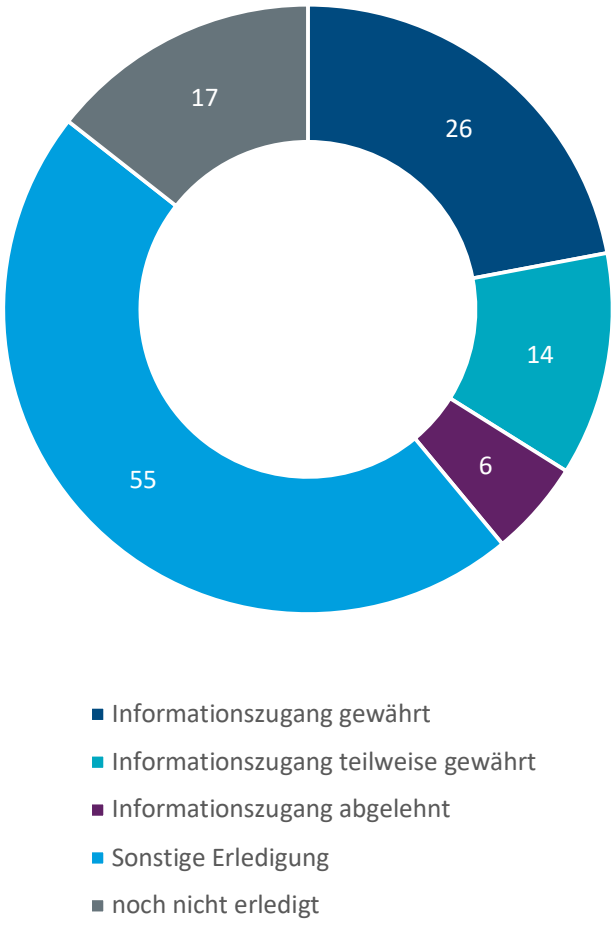
Aus der Abbildung ergibt sich die Verteilung der (teilweisen) Zugangsgewährung, der Zugangsablehnung und der sonstigen Erledigung im Jahr 2023. Fälle der sonstigen Erledigung umfassen beispielsweise Vorgänge, bei denen der Antrag wegen voraussichtlicher Gebühren-

Anrufungen nach § 12 IFG im Berichtszeitraum nach Ressorts



pflichtigkeit nicht weiter verfolgt wird oder Vorgänge, bei denen der Antragsteller nicht hinreichend mitwirkt. Gründe für Ablehnungen waren im Wesentlichen weiterhin andauernde Beratungen oder die Tatsache, dass die erbetene Information bei meiner Behörde nicht vorliegt.

IFG-Anträge an meine Behörde im Jahr 2023



6.2 Gremien

Im Berichtsjahr hatte ich den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten aus Bund und Ländern (IFK) inne. Deren Ziel ist es, das Recht auf Zugang zu amtlichen Informationen zu fördern und für die Weiterentwicklung der Informationsfreiheit einzutreten.

Auf internationaler Ebene engagiere ich mich als Mitglied des Executive Committees in der Internationalen Konferenz der Informationsfreiheitsbeauftragten (ICIC). Die ICIC bringt Informationsbeauftragte, Ombudsleute und andere Gremien zusammen, die mit der Überwachung der Umsetzung der Gesetzgebung zum Zugang zu öffentlichen Informationen betraut sind. Die ICIC verfolgt das Anliegen, den Schutz und die Förderung des Zugangs zu öffentlichen Informationen als Grundpfeiler der sozialen, wirtschaftlichen und demokratischen Regierungsführung sicherzustellen.

6.2.1 Konferenz der Informationsfreiheitsbeauftragten in Deutschland

Im Jahr 2023 hatte ich den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) inne. Inhaltlicher Schwerpunkt meines Vorsitzes war die umfassende Weiterentwicklung staatlicher Transparenz in Zeiten der Digitalisierung.

Die IFK tagte am 14. Juni 2023 in Berlin und am 7. November 2023 in Bonn. Beide Konferenzen wurden inhaltlich vom Arbeitskreis Informationsfreiheit (AKIF) vorbereitet, der im Mai und im September des Berichtsjahres tagte.

Im Rahmen der Sitzung vom 14. Juni 2023 verabschiedete die IFK die Entschließung „Die Demokratie braucht starke Medien – Bundespressegesetz jetzt einführen!“. Die IFK fordert den Bundesgesetzgeber auf, zeitnah ein effizientes Bundespressegesetz zu schaffen, das der herausragenden Rolle der Presse und den Erfordernissen einer modernen Medienlandschaft Rechnung trägt.

Der Bund verfügt im Gegensatz zu den Ländern nicht über ein Pressegesetz. Bis zum Jahr 2013 hat sich die Presse für ihren Auskunftsanspruch auch gegenüber Bundesbehörden auf die Pressegesetze der Länder berufen. 2013 hat das Bundesverwaltungsgericht jedoch entschieden, dass dies unzulässig sei. Vielmehr ergebe sich der presserechtliche Auskunftsanspruch gegenüber Bundesbehörden unmittelbar aus dem Recht auf Pressefreiheit aus dem Grundgesetz.

Aus diesem Grund begrüßt es die IFK, dass sich die amtierende Bundesregierung in ihrem Koalitionsvertrag darauf verständigt hat, diese Lücke zu schließen. Eine starke Presse ist für eine lebendige Demokratie existenziell. Dazu ist sie auf einen raschen und umfassenden Informationszugang angewiesen.

Im Rahmen der Konferenz vom 7. November 2023 verabschiedete die IFK zwei Handreichungen. Die eine konkretisiert, wie die Umsetzung von „Informationsfreiheit by Design“ in der Verwaltung gelingen kann. Die andere ist einen Leitfaden zum Aufbau staatlicher Transparenzportale.

Zudem verabschiedet die IFK drei Entschließungen. In der Entschließung „Moderne Informationsfreiheitsgesetze bundesweit“ fordern die Informationsfreiheitsbeauftragten die Abschaffung der bestehenden „drei

Klassen Gesellschaft“ hinsichtlich der Möglichkeit, in Bund und Ländern an Informationen öffentlicher Stellen zu gelangen. Noch immer gibt es in Bayern und in Niedersachsen keinen gesetzlich normierten allgemeinen und voraussetzungslosen Zugang zu amtlichen Informationen. In einigen Ländern bestehen hingegen bereits umfassende Pflichten zur proaktiven Veröffentlichung auf Transparenzportalen in modernen Transparenzgesetzen. Im Bund und allen anderen Ländern gilt der Informationszugang auf Antrag. Die IFK fordert den Bundes- und die Landesgesetzgeber dazu auf, mit modernen Transparenzgesetzen das Recht auf Informationszugang deutschlandweit auf ein einheitlich hohes Niveau zu bringen.

Weitere Entschließungen waren „Künstliche Intelligenz als Instrument für proaktive Informationsbereitstellung nutzen“ und „25 Jahre Århus-Konvention – Veröffentlichungsanspruch muss ins Gesetz!“. Nach 25 Jahren Århus-Konvention ist die so wichtige proaktive Veröffentlichung von Umweltinformationen in Deutschland immer noch abhängig vom Transparenzwillen der Behörden.

Derzeit sehen die Umweltinformationsgesetze in Deutschland vor, dass Behörden Umweltinformationen proaktiv und nicht nur auf Antrag Einzelner veröffentlichen müssen. Allerdings stellt diese Pflicht zur „Unterrichtung der Öffentlichkeit“ in den allermeisten Ländern und auf Bundesebene keinen selbständigen, einklagbaren Anspruch für jedermann dar. Bei Verstößen gegen die Pflicht fehlt somit die Möglichkeit zur Durchsetzung. Die Nichtbeachtung ist nach aktueller Gesetzeslage nicht gerichtlich überprüfbar und die bloße Veröffentlichungspflicht droht zu verpuffen. Nur in den Transparenzgesetzen von Hamburg, Bremen und Rheinland-Pfalz besteht bislang – in gewissem Maße – ein subjektives Recht auf Veröffentlichung.

Um die Bürgerinnen und Bürger bei der Wahrnehmung ihres Rechts auf Zugang zu Umweltinformationen – ganz im Geiste der Århus-Konvention – zu stärken, ist eine Novellierung des Umweltinformationszugangsrechts nötig. Die IFK fordert die bisher untätigen Gesetzgeber dazu auf, die Verpflichtung zur Unterrichtung der Öffentlichkeit zu modernisieren und als selbständigen Anspruch zu formulieren.

6.2.2 Internationale Konferenz der Informationsfreiheitsbeauftragten

Im Berichtsjahr fand die 14. Internationalen Konferenz der Informationsfreiheitsbeauftragten – der International Conference of Information Commissioners (ICIC) – in Manila statt.

Das Thema der Konferenz lautete: „Brückenschlag zwischen Informationen und Nationen: Konkretisierung der globalen Rolle des Zugangs zu Informationen für die Bewahrung der Demokratie, für die Inklusion und die Entwicklung“. Eine Vertreterin meines Hauses hat zu dem Thema „Der politische Rahmen für das Recht auf Informationszugang in der globalen Arena: Paradigmenwechsel und Reformen“ bei einer Podiumsdiskussion gesprochen und vom status quo auf Bundesebene berichtet. Dass der Bund derzeit auf dem Weg von der Informationsgewährung auf Antrag zu einem Transparenzgesetz ist, sorgt international immer wieder für Erstaunen. Transparenzgesetze sind mittlerweile der globale Standard in demokratischen Systemen. Ich wünsche mir, dass wir bald mit einem modernen Transparenzgesetz aufschließen werden.

Während der Konferenz wurden Perspektiven zu zahlreichenden spannenden Transparenzthemen ausgetauscht, beispielsweise zu den Innovationsmöglichkeiten, die sich durch die Ausnahmephase der Covid 19-Pandemie ergeben haben, zu den Risiken und Möglichkeiten von Künstlicher Intelligenz beim Informationszugang, die Chancen offener Auftragsvergabe für Kosteneffizienz im öffentlichen Sektor oder die Rolle der Informationsfreiheit für die demokratische Entwicklung von Schwellenländern.

Die Konferenz findet regelmäßig über einen Zeitraum von drei Tagen statt. Der erste Tag ist mit Vorträgen und Diskussionen im Plenum gewidmet. Die beiden anderen Tage beginnen und enden auch im Plenum, bieten aber zudem die Möglichkeit sich inhaltlich zu spezialisieren, da während des Tages drei Panel mit stündlich wechselnden Themen, Sprechenden und Diskutanten parallel laufen. Auf den Treffen der regionalen Netzwerke findet der Austausch mit den Informationsfreiheitsbeauftragten und den Ombudspersonen aus ganz Europa statt. Auch die Zivilgesellschaft informiert in eigenen Panels über ihre Themen und ihre Arbeit. Die Kernthemen der ICIC – freier Zugang zu Informationen, Meinungsfreiheit und Korruptionsbekämpfung – sind weltweit auf eine starke Zivilgesellschaft als Motor und Wächter angewiesen.

Im Nachgang der dreitägigen Konferenz trifft sich das ICIC Executive Committee und evaluiert die Veranstaltung, um sich kontinuierlich zu verbessern und die angebotenen Themen und Formate an den Informations- und Beratungsbedarf und die Interessen der Teilnehmenden anzupassen. So wird sichergestellt, dass die jährliche Konferenz der Informationsfreiheit verbundene Menschen aus aller Welt anzieht und einen echten inhaltlichen Mehrwert bieten kann.

Ich engagiere mich in der ICIC als Mitglied des Executive Committee. Mein Haus bringt sich zudem inhaltlich in der Law and Cases Working Group und im Planning Committee für die kommende ICIC 2024 in Albanien ein.

6.3 Erfahrungsaustausch

Anders als im Datenschutzrecht gibt es keine europaweit einheitlichen Gesetze, die den Zugang zu Informationen regeln. Gleichwohl bietet der Austausch über die praktische Handhabung und die Konzeption verschiedener Informationsfreiheitsgesetze viele neue Ansatzpunkte, die eigene Arbeit einer Überprüfung zu unterziehen und Potential für Verbesserungen zu erkennen. Die positiven Erfahrungen mit meinem Erfahrungsaustausch auf nationaler Ebene haben mich darin bestärkt, den Austausch auch auf europäischer Ebene zu suchen.

6.3.1 Erfahrungsaustausch der Bundesbehörden zur Informationsfreiheit

Neben dem Erfahrungsaustausch der obersten Bundesbehörden habe ich erstmals auch zu einem Erfahrungsaustausch mit verschiedenen Bundesoberbehörden und –anstalten zur Bearbeitungspraxis des Informationsfreiheitsgesetzes (IFG) und Umweltinformationsgesetzes (UIG) eingeladen.

Der im Jahr 2022 wiederaufgenommene Erfahrungsaustausch der obersten Bundesbehörden zur Informationsfreiheit hat sich als Format etabliert. Die Veranstaltung fand im Berichtsjahr an mehreren Terminen statt. Aufgrund dieser positiven Erfahrungen veranstalte ich seit diesem Jahr auch einen Erfahrungsaustausch mit verschiedenen Bundesoberbehörden und -anstalten in Bonn. Meine Absicht ist hier vor allem, eine Plattform für den Austausch unter den mit der Bearbeitung von Informationsfreiheitsanträgen befassten Personen in den Bundesoberbehörden zu schaffen.

Im Rahmen der Treffen wurde unter anderem über aktuelle Entwicklungen in der Rechtsprechung und die konkreten Auswirkungen auf die praktische Arbeit diskutiert. Als relevanter Punkt stellte sich dabei beispielsweise die Verfügungsberechtigung einer informationspflichtigen Stelle dar. Einige Aspekte dieser wichtigen Frage sind in der Rechtsprechung und Wissenschaft weiterhin ungeklärt. Praktische Relevanz erlangt die Verfügungsberechtigung beispielsweise dann, wenn ein Dokument bei zwei Bundesbehörden vorhanden ist. Nach der Rechtsprechung des Bundesverwaltungsgerichts ist das Vorhandensein einer amtlichen Information notwendige, aber nicht hinreichende Bedingung für die Verfügungsberechtigung. Es wurde diskutiert, ob die Entscheidung über die Herausgabe stets nur der Stelle zuzuordnen ist, die das Dokument erstellt hat. Ferner wurden verschiedene Fragen des Gebührenrechts diskutiert.

Aus den Diskussionen und Beiträgen ergaben sich wertvolle Erkenntnisse für die praktische Arbeit. Daneben bietet das Format auch die Möglichkeit, in einen Austausch über allgemeine Fragen wie z. B. die Organisation der IFG-Bearbeitung, zu treten. Den Kolleginnen und Kollegen aus den verschiedenen Behörden wird dabei auch meine Ombudsfunktion als Bundesbeauftragter für die Informationsfreiheit im Vermittlungsverfahren erläutert.

Über das große Interesse an diesem Angebot und die gehaltvolle und engagierte Diskussion im Rahmen der ersten Veranstaltung habe ich mich sehr gefreut. Aufgrund der positiven Resonanz beabsichtige ich, auch diesen Austausch fortzusetzen.

6.3.2 Case Handling Workshop zur Informationsfreiheit

Vom 16. bis 17. Mai 2023 fand erstmalig ein von mir veranstalteter Case Handling Workshop zur Informationsfreiheit im Europäischen Haus in Berlin statt.

30 Teilnehmende aus 15 Europäischen Ländern und von der europäischen Bürgerbeauftragten haben sich zwei Tage lang intensiv über Erfahrungen und aktuelle Fragestellungen in der praktischen Anwendung des Informationsfreiheitsrechts ausgetauscht.

Die Europäische Bürgerbeauftragte

Die Europäische Bürgerbeauftragte und ihr Team helfen Menschen, Organisationen und Unternehmen, indem sie Verwaltungsbeschwerden nachgehen und allgemeinere systemische Fragen auf EU-Ebene untersuchen. Die Vorschläge und Empfehlungen der Bürgerbeauftragten tragen dazu bei, in den EU-Organen und -Einrichtungen hohe Standards hinsichtlich Rechenschaftspflicht und Transparenz zu wahren.

Am ersten Tag des Workshops wurden die unterschiedlichen Situationen in den verschiedenen teilnehmenden Ländern beleuchtet. Hierbei lag ein besonderes Augenmerk auf den Herausforderungen der einzelnen Ombudsstellen in der täglichen Arbeit sowie auf Transparenzplattformen mit proaktiven Veröffentlichungspflichten. Der zweite Tag des Workshops stand dagegen

ganz im Zeichen des Zugangs zu Umweltinformationen und wurde abgerundet durch Betrachtungen zum Ausgleich gegenläufiger Interessen bei der Fallbearbeitung.

Aufgrund der durchweg positiven Resonanz aus dem Kreis aller Teilnehmenden ist für das kommende Jahr eine Folgeveranstaltung geplant. Als möglicher Gastgeber hat Spanien Interesse geäußert. Aus meiner Sicht ist es wünschenswert, aus der gelungenen Auftaktveranstaltung ein etabliertes Format und eine Plattform für den europäischen Erfahrungsaustausch zu praktischen Anwendungsfragen des Informationsfreiheitsrechts zu entwickeln. Mein Haus hat deshalb die Aufgabe des Sekretariats übernommen, um das Fortbestehen des Formats zu gewährleisten.

6.4 IFG-Vermittlungsverfahren

Jeder kann den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit anrufen, wenn er sein Recht auf Informationszugang nach dem Informationsfreiheitsgesetz (IFG) bzw. Umweltinformationsgesetz als verletzt ansieht. Von diesem Recht wurde im Berichtsjahr 372 Mal Gebrauch gemacht. Gegenstand der Anrufungen waren zunehmend komplexere rechtliche Fragestellungen. Ebenso habe ich festgestellt, dass die an die öffentlichen Stellen des Bundes gerichteten IFG-Anträge immer umfangreicher und detaillierter werden.

6.4.1 Problem erkannt, Gefahr gebannt

Von der Unanbringlichkeit eines IFG-Antrags bei der Agentur für Arbeit Hamburg zu einer grundsätzlichen Problemlösung für alle Dienststellen im Zuständigkeitsbereich der Bundesagentur für Arbeit

Eine Petentin wandte sich mit der Bitte um Vermittlung an mich, weil sie Schwierigkeiten hatte, ihren IFG Antrag bei der Agentur für Arbeit Hamburg per E-Mail anzubringen. Das Service Center der Agentur für Arbeit wies die Antragstellerin wiederholt darauf hin, dass ihr Anliegen nicht abschließend bearbeitet werden könne, da noch weitere Informationen von ihr benötigt würden und bat um Verständnis, dass ihr Anliegen aus Gründen des Datenschutzes nicht per E-Mail bearbeitet werden könne. In dem Vermittlungsverfahren stellte die umsichtige Petentin selbst die Vermutung auf, dass das eigentliche Problem in dem Umgang mit entsprechenden E-Mail-Anfragen bei dem der Agentur für Arbeit Hamburg vorgeschalteten Service Center liegen könnte. Sie wies darauf hin, dass die Vorgaben bzw. Leitlinien für die Bearbeitung von Anfragen per E-Mail („EMB-Arbeitshilfen für die Service Center SGB III“) eine Antragsstellung nach dem IFG nicht hinreichend abbilden würden.

Auf meine Bitte um Stellungnahme nahm die Zentrale der Bundesagentur für Arbeit in Nürnberg den Vorfall zum Anlass, die den Service Centern zur Verfügung stehenden Arbeitsmittel daraufhin zu überprüfen, ob ausreichend Hinweise zur Vorgehensweise bei per E-Mail eingehenden IFG Anträgen vorhanden sind. Nach Auskunft der BA wurden dort mittlerweile klarstellende Ergänzungen vorgenommen und die Service Center entsprechend unterrichtet.

Aus meiner Sicht illustriert der Vorgang eindrücklich, wie bestenfalls aufgrund des konstruktiven Zusammenwirkens aller Beteiligten eine Problemlösung gefunden werden kann, die weit über den Einzelfall hinausreicht.

6.4.2 Zur Gefährdung der öffentlichen Sicherheit und rechtlichen Einordnung interner Vertraulichkeitsvereinbarungen

Der Ausschlussgrund des § 3 Nr. 2 IFG setzt die Darlegung von Anhaltspunkten für eine konkrete Gefährdung der öffentlichen Sicherheit voraus. Eine abstrakte Gefahr für das Schutzgut genügt nicht. Interne Vertraulichkeitsvereinbarungen können dem Informationszugang nur entgegenstehen, soweit hierdurch ein Ausschlussgrund nach dem IFG erfüllt wird.

Mehrere Petenten beantragten die Herausgabe einer an Hersteller von Covid-19-Impfstoffen gerichteten Unterrichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Unterrichtung enthielt Informationen über eine mögliche Gefährdung von Geschäftsprozessen aufgrund einer zivilgesellschaftlichen Online-Kampagne. Diese Anträge wurden unter Hinweis auf die Gefährdung der öffentlichen Sicherheit (§ 3 Nr. 2 IFG) vollumfänglich abgelehnt. Das BSI führte zur Begründung aus, dass die gewünschten Unterlagen Informationen zu verwaltungsinternen Abläufen und Strukturen sowie Informationen zu möglichen Aktivitätsformen mit gegebenenfalls technischen Auswirkungen auf den Geschäftsbetrieb der Betroffenen enthielten. Es sei eine nicht mehr zu kontrollierende Veröffentlichung von Abwehrhinweisen des BSI und eine Begünstigung zukünftiger Angriffe zu befürchten. Die begehrten Informationen seien zudem durch ein Non-Disclosure-Agreement (Vertraulichkeitsabrede) geschützt.

Wenngleich ich die Argumentation des BSI abstrakt für nachvollziehbar halte, konnte ich nach Einsichtnahme in die antragsgegenständlichen Unterlagen keine hinreichende Grundlage für eine vollumfängliche Ablehnung der Anträge erkennen. Im Lichte des weiten Schutzumfangs des § 3 Nr. 2 IFG erscheint eine enge Auslegung des Ausschlussgrundes nach den üblichen Auslegungsregeln sachgerecht. Die Darlegung von tatsächlichen An-

haltspunkten für eine konkrete und nicht nur abstrakte Gefahrenlage obliegt der informationspflichtigen Stelle. Die hinreichende Wahrscheinlichkeit des Eintritts eines Schadens für die öffentliche Sicherheit konnte nach meiner Auffassung jedenfalls nicht hinsichtlich des Bekanntwerdens sämtlicher antragsgegenständlicher Informationen dargelegt werden. Ich habe das BSI deshalb darauf hingewiesen, dass dem Schutz öffentlicher Belange, auch unter Berücksichtigung des gesetzlichen Auftrags als nationale Cyber-Sicherheitsbehörde, im konkreten Fall durch eine Unkenntlichmachung einzelner Passagen begegnet werden kann.

Soweit zudem interne Vertraulichkeitsvereinbarungen die Geheimhaltung des gesamten Dokuments vorsehen, kann dies den Anspruch auf Informationszugang nur ausschließen, wenn hierdurch ein Ausnahmetatbestand nach dem IFG verwirklicht wird. Die gesetzlich vorgesehenen Ausschlussgründe dürfen nicht durch interne Vereinbarungen unterlaufen werden. Bereits in vergangenen Tätigkeitsberichten (2. TB-IFG Nr. 2.1.7, vgl. auch 3. TB-IFG Nr. 3.2.3) habe ich darauf hingewiesen, dass der Informationsanspruch der Bürgerinnen und Bürger nicht in der Verfügungsmacht der Verwaltung steht.

Trotz meiner Anregungen konnte in den Vermittlungsverfahren keine Einigung im Sinne einer Abänderung Entscheidung des BSI erzielt werden. Dennoch begrüße ich es, dass das BSI sich auf meine Bitte hin bereit erklärte, die aufgeworfenen rechtlichen und technischen Fragen sachlich, ausführlich und ergebnisoffen mit meinen Mitarbeiterinnen und Mitarbeitern zu erörtern.

6.5 Beratungs- und Kontrollbesuche

Im Berichtsjahr führte ich drei Beratungs- und Kontrollbesuche durch. Insgesamt lässt sich dabei feststellen, dass die Bearbeitung von IFG- und UIG-Anträgen in den besuchten Häusern professionell und mit großer Expertise erfolgt. Die Qualität der Bearbeitung verbessert sich bei guter Organisation der Abläufe und eingespielter Zusammenarbeit der Referate erkennbar. Ebenso verkürzen klar definierte Prozesse die Bearbeitungsdauer der Antragsverfahren. Die Beratungs- und Kontrollbesuche bieten mir einen unverzichtbaren Einblick in die Antragsbearbeitung und eröffnen dadurch die Möglichkeit einer fundierten, auf die besuchte Stelle zugeschnittenen Beratung.

6.5.1 Beratungs- und Kontrollbesuch im BMDV

Im Bundesministerium für Digitales und Verkehr (BMDV) ist ein grundlegendes und wachsendes Bewusstsein für die Bedeutung der Informationsfreiheit zu erkennen.

Im März 2023 führte ich einen Beratungs- und Kontrollbesuch beim BMDV durch. Aufgrund der großen Zahl an IFG-Anträgen wurde eine Stichprobe der Verfahren aus den Jahren 2019 bis 2022 überprüft.

Die Anwendung des IFG im BMDV erfolgt mittlerweile bürger- und serviceorientiert und die Verfahrensvorschriften sowie die materiell-rechtlichen Vorgaben des IFG werden im Wesentlichen beachtet. Phasenweise kam es zu Fristüberschreitungen bei der Bearbeitung der IFG-Anträge.

Die Erfassung von IFG-Anträgen erfolgt zentral bei einem Referat in der Zentralabteilung, das auch die weitere Bearbeitung der Anträge im Haus koordiniert. Die inhaltliche Bearbeitung und Entscheidung über den IFG-Antrag, einschließlich Bescheiderstellung, obliegt den Fachreferaten. Das Referat in der Zentralabteilung leistet umfangreiche Beratung und sonstige Hilfestellung, z. B. durch ausführliche hausinterne Regelungen und Musterformulare.

Allerdings war sowohl in der Tenorierung als auch in der Begründungsdichte der Bescheide ein heterogenes Bild festzustellen. Die Durchführung der Drittbeteiligungsverfahren konnte nur teilweise überprüft werden, da diese weitgehend nicht in den zur Verfügung gestellten Akten des Referats der Zentralabteilung enthalten waren. Soweit die Drittbeteiligungsverfahren überprüft werden konnten, waren die entsprechenden Schreiben gelegentlich eher pauschal gehalten. Zu dem festgestellten Verbesserungsbedarf bei der Tenorierung und Begründung der Bescheide und bei der Durchführung von Drittbeteiligungsverfahren habe ich Hinweise und Anregungen gegeben.

Die Gebührenpraxis des BMDV stellt sich als einheitlich und sachgerecht dar. Hinweise auf eine abschreckende Gebührenpraxis konnte ich nicht erkennen.

Zum Kontrollbericht geht's hier:

(QR-Code scannen oder klicken)

6.5.2 Beratungs- und Kontrollbesuch bei der BNetzA

Im August 2023 führte ich einen Beratungs- und Kontrollbesuch bei der Bundesnetzagentur (BNetzA) in Bonn durch. Gegenstand des Besuchs war die Bearbeitung von Anträgen nach dem Informationsfreiheitsgesetz (IFG) und dem Umweltinformationsgesetz (UIG).

Aufgrund der Vielzahl von IFG-Anträgen an die BNetzA habe ich eine umfangreiche Überprüfung der Verfahren aus den Jahren 2019 bis 2023 vor Ort bei der BNetzA in Bonn durchgeführt. Die an die BNetzA gestellten IFG-Anträge sind auf alle Tätigkeitsbereiche ihrer breit gefächerten Aufgaben gerichtet. Regelmäßig erfordern IFG-Anträge auch die Durchführung eines Drittbeteiligungsverfahrens, da Rechte Dritter, insbesondere Betriebs- und Geschäftsgeheimnisse, betroffen sein können. Die Prüfung von Betriebs- und Geschäftsgeheimnissen im Sinne von § 6 S. 2 IFG bei der BNetzA erfolgte weitestgehend sachgemäß und war nicht zu beanstanden. Insbesondere die geprüften Vorgänge, die von den bei der BNetzA als Regulierungsbehörde eingerichteten Beschlusskammern bearbeitet wurden, wiesen eine fundierte Prüfung des Vorliegens von Betriebs- und Geschäftsgeheimnissen auf. Zu weiteren Details der Verfahrensweise habe ich Hinweise und Anregungen gegeben.

Die Bearbeitung der IFG/UIG-Anträgen erfolgt bei der BNetzA dezentral in den jeweiligen Fachbereichen mit umfangreicher fachlicher und koordinierender Unterstützung von zentraler Stelle. Die Antragsbearbeitung erfolgte insgesamt bürger- und serviceorientiert. Dabei war eine offene Haltung gegenüber der Informationsfreiheit erkennbar. Auf der Website der BNetzA kann zudem auch auf eine Vielzahl von Publikationen und digitalen Angeboten zugegriffen werden. Insbesondere gibt ein umfangreiches Datenportal Zugriff auf Daten zu den regulierten Märkten.

Zum Kontrollbericht geht's hier:

(QR-Code scannen oder klicken)

6.5.3 Beratungs- und Kontrollbesuch beim BMWK

Die Bearbeitung von IFG-Anträgen im Bundesministerium für Wirtschaft und Klimaschutz (BMWK) erfolgt auf einem hohen Niveau.

Im November 2023 führte ich einen Beratungs- und Kontrollbesuch beim BMWK durch. Aufgrund der hohen Zahl von IFG-Anträgen an das BMWK im Prüfzeitraum von 2019 bis Juni 2023 erfolgte die Kontrolle anhand einer gleichmäßigen Stichprobe über diesen Zeitraum.

Insgesamt ist im BMWK eine erfreulich offene Haltung zur Informationsfreiheit festzustellen. Es ist deutlich erkennbar, dass ein Verständnis für die Bedeutung der Informationsfreiheit und der Transparenz für die Nachvollziehbarkeit von Verwaltungsentscheidungen vorhanden ist. Diese Grundhaltung spiegelt sich auch in der Zusammenarbeit der Fachreferate mit dem Referat ZR, das die IFG-Bearbeitung koordiniert, wider. Die Prozesse und Arbeitsschritte in der Zusammenarbeit mit den Fachreferaten sind pragmatisch und nachvollziehbar strukturiert. Aufgrund der guten Organisation und der eingespielten Verfahrensabläufe werden auch komplexe Vorgänge strukturiert und sachgerecht bearbeitet.

Die inhaltliche Bearbeitung der IFG-Anträge, bis hin zur Bescheiderstellung, erfolgt in den Fachreferaten. Auch hier konnte ich ein großes Maß an fachlicher Kenntnis und Engagement hinsichtlich der Anwendung des IFG und des UIG feststellen.

Aufgrund besonderer Umstände und der fachlichen Zuständigkeit einzelner Referate im BMWK wurde ein zeitweise besonders hohes Antragsaufkommen festgestellt. Der Informationszugang wird größtenteils innerhalb der Monatsfrist gewährt. Soweit der Gewährung des Informationszugangs Ausschlussgründe entgegenstehen, erfolgt regelmäßig eine nachvollziehbare und zutreffende Begründung der Ablehnung.

7 Sicherheitsbereich

7.1 Bundesverfassungsgericht entscheidet zu polizeilicher Datenanalyse

Mit seinem Urteil vom 16. Februar 2023 hat das Bundesverfassungsgericht grundlegende Weichen für polizeiliche automatisierte Datenanalysen gestellt. Dabei geht es auch um den Einsatz Künstlicher Intelligenz (KI). Die Gesetzgeber im Bund und den Ländern sollten die Ausführungen des Gerichts als „Werkzeugkasten" nutzen und den Einsatz komplexer Analysesysteme auf ein solides gesetzliches Fundament stellen.

Am 16. Februar 2023 verkündete das Bundesverfassungsgericht ein Grundsatzurteil zur automatisierten Datenanalyse.[93] Gegenstand der Entscheidung waren Vorschriften in Landesgesetzen, die die Polizei in Hamburg und Hessen in die Lage versetzen sollten, umfassende Datenanalysen durchzuführen. Die hessische Vorschrift in § 25a Abs. 1 Alt. 1 HSOG ist nach der Entscheidung des Bundesverfassungsgerichts nicht mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar. Die noch nicht in der Praxis umgesetzte Hamburgische Vorschrift in § 49 Abs. 1 Alt. 1 PolDVG erklärte das Gericht für nichtig. Die sich hieraus ergebende Pflicht zur Neuregelung der Norm ist bereits in der vom Gericht gewährten Übergangsfrist erfolgt.

Der Urteilsverkündung war am 20. Dezember 2022 eine mündliche Verhandlung vorausgegangen, bei der ich neben den beiden direkt betroffenen Landesbeauftragten für Datenschutz als sachverständiger Dritter angehört wurde. Dabei habe ich unter anderem die Auffassung vertreten, dass Datenabgleiche über umfassende sensible Datenbestände – wie im Fall von Funkzellendateien – nicht auf Generalklauseln gestützt werden können. Dies wurde letztlich auch von der Entscheidung des Gerichts gestützt.

Das Urteil ist aus datenschutzrechtlicher Sicht sehr zu begrüßen. Das Bundesverfassungsgericht hat klargestellt, dass automatisierte Datenanalysen als Grundrechtseingriff ein eigenständiges Eingriffsgewicht haben. Wie schwer der Eingriff im Einzelfall wiegt, hängt besonders davon ab, welcher Art das neue Wissen sein kann, das durch die automatisierte Datenanalyse erzeugt wird. Je nach der eingesetzten Analysemethode können durch verknüpfende Auswertung vorhandener Daten neue persönlichkeitsrelevante Informationen gewonnen werden, die den Behörden ansonsten so nicht zugänglich wären. Unter Umständen kann sich eine automatisierte Datenanalyse sogar einem „Profiling" annähern. Auch deshalb sind automatisierte Datenanalysen an spezifisch geregelte gesetzliche Voraussetzungen zu binden.

Besonders erfreulich ist, dass das Gericht auch die Daten aus Vorgangsbearbeitungssystemen thematisiert hat. Denn Personen, deren Daten dort gespeichert sind, sind nicht zwingend selbst „in ein kriminelles Geschehen verfangen". Das können z. B. Zeugen, Opfer, Unfallbeteiligte sein oder aber Menschen, gegen die sich ein einmal bestehender Verdacht nicht bestätigt hat oder bei denen anzunehmen ist, dass sie in Zukunft keine Straftaten begehen werden. Deshalb ist der Abgleich mit diesen Daten eingriffsintensiv.

Ebenfalls erfreulich ist, dass das Gericht auch potentielle neue Analysemethoden wie KI und mögliche Diskriminierungspotentiale in den Blick genommen hat. Das war für mich in dem Verfahren ebenfalls ein sehr wichtiger Punkt. Diskriminierungen bei algorithmenbasierten Datenverarbeitungen zu verhindern, ist eine der zentralen Herausforderungen der Zukunft. Die Entscheidung zeigt, dass es aus verfassungsrechtlicher Perspektive nicht maßgeblich darauf ankommt, ob eine Anwendung einer bestimmten Technologie – wie z. B. einem bestimmten Begriff von KI – zuzuordnen ist, sondern darauf, welche

93 Urteile des Bundesverfassungsgerichts: 1 BvR 1547/19 und 1 BvR 2634/20

Auswirkungen die jeweilige Analysemethode auf das Gewicht des Grundrechtseingriffs hat oder haben kann.

Bei neuen gesetzlichen Vorschriften ist nunmehr schrittweise zu prüfen, ob automatisierte Datenabgleiche zu rechtfertigen sind. Dabei hat das Gericht in seinem Urteil dem Gesetzgeber einerseits Spielraum gegeben, andererseits aber viele konkrete Vorgaben gemacht. Der Gesetzgeber kann beispielsweise das Eingriffsgewicht mindern, indem er die Analysemöglichkeiten, insbesondere im Hinblick auf Art und Umfang der verwendeten Daten sowie die Analysemethode, eng begrenzt. Nicht nur die Gesetzgeber in Hamburg und Hessen sind nunmehr gehalten, die Rechtslage an die verfassungsrechtlichen Vorgaben anzupassen. Vielmehr hat das Bundesverfassungsgericht allgemeingültige klare Maßstäbe für automatisierte Datenanalysen aufgestellt, an denen sich sämtliche Gesetzgebung und Rechtsprechung messen lassen müssen.

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.

7.2 Polizei 20/20

Die Planungen des gemeinsamen Datenhauses der Polizeibehörden des Bundes und der Länder schreiten fort. Von rund 40 Teilprojekten haben im Berichtszeitraum unter anderem der Proof of Concept Datenkonsolidierung (PoC), die „Hypothetische Datenneuerhebung", der Polizeiliche Informations- und Analyseverbund (PIAV), das European Police Record Index System (EPRIS) und das einheitliche Fallbearbeitungssystem (eFBS) eine wichtige Rolle gespielt.

Über das Gesamtprogramm Polizei 20/20 (P 20) als IT-Großprojekt der Polizeibehörden des Bundes und der Länder berichte ich regelmäßig, zuletzt in meinem 31. Tätigkeitsbericht (Nr. 7.2). Insgesamt positiv zu bewerten ist, dass die Projektgruppe P 20 die Datenschutzaufsichtsbehörden in regelmäßigen Treffen über den aktuellen Sachstand informiert. Hinzu kommen Informationen über den Fortgang der in dem Projekt zusammengefassten Einzelprojekte. Hierzu steht die Projektgruppe P 20 regelmäßig im Austausch mit mir und der Arbeitsgemeinschaft Informationssystem der Polizeien (AG INPOL) der Datenschutzbehörden. Die AG INPOL ist eine Arbeitsgruppe des Arbeitskreises Sicherheit der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). Insgesamt hat sich eine sehr konstruktive und angenehme Beteiligungskultur entwickelt.

Entwicklung des Datenhauses

Ein Schwerpunkt des Programms des letzten Jahres lag darin, Fortschritte bei der Entwicklung des gemeinsamen Datenhauses zu erzielen. Die Projektgruppe im Bundesministerium des Innern und für Heimat (BMI) hat mir im dritten Quartal des Berichtsjahres den aktuellen Sachstand mitgeteilt. Das Datenhaus soll künftig aus einer voneinander getrennten Primär- und Sekundärdatenhaltung bestehen. Zwischen beiden Ebenen findet eine Synchronisation statt. In der Primärdatenhaltung ist die Änderung, Löschung und Speicherung von personenbezogenen Daten möglich. Über die Sekundärebene werden Suchen und Recherchen durchgeführt.

Eine Entscheidung über die Softwarelösung wurde Ende des Jahres 2023 getroffen. Ein entsprechendes Konzept lag mir bis zum Redaktionsschluss allerdings noch nicht vor, so dass ich das Datenhaus datenschutzrechtlich noch nicht bewerten konnte. Sobald mir dieses vorliegt, werde ich unter anderem prüfen, ob die Unterteilung in zwei Ebenen zulässig ist und der Frage nachgehen, wie die Synchronisation realisiert wird. Ein Schwerpunkt wird zudem die mandantenfähige Trennung sein, die in der Primärdatenhaltung erfolgen soll. Das BMI hat mir eine Beteiligung zum gemeinsamen Datenhaus zugesagt, sobald neue Erkenntnisse vorliegen.

Proof of Concept Datenkonsolidierung

Auch über dieses Teilprojekt habe ich schon mehrfach berichtet (zuletzt 31. TB Nr. 7.2). Mit dem PoC war beabsichtigt, ein weiteres Verbundsystem außerhalb des polizeilichen Informationsverbundes nach dem Bundeskriminalamtsgesetz (BKAG) zu betreiben. Mit dem PoC sollte ein Datenaustausch unterhalb der im BKAG festgelegten Schwelle der Verbundrelevanz ermöglicht werden.

Anfang des Jahres 2021 hatte ich formell eine Warnung ausgesprochen, dass die damit verbundene Datenverarbeitung rechtswidrig sein könnte. Außerdem hatte ich mich Anfang des Jahres 2022 in einem mit der AG INPOL abgestimmten Schreiben noch einmal gegen den PoC ausgesprochen.

Das Projekt wurde nun bis auf weiteres gestoppt. Damit wurde deutlich, dass die Projektgruppe die geltend gemachten datenschutzrechtlichen Bedenken ernst nimmt. Da das PoC neben datenschutzrechtlichen auch grundsätzliche staatsorganisations- und verfassungsrechtliche Fragen aufwirft, hatte ich Anfang des Jahres

ein Rechtsgutachten in Auftrag gegeben.[94] Die Trageweite der mit dem PoC beabsichtigten Datenverarbeitung wird auch in diesem Gutachten von Herrn Professor Mathias Bäcker noch einmal verdeutlicht. Im Ergebnis dürfen landesrechtliche Ermächtigungen nicht die bundesrechtliche Wertung unterlaufen, dass ein allgemeiner kriminalpolizeilicher Informationsverbund an das Kriterium der Verbundrelevanz geknüpft ist. Verbundrelevant sind Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung.

Hypothetische Datenneuerhebung

Anfang des Berichtsjahres haben mich die Projektverantwortlichen des Teilprojekts „Hypothetische Datenneuerhebung“ zu einem Workshop eingeladen. Hier wurden mir und den Landesdatenschutzaufsichtsbehörden ein Ticket-Label-Verfahren vorgestellt. Mit diesem Verfahren sollen innerhalb von P 20 alle Daten entsprechend der Anforderungen an den Grundsatz der hypothetischen Datenneuerhebung gekennzeichnet werden. Diese Vorgehensweise findet sowohl bei mir als auch bei den Datenschutzaufsichtsbehörden der Länder Zuspruch.

Die in der AG INPOL vertretenen Behörden haben die Gelegenheit genutzt, auf Basis der Erkenntnisse des Workshops eine gemeinsame Stellungnahme gegenüber dem BMI abzugeben. Eine Antwort lag bis zum Redaktionsschluss noch nicht vor. Über den Fortgang werde ich berichten.

Strategische Komponente des Polizeilichen Informations- und Analyseverbundes

Zu der strategischen Komponente des Polizeilichen Informations- und Analyseverbundes (PIAV-S) stehe ich schon seit 2019 mit dem BMI und Bundeskriminalamt (BKA) in einem Austausch (31. TB. Nr. 7.2). Bislang konnte noch nicht abschließend geklärt werden, ob mit PIAV-S personenbezogene Daten in pseudonymisierter Form oder anonymisiert verarbeitet werden. Im Mai 2023 hatte ich gegenüber dem BKA einen Informationsbesuch angekündigt. Leider kann ein Termin erst nach Redaktionsschluss stattfinden.

Hypothetische Datenneuerhebung als Spezialfall der Zweckbindung

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

Zum Aufrufen des Auszugs aus meinem Positionspapier zum Grundsatz der Zweckbindung in polizeilichen Informationssystemen vom 6. April 2021 den QR-Code scannen oder klicken.

Polizeilicher Informations- und Analyseverbund Politisch motivierte Kriminalität:

In meinem Berichtszeitraum ist mir das Projekt Polizeilicher Informations- und Analyseverbund Politisch motivierte Kriminalität (PIAV-S-PMK) bekannt geworden. PIAV-S-PMK ist ein auf derselben Technik wie PIAV-S basierendes, aber anders ausgestaltetes Meldesystem für den Bereich des Staatsschutzes. In einem Informationsbesuch zu PIAV-S-PMK im Sommer dieses Jahres schilderte das BKA, es handele sich um ein Projekt, welches ausschließlich in der Abteilung Staatsschutz in Planung sei und als Teilprojekt von P 20 Anfang 2025 in den Wirkbetrieb gehen solle.

Mit dem System würden die Landespolizeibehörden künftig personenbezogene Daten aus dem Phänomenbereich des Staatsschutzes elektronisch an das BKA liefern. Dies soll den kriminalpolizeilichen Meldedienst ersetzen. Die Daten würde das BKA zum einen als Zentralstelle personenbezogen speichern. Zum anderen würde es die Daten in pseudonymisierter Form für Lagebilder, Analysen und Statistiken verwenden.

94 Gutachten „Polizeirechtlicher und verfassungsrechtlicher Rahmen eines polizeilichen Informationsverbunds der Länder“ vom 27. März 2023, abrufbar unter: www.bfdi.bund.de/dokumente

Für die Weiterverarbeitung der Daten stützt sich das BKA auf die Generalklausel des § 16 Abs. 1 BKAG. Das bewerte ich nach meinem derzeitigen Sachstand kritisch. Hier stellt sich die Frage, ob die Generalklausel des § 16 Abs. 1 BKAG Grundlage für eine Analyse und das Erstellen von Lagebildern sein kann. Das BKA hat mir eine weitere Beteiligung zugesagt.

Einheitliche Fallbearbeitungssystem

Beim einheitlichen Fallbearbeitungssystem (eFBS) des BKA handelt es sich um eine Datei, in der personenbezogene Daten im Hinblick auf Tat- und Täterzusammenhänge hin verarbeitet werden. Dabei können die personenbezogenen Daten in Beziehung zueinander gesetzt sowie recherchiert, gefiltert und visualisiert werden. Eine Kontrolle hierzu habe ich begonnen und werde über diese im nächsten Tätigkeitsbericht berichten.

European Police Record Index Sytem:

Anfang des Berichtsjahres hatte ich einen Informationsbesuch zu EPRIS im BKA wahrgenommen. Das BKA hat mir als europaweiter Projektleiter das System vorgestellt und mich sehr kooperativ und konstruktiv unterstützt.

Ziel des Projektes ist es, ein EU-weites Fundstellennachweissystem für polizeiliche Kriminalakten zu schaffen (31. TB Nr. 7.2). In pseudonymisierter Form werden mittels eines HIT/No-Hit-Verfahrens dezentral gespeicherte Daten abgeglichen. Hierzu wird ein engbegrenzter Datenumfang genutzt (Name, Vorname, Geburtsdatum, Geschlecht, Nationalität).

Das BKA begründet die derzeitige Verarbeitung von Test- und Produktivdaten mit Forschungszwecken (§ 21 BKAG). Diese Rechtsauffassung prüfe ich derzeit und befinde mich hierzu mit dem BKA im Austausch.

Verbundrelevanzkriterien

Mit dem BMI befinde ich mich außerdem aktuell in einem Austausch über die Bestimmung der Verbundrelevanzkriterien nach § 30 Abs. 1 Nr. 1 BKAG. Die am polizeilichen Informationsverbund und damit an P 20 teilnehmenden Stellen verarbeiten im polizeilichen Informationsverbund ausschließlich personenbezogene Daten, deren Verarbeitung für die Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung erforderlich ist. Um die Verbundrelevanz zu bestimmen, legen die teilnehmenden Stellen Kriterien fest. Die Festlegung erfolgt im Benehmen mit mir (§ 30 Abs. 2 BKAG). Das BMI hat mir hierzu einen Dokumentenentwurf übersandt. Auf dieser Grundlage hat bereits ein Auftaktgespräch stattgefunden.

7.3 Internetrecherchen für die nationale Sicherheit – Auch hier gibt es Grenzen!

Nachrichtendienste sehen in der Internetrecherche zunehmend eine Art Allheilmittel, um sich einen umfassenden Überblick über Personen oder bestimmte Sachverhalte zu verschaffen. Deshalb mehren sich die Anwendungsfelder und Anzahl der Betroffenen. Eine Herausforderung für den Schutz des Grundrechts auf informationelle Selbstbestimmung.

Das Internet und soziale Netzwerke sind kein rechtsfreier Raum. Das gilt sowohl für die diese Medien Nutzenden als auch für Sicherheitsbehörden und Nachrichtendienste, die aus diesen Informationen für ihre Arbeit gewinnen wollen.

Zwar wird oftmals entgegnet, das Internet sei eine öffentlich zugängliche Quelle. Auf welche Bereiche dies zutrifft, wird jedoch sehr unterschiedlich bewertet, insbesondere im Hinblick auf Privatsphäre-Einstellungen von Accounts oder möglicherweise durch Allgemeine Geschäftsbedingungen „erlaubte“ Weiternutzungen. Mangels einheitlicher Definition können Internetnutzerinnen oder Internetnutzer nicht darauf vertrauen, dass ihre Daten „privat“ sind.

Zudem ist fraglich, ob der Schutz der Person allgemein nur deshalb entfällt, weil die Information öffentlich zugänglich ist. Wenn zum Beispiel – richtige oder falsche – Daten zu einer Person gegen ihren Willen veröffentlicht wurden, macht das diese Daten bzw. die Person nicht weniger schützenswert. Das Gegenteil ist oft der Fall. Daten stehen sicher nicht deshalb zur freien Verfügung, weil die betroffene Person Opfer von Cybermobbing oder Stalking geworden ist. Oft lässt sich im Internet nicht verifizieren, ob die Einwilligung der betroffenen Person vorliegt.

Insgesamt bedarf es für eine gezielte Internetrecherche verhältnismäßiger, ausreichend bestimmter und normenklarer Rechtsgrundlagen. Hier sollte der Gesetzgeber bei allem Verständnis für technikoffene Formulierungen Farbe bekennen und klare Regelungen treffen. Doch bislang gibt es nur Stückwerk.

So hat der Gesetzgeber in der jüngsten Novelle des Bundesnachrichtendienstgesetzes in § 10a Abs. 2 sowie in § 25d Bundesverfassungsschutzgesetz erhöhte Übermittlungsschwellen für systematisch erhobene oder zusammengeführte allgemein zugängliche personenbezogene Daten geschaffen.

Hierdurch gibt er zwar zu erkennen, dass er sich des schwerwiegenden Eingriffsgewichts systematisch erhobener oder zusammengeführter Daten aus allgemein zugänglichen Quellen bewusst ist. Insbesondere wegen des Gebotes der Normenklarheit und Normenbestimmtheit wäre es aus meiner Sicht allerdings erforderlich gewesen, dass der Gesetzgeber neben der Regelung der Übermittlungsschwellen auch eine Rechtsgrundlage für die vorgelagerte Verarbeitung systematisch erhobener oder zusammengeführter personenbezogener Daten aus allgemein zugänglichen Quellen schafft – und zwar für alle Nachrichtendienste. Hierzu hätte sich eine spezielle Ermächtigungsgrundlage zur Erhebung derartiger Daten mit begleitenden Regelungen unter anderem zu Speicherdauer, Umfang und Art der Zusammenführung oder dem Schutz sensibler Daten unbeteiligter Dritter angeboten. Leider hat mein entsprechender Vorschlag bislang kein Gehör gefunden.

Ohne eine solche gesetzliche Anpassung steht nach der aktuellen Gesetzeslage für derartige Datenverarbeitungen nur der Rückgriff auf die Generalklausel zur Verfügung, welche die Datenverarbeitung unspezifisch zur Erfüllung der Aufgaben des Bundesnachrichtendienstes erlaubt. Diese Generalklausel wird dem mit einer systematischen Erhebung oder Zusammenführung von personenbezogenen Daten aus allgemein zugänglichen Quellen verbundenen Eingriffsgewicht nicht gerecht.

Eine weitere Lücke weisen die Gesetze auf beim Einsatz sogenannter „Virtueller Agenten“, die unter falscher Identität einen Account bei einem sozialen Netzwerk oder Messangerdienst betreiben, um Informationen zu sammeln. Keiner der Nachrichtendienste des Bundes hat hierzu eine explizite Rechtsgrundlage. Das BVerfSchG verweist insoweit aktuell zur Regelung der Befugnisse noch auf eingestufte untergesetzliche Dienstvorschriften. Der jeweilige Eingriff in das Grundrecht auf informationelle Selbstbestimmung kann jedoch schwerwiegende Ausmaße annehmen, insbesondere auch durch die Verknüpfung mit bereits bei den Diensten vorhandenen Daten. Solche intensiven Grundrechtseingriffe durch die Dienste bedürfen einer expliziten Regelung auf gesetzlicher Basis, wie unlängst durch das Bundesverfassungsgericht in mehreren Urteilen festgestellt.

Im für das Jahr 2024 geplanten zweiten Teil der Reform des Nachrichtendienstrechts müssen daher für die Datenerhebung aus dem Internet und deren Weiterverarbeitung durch die Dienste genaue Vorgaben im Gesetz geschaffen werden.

Hierbei ist u. a. zu regeln, wie mit aus dem Internet erhobenen Daten umzugehen ist. So sollte beachtet werden, wer Autor der aus dem Internet gewonnenen Information ist – die betroffene Person selbst oder jemand Drittes. Ebenso zu berücksichtigen ist, zu welchem Anlass und in welchem Kontext die relevante Information veröffentlicht wurde. Weiter maßgeblich ist der Ort der Verarbeitung, ob die betroffene Person Schutzmaßnahmen ergriffen hat und ob besondere Kategorien personenbezogener Daten betroffen sind. Der Empfängerkreis und die hinter der Verbreitung der Information stehende Kommunikationsbeziehung ist ebenfalls im angemessen Umfang zu beachten.

Vor allem sind Anlass, Umfang, Zweck und Speicherdauer eindeutig zu regeln und die Tatbestandsvoraussetzungen der Rechtsgrundlage eindeutig zu definieren, um Rechtsklarheit für betroffene Personen und verantwortliche Stellen zu schaffen.

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.

Querverweise:

3.3.5 SÜG-Evaluierung – Verpasste Chancen, 9.1.7 Kontrollen beim Bundesamt für den Verfassungsschutz

7.4 Bundestagspolizei agiert weiterhin ohne konkrete Rechtsgrundlage

Die Polizei des deutschen Bundestages (BT-Polizei) agiert bisher ohne spezialgesetzliche Rechtsgrundlage. Das wird sich hoffentlich bald ändern.

Die BT-Polizei nimmt mit ca. 400 Mitarbeitenden die polizeilichen Aufgaben im Bundestag wahr. Zu ihren Aufgaben gehören die Abwehr von Gefahren in den Liegenschaften und Räumlichkeiten, die Einlasskontrolle, Ausweisangelegenheiten und polizeiliche Ermittlungen in Strafsachen. Bei der Wahrnehmung dieser Aufgaben muss sie regelmäßig in das Recht auf informationelle Selbstbestimmung der überprüften Personen eingreifen. Dies bedarf einer konkreten verfassungskonformen gesetzlichen Ermächtigungsgrundlage, die noch immer nicht vorhanden ist. Aktuell stützt die BT-Polizei ihre Befugnisse neben Art. 40 Abs. 2 GG insbesondere auf die Hausordnung des Deutschen Bundestages und eine interne Dienstanweisung („Dienstanweisung für den polizeilichen Vollzugsdienst“).

Das Fehlen einer Rechtsgrundlage habe ich schon anlässlich meiner Kontrolle vom Januar 2019 beanstandet (28. TB Nr. 7.2). Auch in den Jahren davor wurde mehrfach auf diesen Missstand aufmerksam gemacht (u. a. 25. TB Nr. 21.1).

Obwohl bereits im Juli 2018 vom damaligen Bundestagspräsidenten schriftlich versichert wurde, dass die Erstellung eines Gesetzentwurfes beauftragt worden sei, liegt mir bis zum Redaktionsschluss dieses Tätigkeitsberichts leider noch immer kein entsprechender Entwurf vor.

Immerhin erhielt ich im Rahmen meiner regelmäßigen Sachstandsanfrage im Sommer dieses Jahres die Mitteilung über die aktuelle Befassung der Bundestagsverwaltung mit dem Entwurf des Gesetzes.

7.5 Zuverlässigkeitsüberprüfungen bei der Fußball-Europameisterschaft der Männer 2024 in Deutschland

Polizeiliche Zuverlässigkeitsüberprüfungen bei Großveranstaltungen sind inzwischen zum Standardinstrument geworden, um die Sicherheit dieser Veranstaltungen zu gewährleisten. Die Forderung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) nach einer bereichsspezifischen Rechtsgrundlage wurde mittlerweile überwiegend umgesetzt.

Im Sommer 2024 ist Deutschland Austragungsort der 17. Fußball-Europameisterschaft der Männer. Personen, die im Zusammenhang mit der Großveranstaltung eine Akkreditierung beantragt haben, müssen grundsätzlich eine Zuverlässigkeitsüberprüfung durchlaufen. Hierzu übermittelt der Veranstalter deren personenbezogenen Daten an die Sicherheitsbehörden des Bundes und der Länder, um festzustellen, ob sicherheitsrelevante Erkenntnisse vorliegen. Solche Verfahren greifen tief in das Grundrecht auf informationelle Selbstbestimmung ein.

Ich begrüße es daher, dass mich das Bundesministerium des Innern und für Heimat (BMI) frühzeitig an dem Planungsprozess zur UEFA EURO 2024™ beteiligt hat. Zudem hatte ich Gelegenheit an einem Workshop zu der Thematik der Zuverlässigkeitsüberprüfungen mit Vertreterinnen und Vertretern der Sicherheitsbehörden des Bundes und der Länder teilzunehmen. Dies bot mir die Möglichkeit, die Teilnehmenden über die Notwendigkeit bereichsspezifischer Rechtsgrundlagen zu sensibilisieren.

In den meisten Bundesländern wurden zwischenzeitlich entsprechende Rechtsgrundlagen geschaffen. Dort, wo noch keine Rechtsgrundlage für das jeweilige Akkreditierungsverfahren existiert, sehe ich Datenübermittlungen durch Bundesbehörden als gefährdet an, insbesondere dann, wenn eine Datenübermittlung lediglich auf einer Einwilligungserklärung beruht. Ich werde die Planungen auf Bundesebene weiterhin datenschutzrechtlich begleiten und stehe hierzu in einem Austausch mit dem BMI.

7.6 Passenger Name Records – Grundsatzurteil des EuGH zeigt erste Wirkung

Aufgrund der Entscheidung des Europäischen Gerichtshofs (EuGH) wird endlich die Verarbeitung von Fluggastdaten in Deutschland angepasst. Die Änderung des Fluggastdatengesetzes (FlugDaG) steht hingegen noch aus.

In den Mitgliedstaaten der EU sind Luftfahrtunternehmen verpflichtet, Informationen über Fluggäste, sogenannte Passenger Name Records (PNR), an die sogenannten Fluggastdatenzentralstellen zu übermitteln. In Deutschland ist diese Stelle beim Bundeskriminalamt eingerichtet. Die Informationen werden dann mit polizeilichen Datenbanken und vorher erstellten Mustern abgeglichen (z. B. Art der Buchung, gewählte Flugroute etc.).

Nationale Rechtsgrundlage für diese Verarbeitungen ist das FlugDaG. Es setzt die Richtlinie (EU) 2016/681 vom 27. April 2016 über die Verwendung von Fluggastdatensätzen zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (PNR-RL) um. Mit dem FlugDaG wurde auch die Pflicht geschaffen, PNR-Daten zu allen innereuropäischen Flügen an die Fluggastdatenzentralstelle zu übermitteln.

Schon bei Beginn der Umsetzung der PNR-RL in deutsches Recht durch das FlugDaG – und seitdem fortwährend – hatten meine Vorgängerin und ich verschiedene Bedenken zum Ausdruck gebracht (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. und zuletzt 31. TB Nr. 7.1). Das Grundsatzurteil des EuGH (C-817/19, vgl. 31. TB Nr. 7.1) hat viele dieser Kritikpunkte bestätigt, wenngleich die Verarbeitung von PNR-Daten in großem Umfang grundsätzlich weiterhin zulässig ist. Die PNR-RL enthält nach der Auslegung des EuGH jedoch zahlreiche Vorgaben, die bisher so nicht umgesetzt wurden.

Das Urteil führt nun dazu, dass die hiesige Praxis geändert wird und personenbezogene Daten in geringerem Umfang erfasst bzw. gespeichert werden dürfen. Das

betrifft z. B. die Speicherfristen, die Einbeziehung innereuropäischer Flüge und Genehmigungsprozesse, aber auch weitere Aspekte.

Wie mir das Bundesministerium des Innern und für Heimat (BMI) sowie das Bundesverwaltungsamt erläutert haben, sind Umsetzungsmaßnahmen in die Wege geleitet worden. So wurden insbesondere solche Datensätze gelöscht, die länger als sechs Monate gespeichert waren. Neue Datensätze werden mit einem Zeitmarker automatisch zur Löschung vorgesehen. Nur Informationen von ausgewählten Intra-EU-Flügen werden von der Fluggastdatenzentralstelle verarbeitet. Retrograde Recherchen werden grundsätzlich erst nach gerichtlicher Genehmigung durchgeführt. Ich begrüße ausdrücklich, dass mittlerweile solche konkreten Umsetzungsmaßnahmen getroffen wurden.

Zuvor hatte ich mehrfach auf Anpassungen der Verwaltungspraxis und des FlugDaG hingewirkt, sowohl gegenüber dem BMI als auch im Europäischen Datenschutzausschuss. Dieser hatte nach dem Urteil des EuGH unter meiner Federführung eine an die Mitgliedstaaten gerichtete Stellungnahme veröffentlicht, die die EU-weite Relevanz des Urteils hervorhebt und unverzügliche Anpassungsmaßnahmen anmahnt. Die laufende Umsetzung der europarechtlichen Vorgaben in der Verwaltungspraxis werde ich weiterhin kritisch begleiten.

Neben Änderungen der Verwaltungspraxis steht aber auch die Anpassung des FlugDaG noch aus. Die Möglichkeit der richtlinienkonformen Auslegung einiger Vorgaben des aktuellen FlugDaG entbindet nicht von den Grundsätzen der Bestimmtheit und Normenklarheit. Verwaltung und Gerichte, aber auch Bürgerinnen und Bürger, sollten durch eine Änderung des FlugDaG wieder klar erkennen können, welche verantwortlichen Stellen unter welchen Voraussetzungen welche Verarbeitungen von personenbezogenen Daten vornehmen dürfen.

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.

7.7 Inbetriebnahme des erweiterten Schengener Informationssystems

Das Schengener Informationssystem der dritten Generation (SIS III) wurde am 7. März 2023 in Betrieb genommen. Diese Erweiterung war vorab mehrfach verschoben worden. Mit Einführung des SIS III wurde eine Vielzahl weiterer Behörden an das System angebunden.

Über die anstehende Erweiterung des Schengener Informationssystems (SIS) habe ich bereits in meinem 31. TB (Nr. 3.5.4) informiert. Grundlage für das modernisierte SIS sind die drei SIS-Verordnungen (EU) 2018/1860, 2018/1861 und 2018/1862. Nachdem diese am 27. Dezember 2018 in Kraft getreten waren, mussten die einzelnen Mitgliedstaaten insbesondere die technischen Voraussetzungen für die Umsetzung der neuen Anforderungen an das System schaffen. Bis die dazu erforderlichen technischen Maßnahmen in allen Mitgliedstaaten vollständig abgeschlossen werden konnten, wurde die Inbetriebnahme des SIS III bis zum 7. März 2023 mehrfach verschoben.

Um die Vorgaben der SIS-Verordnungen für die Inbetriebnahme des SIS III auch rechtlich abzubilden, wurde in Deutschland Ende 2022 das SIS-III-Gesetz verabschiedet, das Rechtsänderungen in verschiedenen Fachgesetzen, z. B. im Bundeskriminalamtgesetz, vorsieht. Diese betreffen vor allem die Regelungen der Zugriffsbefugnisse der verschiedenen zusätzlichen berechtigten Stellen, die entsprechend den SIS-Verordnungen auf nationaler Ebene umzusetzen waren. Auch zu diesem Gesetzgebungsverfahren habe ich in der Vergangenheit berichtet (31. TB Nr. 3.5.4).

Die SIS-Verordnungen erweitern den Anwendungsbereich und die Funktionen des SIS. Das SIS wird etwa um neue Ausschreibungskategorien ergänzt. Insbesondere kann nun anhand von Fingerabdrücken, die an Tatorten schwerer Verbrechen gesichert wurden und mit sehr hoher Wahrscheinlichkeit einem Täter zuzuordnen sind, nach unbekannten Personen gefahndet werden. Zudem können Personenfahndungen unter bestimmten Voraussetzungen zusätzliche biometrische Daten, z. B. Handflächenabdrücke, beigefügt werden. Eine der wesentlichen Neuerungen ist außerdem, dass auch Nichtpolizeibehörden direkt an das SIS angeschlossen werden. In Deutschland sind dies ca. 2.000 zusätzliche Behörden. Dazu gehören u. a. die Ausländerbehörden, das Auswärtige Amt, das Bundesamt für Auswärtige Angelegenheiten, die Auslandsvertretungen und das Bundesamt für Migration und Flüchtlinge sowie die für die Zulassung von Kraftfahrzeugen zuständigen Behörden.

Über die Inbetriebnahme des SIS III und damit einhergehenden Systemänderungen haben sich meine Mitarbeiterinnen und Mitarbeiter beim Bundeskriminalamt in seiner Funktion als zentrale nationale Stelle für den Betrieb des SIS eingehend informiert. Die Nutzung des SIS stellt auch künftig einen wichtigen Teil meiner

Kontrolltätigkeiten dar. Ein besonderes Augenmerk wird dabei auf den mit dem SIS III eingeführten Neuerungen liegen.

7.8 Fehleranfälliger Prozess in der statistischen Erhebung des ZKA führt zu verzögerten Pflichtkontrollen

Zur Vorbereitung meiner Pflichtkontrollen forderte ich in den letzten Jahren das Zollkriminalamt (ZKA) regelmäßig auf, eine Übersicht aller durchgeführten eingriffsintensiven Maßnahmen zu übersenden. Leider stellten sich die übermittelten Zahlen wiederholt als falsch heraus, was zu einer erheblichen Verzögerung bei der Durchführung der Pflichtkontrollen geführt hat.

Nach dem Zollfahndungsdienstgesetz bin ich verpflichtet, Maßnahmen des Zollfahndungsdienstes, die auf Grundlage des polizeilichen Gefahrenabwehrrechts in diesem Gesetz durchgeführt werden, regelmäßig zu kontrollieren. Hierfür fordere ich, aufgeteilt nach der durchführenden Stelle, regelmäßig eine Auflistung der präventiven Maßnahmen an. Diese umfassen beispielsweise längerfristige Observationen, den Einsatz von Vertrauenspersonen oder auch das Aufzeichnen des nichtöffentlich gesprochenen Wortes.

Als ich im September 2022 dem Zollfahndungsamt Frankfurt am Main eine Kontrolle zu verschiedenen in der Statistik gemeldeten Maßnahmen angekündigt habe, erhielt ich die Antwort, dass keine dieser Maßnahmen durchgeführt wurde.

Daher forderte ich beim ZKA eine neue korrigierte Statistik der eingriffsintensiven Maßnahmen für die Jahre 2019 bis 2022 an. Darauf basierend sollte eine Querschnittskontrolle aller Zollfahndungsämter zum Thema „Herstellung von Lichtbildern/Bildaufzeichnungen außerhalb von Wohnungen“ durchgeführt werden. Auch hier ergab eine Rückmeldung der einzelnen Stellen, dass die mir vorgelegte Statistik nicht stimmte.

In einem anschließend von mir durchgeführten Informationsbesuch im ZKA zur Aufklärung der Ursachen für die mehrfach abweichende Statistik, äußerte das ZKA Bedauern über die entstandenen Friktionen im Rahmen der Bereitstellung der Statistik und erläuterte, dass es bei der Erhebung aufgrund eines technischen Fehlers zu einer Vermischung der präventiven und der repressiven eingriffsintensiven Maßnahmen bei der Datenerfassung gekommen sei. Das ZKA versicherte mir, dass man die technische Statistikanwendung angepasst und Maßnahmen für eine mehrstufige Qualitätssicherung eingeleitet habe. Auch eine Trennung in der statistischen Erfassung von repressiven Maßnahmen nach der Strafprozessordung und präventiven Maßnahmen nach dem Zollfahndungsdienstgesetz wurde zugesagt.

Nach dem Informationsbesuch übersandte mir das ZKA eine neue statistische Erhebung. Zur Planung einer erneuten Querschnittskontrolle schrieb ich nochmals die Zollfahndungsämter mit Ankündigung des Kontrollgegenstandes sowie den von mir erwarteten durchgeführten Maßnahmen an. Leider zeigte sich, dass die vorläufige erste Qualitätssicherung im ZKA noch nicht den gewünschten Erfolg erzielt hatte und die übermittelten Zahlen nach wie vor nicht den vor Ort durchgeführten Maßnahmen entsprachen.

Das ZKA reagierte umgehend und räumte ein, dass man die technische Anwendung zur statistischen Erhebung angepasst und korrigiert habe. Allerdings erfolgte lediglich eine Korrektur des Jahres 2021/2022. Dies nahm das ZKA zum Anlass, neben der technischen Anwendung, einen Prozess unter Beteiligung des fachlichen Datenschutzes im ZKA zu etablieren, unter dem die Zollfahndungsämter zukünftig Zahlen aufgrund meiner Anfragen zu melden haben.

Für mich als kontrollierende Stelle führten die mehrfach abweichenden Zahlen dazu, eigene Untersuchungen aufzunehmen, um valide Maßnahmenzahlen zu generieren, beispielsweise durch die Auswertung von Informationen spezieller Stellen der Zollfahndung die Mittel für Maßnahmen zur Verfügung stellen (Koordinierungsstellen).

Ungeachtet der Fehleranfälligkeit der statistischen Erhebung im ZKA, konnte ich erfreut feststellen, dass präventive eingriffsintensive Maßnahmen weitaus weniger häufig Anwendung fanden, als ich eingangs vermutet hatte.

7.9 Vertrauen ist gut, selbst prüfen ist besser

Unrichtige oder fehlerhafte Informationen bei Nachrichtendiensten können nicht nur erhebliche Auswirkungen für die Analyse der Sicherheitslage auslösen mit der Folge, dass mögliche Bedrohungen über- oder unterschätzt werden. Fehlinformationen können auch ernsthafte Folgen für Bürgerinnen und Bürger haben, indem sie aufgrund falscher Erkenntnislage zur Zielperson des Nachrichtendienstes und Gegenstand nachrichtendienstlicher Maßnahmen werden.

Das Bundesamt für Verfassungsschutz (BfV) verfügt zur eigenen Aufgabenwahrnehmung über umfangreiche gesetzliche Befugnisse, personenbezogene Daten von Bürgerinnen und Bürger zu erheben, zu speichern

und auszuwerten. Neben der Möglichkeit, allgemein öffentlich zugängliche Daten zu durchsuchen (z. B. Zeitungsartikel oder öffentliche Meinungsbekundungen in sozialen Netzwerken), darf es bei entsprechenden Anhaltspunkten auch bei Banken sowie Kreditinstituten, Luftfahrtunternehmen oder Telekommunikationsanbietern Auskünfte einholen.

Das BfV ist zugleich befugt, die gesammelten Informationen nach Maßgabe der gesetzlichen Übermittlungsvorschriften mit zahlreichen inländischen Behörden (z. B. Landesämtern für Verfassungsschutz, Bundesnachrichtendienst, Polizeibehörden, Bundesamt für Migration und Flüchtlinge, Staatsanwaltschaften, Finanz- und Steuerbehörden, Bundeskriminalamt, Bundesamt für den Militärische Abschirmdienst) zur Bekämpfung von Gefahren für die innere Sicherheit der Bundesrepublik Deutschland zu teilen. Sofern erforderlich, kann das BfV personenbezogene Daten auch an ausländische Nachrichtendienste übermitteln.

Der häufigste Fall dürfte jedoch die Mitwirkung des Verfassungsschutzverbundes auf nationaler Ebene bei Regelabfragen im Zusammenhang mit Zuverlässigkeitsüberprüfungen, wie z. B. für Gewerbeerlaubnisse oder zu bestimmten sensiblen Arbeitsbereichen, wie im Bereich der Atomsicherheit oder der Flugsicherheit, darstellen.

Angesichts der zahlreichen Möglichkeiten, personenbezogene Daten mit anderen Behörden zu teilen, können Datenübermittlungen von unrichtigen bzw. unwahren Tatsachen aufgrund von möglichen Fehlinformationen oder nicht hinreichend verifizierten Annahmen oder aber Auswertungsfehlern mit erheblichen Beeinträchtigungen für die betroffene Person verbunden sein. Gerade die Schnittstelle bei den Zuverlässigkeitsprüfungen macht deutlich, dass eine Speicherung in Dateien oder Akten des Verfassungsschutzes kein Umstand ist, der die betroffene Person nur geringfügig beeinträchtigt. Zwar werden viele Speicherungen ausschließlich in der Sphäre des Verfassungsschutzverbundes bleiben. Sobald aber ein Sicherheitsrisiko durch die Person bspw. durch Zugang zu sensiblen Informationen möglich ist, muss dieser Zugang zu Recht von einer Prüfung abhängig gemacht werden, und der Verfassungsschutz ist zur Mitwirkung verpflichtet.

Wenn Personen allerdings aufgrund von falschen Informationen ins Visier geraten, können sie zu Unrecht kriminalisiert oder überwacht werden. Auch Auswirkungen für die Berufswahl und die Berufsausübung sogar mit der Folge einer Existenzgefährdung sind möglich. Welche weiteren Nachteile bis hin zu Bedrohungen für die jeweilige Person entstehen können, wenn falsche Informationen an ausländische Nachrichtendienste oder Strafverfolgungsbehörden gelangen, sind nicht absehbar.

Um solche Auswirkungen zu vermeiden, hat das BfV die Aufgabe sicherzustellen, die Qualität und Genauigkeit der vorliegenden Informationen sorgfältig zu überprüfen. Daher müssen die von anderen Behörden übermittelten Erkenntnisse stets einer eigenen kritischen Richtigkeitsprüfung unterzogen werden, bevor weitere schwerwiegende Maßnahmen eingeleitet oder Informationen übermittelt werden, insbesondere ins Ausland.

Schon die Gründe für eine (Erst-)Speicherung, erst recht aber die Rechtmäßigkeit von Datenübermittlungen, prüfe ich daher sehr genau und beanstande gegebenenfalls eine Speicherung und/oder Datenübermittlung. Allerdings fehlen mir wirksame Abhilfebefugnisse, beispielsweise kann ich eine Löschung solcher Daten nicht anordnen. Um die Auswirkungen von unrechtmäßigen Datenverarbeitungen zu verringern, dringe ich auch weiterhin darauf, meine Behörde mit entsprechenden Abhilfebefugnissen auszustatten. Nur dies entspricht im Ergebnis einer wirkungsvollen Kompensationsfunktion.

Ich empfehle dem Gesetzgeber, Abhilfebefugnisse auch im Bereich der Nachrichtendienste einzuführen.

7.10 Eine gesetzliche Regelung des Militärischen Nachrichtenwesens ist erforderlich

Ich habe förmlich beanstandet, dass das Militärische Nachrichtenwesen ohne rechtliche Grundlage Daten erhebt und verarbeitet. Die Tätigkeiten des Militärischen Nachrichtenwesen sind mit zum Teil schwerwiegenden Grundrechtseingriffen verbunden, die einer einfachgesetzlichen Rechtsgrundlage bedürfen. Das Bundesministerium der Verteidigung lehnt dies ab.

Beim Militärischen Nachrichtenwesen handelt es sich um die Teile der Bundeswehr, die – ähnlich einem Nachrichtendienst – für die weltweite Gewinnung von Informationen zuständig sind. Aufgabe und Ziel dieser Nachrichtengewinnung und Aufklärung ist die Deckung des militärischen Informationsbedarfs für die politischen und militärischen Bedarfsträger. Die Soldatinnen und Soldaten des Militärischen Nachrichtenwesens bedienen sich des Werkzeugkastens eines klassischen Nachrichtendienstes. Hierzu zählen menschliche Quellen (Human Intelligence), öffentlich zugängliche Quellen

wie Nachrichten, soziale Netzwerke und Foren (Open Source Intelligence), die Abbildende Aufklärung (Imagery Intelligence), die raumbezogene Aufklärung (Geospatial Intelligence) und die Fernmelde- und Elektronische Aufklärung (Signals Intelligence).

Meine Mitarbeiterinnen und Mitarbeiter haben im Jahr 2022 die Fernmelde- und Elektronische Aufklärung des Militärischen Nachrichtenwesens kontrolliert. Der Bereich Signals Intelligence (SIGINT) und die hierfür genutzten Systeme waren Hauptgegenstand der Kontrolle in der Heinrich Hertz-Kaserne in Daun/Eifel. Aus Gründen der Geheimhaltung kann ich an dieser Stelle nur allgemeine Ausführungen zur Kontrolle mit der Öffentlichkeit teilen. Die Aufgaben im Bereich der Signalerfassung und -auswertung erfüllt das Militärische Nachrichtenwesen in enger personeller, technischer und informationeller Zusammenarbeit mit dem Bundesnachrichtendienst. Bei der Kontrolle wurden datenschutzrechtliche Verstöße festgestellt.

In vielen Fällen blieb die nachrichtendienstliche Relevanz der gespeicherten Information mangels Dokumentation fraglich. Nur wenn eine nachrichtendienstliche Relevanz vorliegt, ist die Verarbeitung von Informationen und damit auch die Speicherung personenbezogener Daten zulässig. Eine solche Relevanz müsste durch eine entsprechende Dokumentation nachgewiesen sein. Wiedervorlagefristen wurden nicht ausreichend eingepflegt und für die Arbeit der Bundeswehr nicht mehr erforderliche personenbezogene Daten dementsprechend nur selten gelöscht. Die mangelnde Pflege der Datenbestände führte in vielen Fällen zu einer Unrichtigkeit der Daten. Das steht im Gegensatz zum Selbstverständnis des Militärischen Nachrichtenwesens, das dynamisch auf sich ändernde Begleitumstände reagieren möchte. Darüber hinaus wurde dem Schutz von Daten Minderjähriger nicht ausreichend Rechnung getragen.

Während für die drei anderen Nachrichtendienste des Bundes, also das Bundesamt für Verfassungsschutz, das Bundesamt für den Militärischen Abschirmdienst sowie den Bundesnachrichtendienst einfachgesetzliche Rechtsgrundlagen bestehen, ist dies beim Militärischen Nachrichtenwesen nicht der Fall. Gleichwohl verfolgt das Militärische Nachrichtenwesen nachrichtendienstliche Ziele und setzt zu deren Erreichung nachrichtendienstliche Mittel ein, die im Einzelfall sehr intensiv in das Grundrecht auf informationelle Selbstbestimmung eingreifen.

Obwohl die Tätigkeiten des Militärischen Nachrichtenwesens mit zum Teil schwerwiegenden Grundrechtseingriffen verbunden sind, lehnt das Bundesministerium der Verteidigung – trotz meiner wiederholten Forderung – die Schaffung einer einfachgesetzlichen Rechtsgrundlage ab. Begründet wird dies unter anderem mit der Auffassung, dass Art. 87a GG, also die Verpflichtung des Bundes zur Aufstellung von Streitkräften, als Rechtsgrundlage für die Tätigkeiten des Militärischen Nachrichtenwesens als integraler Bestandteil der Bundeswehr ausreichend sei. Auch Art. 24 Abs. 2 GG, der die Möglichkeit der Einordnung des Bundes in ein System gegenseitiger kollektiver Sicherheit eröffnet, sei in Verbindung mit einem Bundestagsmandat für Auslandseinsätze als Rechtsgrundlage heranzuziehen. Schließlich könne das Militärische Nachrichtenwesen auch auf das Völkerrecht gestützt werden.

Keine der vom Bundesministerium der Verteidigung herangezogenen Regelungen entspricht indes den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts. Dieses hat zuletzt in seinem Urteil zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 19. Mai 2020 entschieden,[95] dass es für derart eingriffsintensive Maßnahmen einer hinreichend bestimmten einfachgesetzlichen Rechtsgrundlage bedarf (29. TB Nr. 6.3). Das Bundesministerium der Verteidigung hält die in dem vorgenannten Urteil aufgestellten Grundsätze für nicht anwendbar.

Dieser Auffassung folge ich ausdrücklich nicht. Ich habe das Fehlen einer Rechtsgrundlage daher beanstandet und fordere weiterhin eine einfachgesetzliche Regelung des Militärischen Nachrichtenwesens.

7.11 Verbesserte Kooperation des BND

Die stärkere Einbindung der Fachbereiche beim Bundesnachrichtendienst (BND) in Informations- und Kontrollbesuche hat sich positiv auf den inhaltlichen Austausch mit dem BND ausgewirkt. Zudem konnte ohne Beschreitung des Klageweges eine Einigung zwischen dem BND und mir zum praxistauglichen Umfang meiner Einsichtsrechte erzielt werden. Die meiner Behörde Kompensationsfunktion hat hierdurch eine Stärkung erfahren.

In der Vergangenheit fand der inhaltliche Austausch in Informations- und Kontrollbesuchen im Wesentlichen über das Datenschutzreferat des BND statt. Durch

95 Urteil des Bundesverfassungsgericht: 1 BvR 2835/17

die stärkere Einbindung der jeweiligen Fachbereiche konnte im Berichtsjahr eine deutliche Verbesserung des inhaltlichen Austausches erzielt werden. Erfreulich und begrüßenswert ist, dass die Fachbereiche des BND durch die direkte Kommunikationsmöglichkeit vermehrt Beratungsanfragen zu konkreten Datenverarbeitungsvorgängen stellen können. Dabei hat sich gezeigt, dass die Fachbereiche auch proaktiv mit Problemstellungen auf mich zugekommen sind. In der Folge konnte eruiert werden, wie Datenverarbeitungen konkret erfolgen können und für welche Datenverarbeitungen gegebenenfalls zunächst eine Rechtsgrundlage geschaffen werden muss. Es hat sich der Eindruck verfestigt, dass hierdurch ein zusätzlicher spürbarer Mehrwert bei den Fachbereichen generiert werden konnte. Hierbei bin ich bestrebt, praxistaugliche Lösungsvorschläge zu unterbreiten, die für die Fachbereiche in ihrer täglichen Arbeit umsetzbar sind und gleichzeitig den datenschutzrechtlichen Anforderungen des Bundesnachrichtendienstgesetzes entsprechen.

Ebenfalls positiv ist, dass dieses Jahr eine praxistaugliche Einigung zum Umfang meiner Einsichtsrechte erzielt werden konnte. Vor diesem Hintergrund sehe ich zurzeit keine Notwendigkeit, meine Einsichtsrechte gegebenenfalls per Klage durchsetzen zu müssen.

Soweit Überlegungen zur Notwendigkeit der Schaffung neuer gesetzlicher Regelungen aufkamen, wurde dies beim Bundeskanzleramt als federführendes Ressort für Gesetzesvorhaben angeregt.

7.12 Austausch mit anderen nationalen und internationalen Aufsichtsbehörden

Durch den Austausch mit anderen lernen und mehr erreichen – diese Zielsetzung ist bei der Datenschutzaufsicht grundsätzlich schon lange etabliert, und zwar national wie international. Auch im Bereich der Aufsicht über Nachrichtendienste arbeite ich aktiv an einer Verstetigung dieses Austauschs, mit der im Ergebnis die Arbeit aller Beteiligten verbessert wird.

Seit 1978 gibt es auf nationaler Ebene die Konferenz der Datenschutzbeauftragten des Bundes und der Länder. In verschiedenen Arbeitskreisen arbeiten die Datenschutzaufsichtsbehörden hier zusammen. Auch auf europäischer bzw. internationaler Ebene gibt es seit langem regelmäßige Zusammenkünfte der Datenschutzaufsichtsbehörden wie den Europäischen Datenschutzausschuss mit seinen Unterarbeitsgruppen sowie die Global Privacy Assembly. Von einer solchen Tradition und Intensität ist der Austausch mit anderen Aufsichtsgremien, die auf nationaler wie auch auf internationaler Ebene ebenfalls für die Kontrolle der Nachrichtendienste zuständig sind, noch weit entfernt.

Auf Bundesebene gibt es neben meiner Behörde als weitere Kontrollorgane vor allem das Parlamentarische Kontrollgremium (PKGr), die G 10-Kommission und den Unabhängigen Kontrollrat (UK-Rat). Im April 2023 habe ich diese Institutionen zu einem ersten Round Table in Berlin eingeladen. Impulsgeber waren der ehemalige Präsident des Bundesverfassungsgerichts, Herr Prof. Dr. Hans-Jürgen Papier, der Vorsitzende des Parlamentarischen Kontrollgremiums, Herr Dr. Konstantin von Notz, und Herr Dr. Bijan Moini, Leiter des Legal Teams und Syndikus der Gesellschaft für Freiheitsrechte.

Auf internationaler Ebene gibt es seit einigen Jahren verschiedene Initiativen, um Kontrollorgane vor allem aus Europa und Amerika an einen Tisch zu bringen. Teilweise ist der Kreis der Teilnehmenden begrenzt auf die Kontrollorgane selbst, ungeachtet derer durchaus unterschiedlichen Kompetenzen und personellen Ausstattung. Teilweise wird der Kreis weiter gezogen und umfasst z. B. auch die interne Kontrolle in den Nachrichtendiensten selbst.

Im Berichtszeitraum haben meine Mitarbeitenden an zwei entsprechenden Veranstaltungen teilgenommen, einmal am International Intelligence Oversight Forum in den USA und einmal an der European Intelligence Oversight Conference, die in Norwegen tagte. Bei beiden finden die sog. Chatham House Rules Plus Anwendung, was bedeutet, dass die Teilnehmerinnen und Teilnehmer sich in geschützter Atmosphäre über allgemeine Dinge ihrer Arbeit austauschen. Aussagen von Teilnehmenden dürfen nur nach ausdrücklicher Zustimmung weiterverwendet werden.

Auch wenn sich dieser Austausch bislang nur auf allgemeine rechtliche Aspekte und Rahmenbedingungen der Arbeit bezieht, zeigt sich doch, dass die meisten Kontrollorgane mit denselben Problemen zu kämpfen haben, wie z. B. der Frage, ob uneingeschränkte Einsicht in alle Unterlagen ermöglicht wird.

Alle Beteiligten schätzen die Möglichkeit zum Austausch und sind davon überzeugt, dass auf der Ebene der Aufsichtsbehörden die Kooperation wichtig und notwendig sei. Denn wenn die Zusammenarbeit der Nachrichtendienste grenzüberschreitend ist, darf die Zusammenarbeit der Aufsichtsbehörden nicht an der Grenze enden. Faktisch ist dies aber noch ein langer Weg, der auch mit diversen rechtlichen Unklarheiten verbunden ist, zum Beispiel hinsichtlich der Möglichkeit des konkreten

Austauschs von Informationen, die der Vertraulichkeit unterliegen.

Ich werde mich weiterhin dafür einsetzen, dass Kontrollorgane über Nachrichtendienste die Möglichkeiten der Zusammenarbeit bekommen, die sie benötigen, und diese auch im Sinne einer angemessenen Kontrolle zu nutzen.

Ich empfehle dem Gesetzgeber, eindeutige und umfassende Regelungen zur Zusammenarbeit der Aufsichtsorgane über die Nachrichtendienste zu schaffen.

Querverweise:

4.2 Europäischer Datenschutzausschuss, 4.3 Global Privacy Assembly

7.13 Widerspruch gegen meine Einsicht in Sicherheitsakten

Der Begriff Widerspruch ist im Datenschutz durch die DSGVO inzwischen zu Recht sehr positiv besetzt, aber Widerspruch ist nicht gleich Widerspruch. Der Widerspruch gegen die Einsicht des BfDI in die Sicherheitsakte steht in einem anderen Kontext und die tatsächliche Konsequenz scheint nicht allen betroffenen Personen bewusst zu sein.

Das Sicherheitsüberprüfungsgesetz (SÜG) regelt in § 36a die unabhängige Datenschutzkontrolle durch meine Behörde und zugleich ein Widerspruchsrecht der betroffenen Person gegen die Einsichtnahme in Akten über deren Sicherheitsüberprüfung durch mich (§ 36a Abs. 2 Satz 3 SÜG).

Das Widerspruchsrecht ist Ausdruck der Datenhoheit der betroffenen Person. Sicherheits(überprüfungs)akten enthalten Daten aus nahezu allen Lebensbereichen der betroffenen Person und dokumentieren umfassend persönliche, dienstliche und arbeitsrechtliche Verhältnisse. Das reicht von familiären Beziehungen über finanzielle Verhältnisse bis hin zu strafrechtlichen Informationen. Die Sicherheits(überprüfungs)akten können insbesondere auch Aussagen und Bewertungen von Referenzpersonen enthalten. Zum Schutz der überprüften Personen räumt das SÜG diesen die Abwägungsentscheidung zwischen der Aufklärung einer möglichen Verletzung ihrer Rechte und der Geheimhaltung der Daten vor mir ein.

Dem Gesetz nach bezieht sich das Widerspruchsrecht eigentlich auf eine im Einzelfall konkret bevorstehende Kontrolle durch meine Behörde. In der Praxis kommt es allerdings vor, dass auch Widersprüche von sicherheitsüberprüften Personen direkt bei mir eingehen, ohne dass eine Kontrolle durch meine Mitarbeiterinnen und Mitarbeiter bei einer öffentlichen bzw. nichtöffentlichen Stelle konkret bevorsteht. Dementsprechend ist zu vermuten, dass die widersprechende Person davon ausgeht, dass ihr einmal erhobener Widerspruch dauerhaft gilt, solange die Sicherheits(überprüfungs)akte existiert, auf die er sich bezieht.

In der Praxis ist jedoch eine Vernichtung der bei mir eingegangenen Widersprüche im Gleichklang mit der dazugehörigen Sicherheits(überprüfungs)akte nicht umsetzbar, da ich nicht die aktenführende Stelle bin und somit keine Information über die Vernichtung der Akten erhalte. Dies würde de facto zu einer unbefristeten Speicherung der personenbezogenen Daten in meinem Haus führen.

Mit Blick auf den Grundsatz der Speicherbegrenzung, aber auch das Geheimhaltungsinteresse der widersprechenden Person gegenüber meiner Behörde, habe ich einen dringenden Regelungsbedarf in Punkto zeitliche Aufbewahrung von Widersprüchen gesehen und eine entsprechende Regelung meinem Löschkonzept herbeigeführt. Orientiert an der kürzest möglichen Vernichtungsfrist nach dem SÜG, werden danach Widersprüche samt dem damit verbundenen Schriftwechsel künftig nach Ablauf eines Jahres ab Eingangsdatum des Widerspruchs bei mir gelöscht bzw. vernichtet. So ist sichergestellt, dass ein Widerspruch bei meiner Behörde nicht länger als die zugehörige Sicherheitsakte oder Sicherheitsüberprüfungsakte aufbewahrt wird.

Geht ein Widerspruch in meinem Haus ein, informiere ich die betroffene Person in der Eingangsbestätigung über die Speicherdauer und den Vernichtungszeitpunkt ihres Widerspruchs sowie die Möglichkeit, einen dauerhaften Widerspruch unmittelbar bei den verantwortlichen Stellen einzulegen. Die verantwortliche Stelle ist in dem Fall die bzw. der zuständige Sicherheitsbevollmächtigte, Geheimschutzbeauftragte oder Sabotageschutzbeauftragte. Nur so kann sichergestellt werden, dass der Widerspruch der betroffenen Person in der dazugehörigen Sicherheits(überprüfungs)akte abgelegt und damit Teil des Akteninhalts ist. Dadurch ist gewährleistet, dass Widersprüche nicht länger vorgehalten werden als die von ihnen betroffenen Sicherheits(überprüfungs)akten.

Geltende Vernichtungsfristen nach dem SÜG (§§ 30, 19 Abs. 2 und 3 SÜG) bleiben gewahrt und dem Grundsatz der Datensparsamkeit wird Rechnung getragen. Auch bleibt der Widerspruch auf diese Weise im Falle eines Wechsels des Dienstherrn oder Arbeitgebers eindeutig der betreffenden Akte zuzuordnen. Auf diese Weise lässt

sich eine Einsichtnahme durch meine Behörde bis zum Widerruf des Widerspruchs bzw. bis zur Vernichtung der jeweiligen Akte gänzlich ausschließen.

Über die tatsächliche Konsequenz ihres Widerspruchs sind sich allerdings nicht alle betroffenen Personen bewusst. Daher weise ich in meinen Schreiben immer ausdrücklich darauf hin, dass die betroffene Person mit ihrem Widerspruch einen Verzicht auf die unabhängige Aufsicht über den Umgang mit ihren personenbezogenen Daten zugunsten der Geheimhaltung dieser Daten vor meiner Behörde getroffen hat, den sie aber durch Widerruf des Widerspruchs jederzeit wieder ändern kann.

7.14 Speicherung von Daten nach oder trotz Einstellung des Ermittlungsverfahrens

Wird ein Ermittlungsverfahren eingestellt, dürfen die personenbezogenen Daten der betroffenen Person nicht pauschal bis zum Eintritt der Verjährung, sondern nur auf Grundlage einer Einzelfallprüfung in polizeilichen Informationssystemen weiter gespeichert bleiben.

Ist eine Person Ziel polizeilicher Ermittlungen, werden ihre personenbezogenen Daten naturgemäß in polizeilichen Informationssystemen gespeichert. Die Strafverfolgungsbehörden werden tätig, sobald der Anfangsverdacht einer Straftat besteht. Die Schuld der betroffenen Person steht zu Beginn der Ermittlungen nicht fest.

So werden in vielen Fällen Ermittlungsverfahren eingestellt, ohne dass es zu einer Anklage kommt. Dies kann bei geringer Schuld aus Opportunitätsgründen geschehen oder weil die Person der Begehung der Straftat nicht hinreichend verdächtig ist bzw. sich ein Verdacht nicht bestätigt oder weil der Strafverfolgung ein Verfahrenshindernis entgegensteht. Bei jeder Verfahrenseinstellung stellt sich die Frage, ob eine weitere Speicherung der personenbezogenen Daten erforderlich bzw. rechtlich zulässig ist.

Das Bundeskriminalamt (BKA) vertritt die Auffassung, dass eine Datenspeicherung – nach einer Einstellung des Ermittlungsverfahrens mangels hinreichenden Tatverdachts nach § 170 Abs. 2 der Strafprozessordnung – bis zum Eintritt der Verjährung regelmäßig erforderlich sei, weil während dieses Zeitraums neue Beweismittel auftauchen könnten, die Anlass zur Wiederaufnahme der Ermittlungen geben. Etwas Anderes möge sich ausnahmsweise ergeben, wenn der Verdacht einer Straftat bereits zum Zeitpunkt der Einstellung restlos ausgeräumt sei und daher bereits zu diesem Zeitpunkt ausgeschlossen werden könne, dass die Daten in Zukunft noch erforderlich sind.[96] Ob diese Daten ausnahmsweise zu löschen sind, sei von der sachbearbeitenden Stelle bei Einstellung im Einzelfall zu prüfen.

Dieser Haltung des BKA bin ich entgegengetreten. Zwar sind wir uns darüber einig, dass die Erforderlichkeit der weiteren Speicherung im Einzelfall zu prüfen ist. Fehlerhaft ist jedoch aus meiner Sicht die Annahme eines Regel-Ausnahme-Verhältnisses dahingehend, dass eine Datenspeicherung trotz Einstellung regelmäßig bis zum Eintritt der Verjährung erforderlich sei und eine Löschung nur ausnahmsweise in Betracht komme, wenn der Verdacht einer Straftat bereits zum Zeitpunkt der Einstellung restlos ausgeräumt ist. Vielmehr ist bei einer Verfahrenseinstellung immer im Einzelfall zu prüfen, ob der Fortbestand der Speicherung noch begründet werden kann.

Auch wenn ein sogenannter Restverdacht besteht, wirkt sich eine Einstellung auf die Frage aus, ob die weitere Speicherung verhältnismäßig ist. In seinem Beschluss hat das Bundesverfassungsgericht[97] in diesem Sinne ausgeführt, dass es im Falle eines Freispruchs oder der Verfahrenseinstellung der Überprüfung bedarf, ob noch Verdachtsmomente gegen die betroffene Person bestehen, die eine Fortdauer der Speicherung zur präventiv-polizeilichen Verbrechensbekämpfung rechtfertigen.

Um die Intensität des Restverdachts beurteilen zu können, sind die Gründe der Verfahrensbeendigung entscheidend. Bei der Einzelfallprüfung sind neben dem Tatvorwurf auch die Rechtsgutbeeinträchtigung der betroffenen Person und etwaige Stigmatisierungswirkungen zu berücksichtigen.[98] Die vorzunehmende Einzelfallprüfung muss dabei nachvollziehbar dokumentiert werden.

Aufgrund ihrer hohen praktischen Bedeutung beabsichtige ich, diese Problematik bei meinen künftigen Kontrollen noch stärker in den Fokus zu rücken.

96 Beschluss des BayObLG vom 27. Januar 2020 – 203 VAs 1846/19)
97 Beschluss des BVerfG vom 16. Mai 2002, Aktenzeichen: BvR 2257/01
98 Beschluss des OLG Frankfurt a. M. vom 20.12.2022 – 3 VAs 14/22, Rn. 14

7.15 Beanstandung einer Großdatei beim BND

In meinem 31. Tätigkeitsbericht (Nr. 9.4.11) habe ich über die Kontrolle des Archivs einer Großdatei beim Bundesnachrichtendienst berichtet. Die von mir dabei beanstandeten datenschutzrechtlichen Verstöße wurden bis heute nicht abgestellt. In dem Archiv werden einige Millionen personenbezogene Daten rechtswidrig gespeichert.

Im Jahr 2022 haben meine Mitarbeiterinnen und Mitarbeiter das Archiv einer Großdatei beim Bundesnachrichtendienst kontrolliert, in dem sich Dokumente im zweistelligen Millionenbereich befinden. Die Verarbeitung personenbezogener Daten in diesem Archiv habe ich beanstandet.

Hintergrund meiner Beanstandungen ist die ohne Prüfung auf Auftragsrelevanz erfolgende automatisierte Speicherung der zuvor bereits mehr als 10 Jahre in der Großdatei gespeicherten personenbezogenen Daten in dem Archiv sowie das Unterlassen der Erforderlichkeitsprüfung nach Zugriff auf personenbezogene Archivdaten.

Bis zum Redaktionsschluss wurden keine umsetzbaren Maßnahmen zur Abstellung des rechtswidrigen Zustandes ergriffen. Dieser dauert trotz meiner Beanstandungen bis heute weiter an.

8 Einzelthemen

8.1 Onlinezugangsgesetz

2017 hatte der Gesetzgeber im Onlinezugangsgesetz (OZG) Bund und Länder verpflichtet, binnen fünf Jahren, das heißt bis Ende 2022, sämtliche digitalisierbaren Verwaltungsleistungen auch elektronisch anzubieten. Der bisher in den meisten Fällen notwendige „Gang auf's Amt", beispielsweise für die Beantragung von Sozialleistungen, behördliche Genehmigungen oder den Erhalt von Urkunden und Bescheinigungen, sollte weitgehend der Vergangenheit angehören. Dieses Ziel wurde äußerst deutlich verfehlt. Mit dem erst jetzt vorliegenden Entwurf eines OZG-Änderungsgesetzes (auch „OZG 2.0" genannt) versucht der Gesetzgeber, der Verwaltungsdigitalisierung neuen Schwung zu geben.

Zentralisierung der Bürgerkonten zur BundID

Die Identifizierung und Authentifizierung von Bürgerinnen und Bürgern, die eine Verwaltungsleistung nutzen möchten, erfolgt in Nutzerkonten. Bislang bieten sowohl der Bund als auch die Länder solche Konten an. Mit dem OZG 2.0 sollen die Länderkonten nach Ablauf einer Übergangsfrist von 3 Jahren vollständig entfallen und künftig mit der BundID nur noch ein zentrales Bürgerkonto durch den Bund bereitgestellt werden. Das hat jedoch den Nachteil, dass die Identifizierung und Authentifizierung der Bürgerinnen und Bürger bei der Nutzung von Verwaltungsleistungen bundesweit zentralisiert wird. Damit würden sich Online-Behördengänge beinahe der gesamten Bevölkerung verfolgen und auswerten lassen. Bei der Umsetzung wird der Bund den daraus resultierenden Risiken für die Rechte der betroffenen Personen und die Sicherheit der Verarbeitung durch entsprechend strenge technische und organisatorische Maßnahmen Rechnung tragen müssen. Die Umsetzung werde ich weiterhin eng begleiten.

Freiwilligkeit bei der Nutzung elektronischer Verwaltungsleistungen

Positiv ist festzustellen, dass es Bürgerinnen und Bürgern auch künftig freistehen soll, ob sie ein Bürgerkonto einrichten und nutzen. Daraus folgt, dass die Verwaltung die Freiwilligkeit durch eine gestufte Prüfung sicherstellen muss. Diese Prüfung ist für jede einzelne Verwaltungsleistung vorzunehmen.

Einfache elektronische Verwaltungsleistungen, die nicht zwingend einer Identifizierung und Authentifizierung des Bürgers bzw. der Bürgerin bedürfen, müssen auch ohne Einrichtung einer BundID genutzt werden können, zum Beispiel durch Bereitstellung eines einfachen Online-Formulars. Sofern eine Verwaltungsleistung zwar ein Nutzerkonto erfordert, jedoch eine Identifizierung mit dem Vertrauensniveau „hoch" nicht notwendig ist, muss Bürgerinnen und Bürgern eine bloße Basisregistrierung für die BundID möglich sein, bei der zwar personenbezogene Daten wie die Anschrift anzugeben sind, jedoch keine Identifizierung mit dem Personalausweis notwendig ist. Nur wenn eine Verwaltungsleistung eine Identifizierung und Authentifizierung der Nutzenden zwingend erfordert, darf für das Online-Verfahren eine solche gefordert werden. Beispielsweise indem eine nutzende Person sich mit der eID-Funktion seines Personalausweises authentisieren muss. Auch in solchen Fällen ist stets zu beachten, dass die Nutzung der BundID freiwillig ist. Das bedeutet, dass immer alternative, gleichwertige Zugangswege bestehen müssen, für die eine BundID nicht erforderlich ist.

Es wäre wünschenswert, dass der Gesetzgeber die Freiwilligkeit über die Einrichtung und Nutzung der BundID hinaus explizit im Gesetz verankert. Denn es darf nicht nur in der freien Entscheidung der betroffenen Personen liegen, ob sie überhaupt eine BundID verwenden. Sondern sie müssen beispielsweise auch frei darüber entscheiden, ob sie ein dauerhaftes oder nur ein temporäres Nutzerkonto für eine einmalige Identifizierung anlegen und welche Funktionen und Dienste sie in dem Nutzerkonto im Einzelnen verwenden.

Personalausweis als primäres Identifizierungsmittel

Ist eine Identifizierung und Authentifizierung notwendig, so soll diese in der BundID künftig nur noch auf

dem Vertrauensniveau „hoch“ möglich sein. Das würde bedeuten, dass sich Bürgerinnen und Bürger in solchen Fällen in der BundID mit der eID-Funktion des Personalausweises, der eID-Karte oder dem elektronischen Aufenthaltstitel identifizieren müssen. Allerdings soll daneben für Verwaltungsleistungen, die lediglich das Vertrauensniveau „substanziell“ erfordern, mindestens bis zum 30. Juni 2026 die Identifizierung mit Elster-Softwarezertifikaten möglich sein. Mit dem OZG 2.0 soll das Bundesministeriums des Innern und für Heimat (BMI) und das Bundesministerium der Finanzen (BMF) ermächtigt werden, diese Frist durch Rechtsverordnung uneingeschränkt zu verlängern. Die Zulassung von Elster-Softwarezertifikaten für Verwaltungsleistungen auf dem Vertrauensniveau „substanziell“ ist jedoch abzulehnen, da diese Zertifikate keine entsprechend zuverlässige Identifizierung sicherstellen. Erst recht sollte daher die Übergangsfrist, innerhalb derer Elster-Softwarezertifikate im Bürgerkonto noch verwendet werden können, nicht verlängert werden.

Elster als Identifizierungsmittel im Organisationskonto

Anders als das Bürgerkonto ist die Nutzung des Organisationskontos für Unternehmen im Sinne des Unternehmensbasisdatenregistergesetzes verpflichtend – worunter auch natürliche Personen fallen können. Nach dem OZG-Änderungsgesetz werden Elster-Softwarezertifikate als Identifizierungsmittel im Organisationskonto für eine Übergangsfrist von fünf Jahren zugelassen. Vorgeschlagen wird, dass auch diese Frist durch Rechtsverordnung des BMI und des BMF unbeschränkt verlängert werden kann.

Da die Elster-Softwarezertifikate nicht die Mindestanforderungen an ein geeignetes, sicheres Identifizierungsmittel auf dem Vertrauensniveau „substanziell“ erfüllen, ist auch hier eine Verlängerung der Übergangsfrist abzulehnen.

Zudem sieht der Entwurf des OZG 2.0 zwar vor, dass Behörden von der zwingenden Nutzung des Organisationskontos absehen „können“, wenn im Einzelfall ein höheres Vertrauensniveau erforderlich ist – dem Wortlaut nach müssen sie es aber nicht. Im Organisationskonto werden teils sensible personenbezogene Daten verarbeitet, beispielsweise Gesundheitsdaten wie Angaben zu Schwerbehinderungen oder Schwangerschaften von Beschäftigten. In solchen Fällen, in denen ein höheres Vertrauensniveau gefordert ist, werden die Behörden von der Nutzung des Unternehmenskontos in der Regel absehen müssen. Durch die Nutzung eines Elster-Softwarezertifikats zur Identifizierung und Authentifizierung wird das geforderte hohe Vertrauensniveau nämlich nicht erreicht.

Datenverarbeitung im Verwaltungsportal des Bundes

Die Rechtsgrundlagen für die Datenverarbeitung im Verwaltungsportal des Bundes sollen durch das OZG 2.0 weiter gefasst werden als bisher – dem Gedanken folgend, dass an das Verwaltungsportal sehr unterschiedliche Dienste angeschlossen und damit eine Vielfalt an Daten zu verschiedenen Zwecken verarbeitet werden. Darunter werden auch Dienste fallen, die heute noch gar nicht existieren, so dass es einer gewissen Entwicklungsoffenheit der Vorschriften bedarf. Ich freue mich, dass es infolge meiner Beratung gelungen ist, Verbesserungen bei der Normenklarheit zu erreichen. Allerdings sollten noch schärfere Konturierungen vorgenommen werden, da es sich beim Verwaltungsportal im Kern um eine Datendrehscheibe handelt. Die Verwaltungsverfahren werden nicht im Verwaltungsportal, sondern mithilfe besonderer Fachanwendungen abgewickelt, so dass die Verarbeitungsbefugnis im Verwaltungsportal deutlicher auf den eigentlichen Zweck zugeschnitten werden kann, ohne die Entwicklungsoffenheit zu gefährden.

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.

8.2 Registermodernisierung

Die Registermodernisierung entwickelt sich zum Fundament für die Verwaltungsdigitalisierung. Onlinezugangsgesetz und weitere legislative Vorhaben setzen auf die Vorteile eines eindeutigen Identifikators, um das Once-Only-Prinzip voranzutreiben. Die Daten sollen laufen, nicht die Bürgerinnen und Bürger. Doch wie kann dabei sichergestellt werden, dass diese die Hoheit über ihre Daten behalten?

Ausgangssituation

Am 6. April 2021 wurde das Registermodernisierungsgesetz (RegMoG) im Bundesgesetzblatt verkündet. Durch

das darin enthaltene Identifikationsnummerngesetz (IDNrG) wurde die Steueridentifikationsnummer gemäß § 139b Abgabenordnung (AO) als allgemeine, einheitliche Identifikationsnummer (IDNr) zum Zwecke der Erbringung von digitalisierten Verwaltungsleistungen nach dem Onlinezugangsgesetz (OZG) sowie zur Durchführung eines registerbasierten Zensus eingeführt. Gleichzeitig wurden einige wichtige Ausgleichsmaßnahmen bestimmt, die die Risiken mindern sollen, die mit der Nutzung der IDNr und des Systems, in das sie eingebettet wird, verbunden sind. Hierzu gehört vor allem die Errichtung eines Datenschutzcockpits (DSC), anhand dessen mit der IDNr verknüpfte Datenübermittlungen sowie Datenbestände niedrigschwellig transparent gemacht werden sollen. Auch sollen die öffentlichen Stellen, die die IDNr bereichsübergreifend verwenden, nicht direkt miteinander kommunizieren können, sondern ausschließlich über Vermittlungsstellen.

Wie schon in meinen vorangegangenen Tätigkeitsberichten (zuletzt 31. TB Nr. 8.6) dargelegt, halte ich die derzeitige Ausgestaltung der IDNr für nicht vereinbar mit dem Recht auf informationelle Selbstbestimmung und die Einführung der IDNr dementsprechend für verfassungswidrig. In ihrer Form als einheitlicher, bereichsübergreifender Identifikator wird nicht nur die Verknüpfbarkeit innerhalb eines rechtsstaatlich gesicherten Systems stark vereinfacht und deutlich treffgenauer. Durch den für nahezu jeden Lebensbereich eines Bürgers gleichlautenden Identifikator wird zugleich auch die Verknüpfbarkeit außerhalb dieses Systems außerordentlich niedrigschwellig. Die Erfassbarkeit großer Facetten der Persönlichkeit steigt dadurch in einem Maße, dass eine umfassende Katalogisierung nicht mehr nur eine ferne und überaus aufwendige Möglichkeit ist. Diese neuartige Gefährdungslage allein greift bereits übermäßig in das Recht auf informationelle Selbstbestimmung ein.

Näheres finden Sie im Hintergrundpapier des BfDI zur Registermodernisierung

(QR-Code scannen oder klicken)

Diese Gefährdungslage ließe sich nur durch weitere strukturelle Maßnahmen, wie z. B. der Nutzung bereichsspezifischer Kennzeichen sowie nur begrenzt wissender Vermittlungsstellen, auf ein erträgliches Maß mindern. Dabei gingen übrigens weder Funktionalität noch Nutzungskomfort für die Bürgerinnen und Bürger sowie die Verwaltungen verloren.

An dieser fundamentalen Einschätzung hat sich durch den Entschließungsantrag des Ausschusses für Inneres und Heimat des Deutschen Bundestages (Ausschussdrucksache 20(4)258 vom 19. Juli 2023) nichts geändert. Denn auch hiernach wird an der IDNr in seiner jetzigen Form grundsätzlich festgehalten. Die Zuordnung von personenbezogenen Daten anhand der IDNr außerhalb des gesicherten Systems soll dabei in Zukunft lediglich durch rechtliche und organisatorische Maßnahmen stärker gehemmt werden. Strukturelle Maßnahmen, die die Zusammenführbarkeit auch ohne menschliches Zutun einschränken, sind nicht angedacht. Wobei für die Zukunft zumindest geplant ist, dass breit aufgestellte Forschungsprojekte neuartige Ansätze zur Umsetzung der Registermodernisierung untersuchen und bewerten sollen. Ein wichtiger Auftrag, für den ich gerne beratend zur Verfügung stehen werde, der aber natürlich besser innerhalb der letzten Legislaturperiode vor Verabschiedung des RegMoG in seiner jetzigen Form erfolgt wäre.

Besonders begrüßenswert ist allerdings die im Entschließungsantrag enthaltene Forderung nach einem noch stärkeren DSC. Transparenz ist meines Erachtens das wichtigste Mittel, um die ansonsten undurchdringliche Macht zur Zusammenführung auf staatlicher Seite möglichst bürgernah auszugleichen. Nur wenn Bürgerinnen und Bürger wissen, welche öffentlichen Stellen mit welchen Datensätzen an den neuartigen, niedrigschwelligen Datenaustauschmöglichkeiten teilnehmen und sie nutzen, können sie in der Once-Only-Wirklichkeit ihre Rechte effektiv wahrnehmen.

Das Once-Only-Prinzip – eine Abkehr vom Direkterhebungsgrundsatz

Das Once-Only-Prinzip spielt eine erhebliche Rolle bei der geplanten Verwaltungsdigitalisierung. Demzufolge soll ein personenbezogenes Datum einer Bürgerin oder eines Bürgers von staatlicher Stelle nur ein einziges Mal direkt erhoben werden. Alle folgenden staatlichen Verarbeitungen (auch von anderen öffentlichen Stellen) sollen im Optimalfall sodann auf die einmal erhobenen Daten zugreifen.

Das Once-Only-Prinzip steht insofern im direkten Gegensatz zum Grundsatz der Direkterhebung, der als Reaktion auf das Volkszählungsurteil des Bundesverfassungsgerichts durch den damaligen Gesetzgeber in das Bundesdatenschutzgesetz eingeführt wurde. Die Direkterhebung hat den Vorteil besonders grundrechtsschonend zu sein. Da die relevanten personenbezogenen Daten unmittelbar beim Betroffenen erhoben werden, herrscht insofern ein sehr hoher Grad an Transparenz und Kontrolle. Weiterhin ist eine verwaltungsübergreifende Zusammenführung alleine dadurch gehemmt, dass ein Datenaustausch unter Behörden in der Regel überhaupt nicht vorgesehen und keine dementsprechende Infrastruktur gegeben ist.

Diese das Recht auf informationelle Selbstbestimmung besonders achtende Variante der Erhebung hat sich auch nicht durch Einführung der DSGVO überholt. Zwar trifft die DSGVO selbst keine wesentliche Unterscheidung zwischen der Erhebung beim Betroffenen und der bei einer dritten Person (Ausnahme: Informationspflichten). Allerdings bleiben öffentlich-rechtliche Datenverarbeitungen auf Grundlage des Art. 6 Abs. 1 lit. e) DSGVO weiterhin an mitgliedsstaatliches Recht gebunden. Dies umfasst im Falle Deutschlands auch das Grundgesetz und die höchstrichterliche Auslegung der darin enthaltenen Grundrechte.

Dennoch ist eine Abkehr von der Direkterhebung auch vor diesem Hintergrund grundsätzlich möglich. Die wesentlichen, besonders grundrechtsschonenden Elemente der Direkterhebung wie Transparenz, Kontrolle und strukturelle Hemmnisse der Zusammenführbarkeit müssen dann allerdings mit anderen Mitteln mindestens ebenso effektiv hergestellt werden.

Diese Anforderungen verschärfen sich je nach Grad der abstrakten Zusammenführbarkeit von personenbezogenen Daten verschiedener Lebensbereiche durch den Staat. Je mehr das Once-Only-Prinzip gelebt wird und die Vernetzung der Behörden untereinander steigt, desto stärker müssen die alternativen Ausgleichsmaßnahmen ausgeprägt sein. Ein eindeutiger Identifikator – wie die IDNr – ist dabei lediglich ein besonders wirksamer Katalysator für die gesteigerte Zusammenführbarkeit. Der Direkterhebung gleichwertige Ausgleichsmaßnahmen müssten aber auch bei einem Once-Only-Ansatz ohne Identifikator vorgesehen werden.

Gesamtsteuerung Registermodernisierung

Tatsächlich umgesetzt wird die Registermodernisierung seit Ende 2021 durch eine dem IT-Planungsrat (IT-PLR) unterstehende Bund-Länder-Arbeitsgruppe „Gesamtsteuerung Registermodernisierung“ (GS RegMo). Auf der operativen Ebene findet die Arbeit in Programmbereichen statt. Auch in diesem Berichtszeitraum beriet ich die GS RegMo gemeinsam mit Vertreterinnen und Vertretern der Datenschutzkonferenz (DSK) auf mehreren Ebenen, vorwiegend innerhalb des Lenkungskreises und des Programmbereichs Recht.

Schwerpunkt der Beratungen innerhalb der Programmbereiche war weiterhin das Nationale Once-Only-Technical-System (NOOTS). Das NOOTS wird die zentrale technische Einrichtung für den Austausch von Nachweisen zwischen Online-Diensten nach dem OZG und Registern sein. Zudem wird das NOOTS über eine Schnittstelle, genannt Intermediäre Plattform (IP), mit dem OOTS der EU verbunden werden, die einen grenzüberschreitenden Nachweisaustausch auf Grundlage der Single-Digital-Gateway-VO (SDG-VO) zulassen wird.

Bei den Beratungen zum NOOTS und der IP ging es insbesondere um die Rechtsnatur dieser Komponenten. Sollen es rein technische Komponenten sein, die durch die angeschlossenen Behörden betrieben werden oder ist es eine eigenständige Stelle mit entsprechendem gesetzlichen Auftrag? Aktuell werden insofern noch verschiedene architektonische Ansätze innerhalb der verschiedenen Programmbereiche diskutiert. Datenschutzrechtlich gibt es dabei leider entgegengesetzte Anforderungen: Auf der einen Seiten würde eine eigenständige Organisation der Komponenten zu einer klaren Verantwortungsverteilung im Sinne des Art. 4 Nr. 7 DSGVO führen. Jeder öffentlichen Stelle wäre so ohne weitere Verhandlungen bewusst, welche Aufgaben ihr obliegen. Auf der anderen Seite würde der ohnehin schon stark zersplitterte digitalisierte Verwaltungspro-

zess noch weiter unterteilt werden. Bereits nach aktuellen Planungen sind eine Vielzahl an öffentlichen Stellen an einem Online-Antrag beteiligt (Beispiel: Online-Dienst betreibende Behörde, mehrere nachweisliefernde Stellen, Nutzerkonto Bund und die letztlich über den Antrag entscheidende Fachbehörde). Kämen mit dem NOOTS und der IP noch zusätzliche Verantwortliche alleine für den Übermittlungsweg hinzu, könnte dies dazu führen, dass die Betroffenen kaum mehr von außen nachvollziehen können, an welche Stelle sie sich für ein spezifisches Anliegen richten müssen. Auf der anderen Seite wäre eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit im Ergebnis reine Augenwischerei. Denn bei einem Auftragnehmer und mehreren tausenden Verantwortlichen ist klar, wer eigentlich die Vorgaben macht. Hier sind gegebenenfalls neuartige gesetzliche Lösungen, wie z. B. die Einrichtung einer gemeinsamen Anlaufstelle für Betroffene, notwendig, die sowohl den Anforderungen der Verantwortlichen als auch der Betroffenen gerecht werden.

Darüber hinaus fanden gemeinsame Beratungen zu Pilotprojekten zur Umsetzung der SDG-VO sowie zur Gestaltung der Vorschaufunktion statt. Die Vorschaufunktion ist ein wichtiges Mittel der Transparenzschaffung, die durch die SDG-VO verpflichtend vorgesehen ist und die der Gesetzgeber im Wege des OZG-Änderungsgesetzes auch für den Betrieb des NOOTS plant. Um die grundrechtsschonende Wirkung zu entfalten, müssen meines Erachtens sowohl Antragsstellung, als auch Nachweisabruf übersichtlich und leicht verständlich eingerichtet werden. Auch ungeübte Bürgerinnen und Bürger müssen direkt erkennen können, welche Nachweise zu welchem Zeitpunkt abgerufen werden und wann sie letztlich an die zuständige Fachbehörde übermittelt werden. Hier könnte sich interessanterweise eine Anlehnung an Online-Shops anbieten. Letztlich stellen aus Sicht des Betroffenen Antrag und Nachweise eine Art Warenkorb dar, der einer Bestellung bei einer Behörde dient.

Zuletzt bin ich auch in die Gestaltung einer Rechtsverordnung zur Festlegung der Verwaltungsbereiche im Sinne des § 7 Abs. 2 IDNrG eingebunden. Hiernach erfolgen Übermittlungen anhand der IDNr zwischen verschiedenen Verwaltungsbereichen (laut Gesetzesbegründung z. B. Inneres, Soziales o. ä.) nur indirekt über Vermittlungsstellen, die den Inhalt der Übermittlung nicht kennen, dafür aber die Berechtigung zur Kommunikation abstrakt prüfen. Die Frage nach der Ziehung der Verwaltungsbereiche ist dabei datenschutzrechtlich enorm bedeutsam, denn nur in den bereichsübergreifenden Fällen entfaltet sich nach aktueller Rechtslage dieses grundrechtsschonende strukturelle Hemmnis. Es ist insofern besonders darauf zu achten, dass die Bereiche nicht zu groß gezogen werden. Gerade ein Bereich „Soziales“, der von Rente, Arbeit bis hin zur Krankenversicherung viele besonders schützenswerte Lebensbereiche der Bürgerinnen und Bürger berühren würde, würde den datenschützenden Effekt praktisch aushebeln. Hier ist eine differenzierende Sichtweise nötig. Zudem muss darauf geachtet werden, dass die abstrakte Berechtigungsprüfung nicht zur bloßen Formalität verkommt. Insbesondere wenn es sich um digitalisierte Verwaltungsverfahren handelt, muss die Berechtigungsprüfung auch den korrekten Anlass, also das Anstoßen des Verfahrens durch die Bürgerinnen und Bürger, umfassen. Andernfalls würde der Wille der Betroffenen nicht ausreichend im Prozess weiterwirken.

Insofern ist es entscheidend, dass die Vermittlungsstellen oder ähnlich sichere Einrichtungen tatsächlich zwischen den öffentlichen Stellen stehen und nicht bloß auf Entfernung eine Freigabe erteilen, deren Beachtung ggf. nur rechtlich oder organisatorisch vorgeben wäre.

Once-Only-Generalklausel im OZG-Änderungsgesetz

Bereits im letzten Tätigkeitsbericht stellte ich kurz die Pläne des BMI zur Once-Only-Generalklausel vor. Die Klausel soll es allen öffentlichen Stellen erlauben, die IDNr auf Grundlage des § 6 Abs. 2 IDNrG zur Erbringung von OZG-Leistungen zu verarbeiten. Damit werden vor allem die Fachbehörden und die Online-Dienste erfasst. Dabei führte ich bereits im 31. Tätigkeitsbericht (Nr. 8.6) aus, dass bei einem derart großflächigen Einsatz der IDNr, zumindest die Sicherungen des IDNrG ebenso großflächig angewendet werden müssen, allem voran dabei die Transparenz durch einen Anschluss dieser öffentlichen Stellen an das DSC.

Die Once-Only-Generalklausel wurde als § 5 E-Government-Gesetz Teil des Änderungsgesetzes zum OZG. Das Gesetz befindet sich aktuell im parlamentarischen Verfahren. Trotz der vorherigen Zusammenarbeit und der weiteren Beratungen im Rahmen der Ressortbeteiligung blieb die Bundesregierung allerdings dabei, keine entsprechende Anschlusspflicht an das DSC für alle öffentlichen Stellen im finalen Entwurf des OZGÄndG vorzusehen.

Dies ist meines Erachtens weiterhin ein schwerwiegender Konstruktionsfehler, der die ohnehin fehlende Balance im IDNrG weiter verschlechtert. Selbst das Flaggschiff an grundrechtsschonenden Maßnahmen, die Transparenz, würde dadurch derart geschwächt, dass sie kein wirksamer Ausgleich mehr für die fortgeschrittene Vernetzung wäre. Die Unsicherheit über den Verbleib der eigenen Daten innerhalb der miteinander verknüpf-

ten Bestände würde sich so realisieren. Das Recht auf informationelle Selbstbestimmung bliebe deutlich weniger geschützt als bei der Direkterhebung.

Dieser Entwurf erstaunt vor allem auch deshalb, weil völlig unzweifelhaft ist, dass die öffentlichen Stellen in jedem Fall Protokolle gemäß § 9 IDNrG anzulegen haben. Denn es handelt sich in diesen Fällen um Datenübermittlungen zwischen öffentlichen Stellen unter Nutzung der IDNr. Diese Protokolle dienen aber gerade dem Datenschutz und der Transparentmachung über das DSC. Es fehlt bisher allein an der Pflicht diese an das DSC zu übermitteln, wie es § 2 Nr. 3 IDNrG für die Register festlegt.

Datenschutzcockpit

Die gemeinsame Arbeit am Unterprojekt Datenschutzcockpit wurde auch 2023 erfolgreich fortgesetzt. Ich nahm gemeinsam mit Vertretern der DSK regelmäßig an den Sitzungen des Steuerungskreises sowie einigen Unterarbeitsgruppen teil. Wie im letzten Jahr stand dabei vor allem die Umsetzungsarbeit im Vordergrund. Das DSC soll über die nächsten Jahre hinweg iterativ weiterentwickelt werden. Die aktuelle erste Ausbaustufe des DSC umfasst dabei die fundamentalen Funktionen zum Abruf der Übermittlungsprotokolle der öffentlichen Stellen sowie der von ihnen übermittelten Inhaltsdaten. Weitere wichtige Funktionen, die das Navigieren und Anfragen von zahlreichen Registern erleichtern sollen, werden voraussichtlich erst in späteren Versionen Teil des DSC. Da aber die Registermodernisierung insgesamt ein iterativer Prozess ist und zunächst erst wenige Stellen angeschlossen sein werden, ist dieses Vorgehen meines Erachtens unproblematisch. Aufgrund der grundsätzlich zustandslosen Konfiguration des DSC (sog. Quellenmodell; das DSC speichert keine Daten dauerhaft, sondern ruft diese erst innerhalb der Nutzersitzung ab) sollten schon jetzt die Möglichkeiten zum Herunterladen der abgerufenen Daten geplant werden. Auch sollten die Bürgerinnen und Bürger eine Liste mit favorisierten öffentlichen Stellen und Registern lokal speichern können, die bei erneuter Nutzung des DSC dann für einen erleichterten Wiederabruf hochgeladen werden könnte.

Nach aktuellen Planungen wird die erste Ausbaustufe des DSC im Frühling 2024 in den Echtbetrieb gehen können. Dabei stünde das DSC technisch bereits jetzt bereit. Leider fehlt es an einer für den Betrieb notwendigen Rechtsverordnung im Sinne des § 10 Abs. 5 OZG. Mit Blick auf die anlaufenden Projekte unter Nutzung der IDNr schafft dies eine datenschutzrechtlich unbefriedigende Situation, in der zwar bereits Verarbeitungen stattfinden, aber noch keine Transparentmachung stattfinden kann. Dieser Zustand sollte so schnell wie möglich behoben werden.

Daneben gab es noch gemeinsame Beratungen über die Implementierung der Bestandsdatenauskunft gemäß § 10 Abs. 2 OZG. Hier steht das Projekt aber noch ganz am Anfang. Letzteres gilt auch für die im Entschließungsantrag 20(4)258 (s. o.) enthaltene Forderung nach einem Ausbau des DSC zu einem Steuerungsinstrument. Aktuell sind im DSC keine Möglichkeiten zur Freigabe oder Einflussnahme auf die Datenübermittlungen vorgesehen. Es ist im Moment lediglich ein Mittel der Transparentmachung. Diesbezüglich werden daher noch weitere intensive Beratungen notwendig sein.

In-Kraft-Setzung IDNr und Pilotierung des NWR

Am 31. August 2023 gab das BMI im Bundesgesetzblatt bekannt, dass die technischen Voraussetzungen für den Betrieb vorlägen und daher das IDNrG inkrafttrete. Zeitgleich begann das Bundesverwaltungsamt (BVA) als Registermodernisierungsbehörde mit dem Abruf der IDNr und der dazugehörigen Basisdaten beim Bundeszentralamt für Steuern zum Zwecke der Einspeicherung in das Nationale Waffenregister (NWR). Das NWR war gezielt als Pilotregister ausgewählt worden. Dieser erstmalige Abruf der IDNr, auch Ersteinspeicherung genannt, ist bereits seit Längerem Gegenstand ausführlicher Beratungen meinerseits mit dem BMI sowie dem BVA gewesen, die auch aktuell anhalten. Thema ist dabei u. a. die Auslegung des § 9 Abs. 1 IDNrG. Diskussionsgegenstand ist vor allem, ob bereits die Ersteinspeicherung eine Nutzung der IDNr in diesem Sinne ist, die entsprechend zu protokollieren und im DSC zur Anzeige zu bringen ist.

Meiner Ansicht nach ist der Begriff der Nutzung an dieser Stelle weit zu verstehen. Auch als Teil eines Datensatzes dient die IDNr der eindeutigen Unterscheidung ansonsten möglicherweise gleichlautender Basisdatensätze. Sie kann zudem im weiteren Verfahren als Hilfsmittel genutzt werden, um die Zuordnung und Qualität der erstmals empfangenen Daten zu erleichtern. Die Ersteinspeicherung bildet dabei auch einen natürlichen Anknüpfungspunkt für die Gewährleistung der grundrechtsschonenden, niedrigschwelligen Transparenz. Ohne Anknüpfung bliebe es mehr oder minder dem Zufall weiterer Übermittlungen überlassen, ob Bürgerinnen und Bürger von der Erfassung ihrer Datensätze mit der IDNr erfahren. Denn selbst wenn man die Bekanntmachung von gesetzlichen Regelungen als gleichsam wahrnehmbar für die Bürgerinnen und Bürger ansähe, wäre daraus nicht der jeweilige tatsächliche Beginn der Ersteinspeicherung erkennbar. Dieser Prozess könnte so über Jahre unsichtbar bleiben. Sinn und Zweck der

ausgleichenden Transparenz via DSC wären für einen erheblichen Zeitraum gemindert. Die Ersteinspeicherung ist damit ebenfalls zu protokollieren und sichtbar zu machen. Die Bundesregierung sieht das bislang nicht so, so dass die Ersteinspeicherung der IDNr nicht mit DSC angezeigt wird. In diesem Zusammenhang möchte ich darauf hinweisen, dass § 9 Abs. 3 IDNrG nicht so auszulegen ist, dass Regelungen bezüglich kürzerer Aufbewahrungsfristen für fachliche Protokolldaten auf die Protokolldaten für den IDNr-Gebrauch angewendet werden. Dies würde zu einer unbilligen Einschränkung der mit der Regelung des § 9 IDNrG beabsichtigten Transparenz behördlichen Handelns gegenüber Bürgerinnen und Bürgern führen.

Zukunft der Verwaltungsdigitalisierung und der Einsatz der Steuer-ID

Mit Sorge betrachte ich die aktuelle Entwicklung, eine eindeutige Zuordenbarkeit über den direkten Einsatz der Steuer-ID im Sinne des § 139b AO vorzunehmen, zumindest soweit sie Bereiche außerhalb der Finanzverwaltung betrifft. Dies ist aktuell u. a. beim Entwurf für eine Kindergrundsicherung vorgesehen sowie bei der Umsetzung des Pflegeunterstützungs- und –entlastungsgesetzes. Meiner Ansicht nach hat der Gesetzgeber mit dem IDNrG umfassend und erschöpfend den Einsatz der Steuer-ID (dort in Form der IDNr) außerhalb des Finanzbereichs für Zwecke der eindeutigen Zuordnung und der Verwaltungsdigitalisierung geregelt. Hierfür wurden Sicherungsmaßnahmen etabliert, die zumindest in Teilen einen wirksamen Ausgleich für die besonders niedrigschwellige Zusammenführbarkeit darstellen. Darunter an erster Stelle die Transparenz durch das DSC. Die Etablierung eines parallelen Systems mit mehr oder minder gleicher Zielsetzung (eindeutige Zuordnung sowie Verwaltungsdigitalisierung), welches dagegen keine derartigen Sicherungen vorhält, obwohl es materiell im Grunde denselben Identifikator nutzt (Steuer-ID und IDNr sind identisch), käme einer Umgehung gleich. Die Zusammenführbarkeit noch weiterer Persönlichkeitsfacetten der Bürgerinnen und Bürger stiege in einem nicht mehr zu rechtfertigenden Maße. Außerdem würde die Steuer-ID selbst spätestens dann ihren Status als spezifisches Kennzeichen für den Steuerbereich gefährden und selbst zu einem übergreifenden Personenkennzeichen werden. Ich empfehle daher für die Zukunft dringend, wenigstens die IDNr nach dem IDNrG für Zwecke der Zuordnung und Digitalisierung zu verwenden. Dies gilt trotz meiner weiterhin bestehenden fundamentalen Bedenken gegen die IDNr in ihrer jetzigen Form.

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.

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.

Querverweise:

8.1 Onlinezugangsgesetz, 8.11 Kindergrundsicherung, 9.2.3 Kontrolle der steuerlichen Identifikationsnummer beim Bundeszentralamt für Steuern

8.3 Quo vadis Vorratsdatenspeicherung?

Die Debatte um die Vorratsdatenspeicherung wird auch im Jahr 2023 sehr kontrovers geführt. Umso wichtiger ist es mir, für die Grundrechte aller Bürgerinnen und Bürger einzustehen. Ich werde mich für eine grundrechtsschonende Balance aus Freiheit und Sicherheit einsetzen.

Mit Urteil vom 20. September 2022 (C-793/19 SpaceNet und C-794/19 Telekom Deutschland) hat der Europäische Gerichtshof (EuGH) es nochmals in aller Deutlichkeit klargestellt: Die im deutschen Recht vorgesehene *anlasslose* Speicherung von Verkehrs- und Standortdaten ist mit dem europäischen Recht nicht vereinbar. Ich begrüße diese Entscheidung, denn die allgemeine und unterschiedslose Vorratsdatenspeicherung stellt einen erheblichen Eingriff in die Grundrechte dar.

In der Folge hat auch das Bundesverwaltungsgericht mit Urteil vom 14. August 2023 (vgl. BVerwG 6 C 6.22 – Urteil vom 14. August 2023) entschieden: Die in § 175 Abs. 1 Satz 1 i. V. m. § 176 TKG (§ 113a Abs. 1 Satz 1 i. V. m. § 113b TKG a. F.) geregelte Verpflichtung der Anbieter öffentlich zugänglicher Telekommunikationsdienste zur Speicherung der dort genannten Telekommunikations-Verkehrsdaten ist in vollem Umfang unvereinbar mit Art. 15 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) und daher nicht anwendbar.

Sehr zeitnah nach dem Urteil des EuGHs hatte das Bundesjustizministerium im Jahr 2022 einen Gesetzentwurf zum sogenannte „Quick-Freeze-Verfahren“ vorgelegt. Mangels politischem Konsens ist dieser – zwischenzeitlich geleakte – Entwurf aber noch nicht in die Ressortabstimmung gelangt. Möglich würde damit das „Einfrieren“ von Daten bei einem konkreten Anlass und auf Basis einer hierauf gerichteten richterlichen Anordnung. Die Daten würden für maximal drei Monate gesichert.

Am 11. Oktober 2023 befasste sich auch der Rechtsausschuss des Deutschen Bundestages in einer Anhörung mit der Vorratsdatenspeicherung. Konkret ging es um den Antrag der CDU/CSU Fraktion zum Thema „IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen“ (BT-Drucksache 20/3687). In dem Antrag wird die Bundesregierung aufgefordert, einen Gesetzentwurf vorzulegen, der eine solche Speicherung im Einklang mit den höchstrichterlichen Vorgaben ermöglicht.

An dieser Anhörung habe ich als Sachverständiger deutlich gemacht, dass der EuGH nur einen sehr schmalen Grat einer grundrechtskonformen allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen vorgegeben hat. Diese kommt nur zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit in Betracht. Auch die Dauer der Speicherung darf im Hinblick auf das verfolgte Ziel das absolut Notwendige nicht überschreiten.

Neben der Speicherdauer, die im Antrag mit 6 Monaten für mich nicht mehr angemessen ist, würde eine Vorratsdatenspeicherung von IP-Adressen eine genaue Bewertung der Aufzeichnung von Portadressen voraussetzen. Diese ist manchmal erforderlich, kann bei dynamischer Zuweisung ggf. aber zu einer deutlichen Erhöhung der Eingriffsintensität führen.[99]

Auch wenn der EuGH der Speicherung von IP-Adressen keinen endgültigen Riegel vorgeschoben hat, stellt sich die grundsätzliche Frage, wie nützlich dieses Instrument überhaupt ist. Denn gerade diese Nützlichkeit ist abzuwägen mit dem erheblichen Grundrechtseingriff, der mit einer Speicherung einhergeht. Dies gilt insbesondere vor dem Hintergrund möglicher Umgehungsmöglichkeiten durch Täterinnen, Täter und Tätergruppierungen in Form der Nutzung von sog. Virtual Private Networks (VPN) oder bestimmter Browser, die die IP-Adresse verschleiern und damit wiederum eine anonyme Nutzung des Internets ermöglichen – und so eine Vorratsdatenspeicherung von IP-Adressen konterkarieren.

Aus meiner Sicht bietet für viele Fallgestaltungen zudem bereits das „Quick-Freeze-Verfahren“ eine gute Balance aus Datenschutz und effektiver Strafverfolgung. Vor neuen gesetzgeberischen Aktivitäten im Bereich einer Vorratsdatenspeicherung von IP-Adressen sollte eine umfassende, unabhängige Evaluation bzw. die von dem BVerfG auch geforderte „Überwachungsgesamtrechnung“ vorgenommen werden. Wer zu weitgehend, zu pauschal oder „ins Blaue hinein“ neue Speicherbefugnisse fordert, ist weiterhin dem Risiko ausgesetzt, unverhältnismäßig zu handeln.

Diese und weitere sehr komplexe Fragestellungen gilt es bei den zu erwartenden Gesetzesentwürfen zu klären. Wer für eine Vorratsdatenspeicherung von IP-Adressen streitet, muss für alle genannten Kritikpunkte eine überzeugende Antwort liefern können.

Ich empfehle der Bundesregierung, sich bei der Diskussion um eine Vorratsdatenspeicherung für eine grundrechtsschonende Balance aus Freiheit und Sicherheit einzusetzen.

8.4 Messengerdienste

Aufgrund der rasanten Verbreitung von Smartphones und der damit einhergehenden Nutzung des mobilen Internets haben sich moderne Messengerdienste zu einem der meist genutzten Kommunikationsmittel entwickelt. Die Dienste vereinfachen die Kommunikation im Privaten und in der Arbeitswelt, bringen aber auch Herausforderungen für den Datenschutz und die Privatsphäre mit sich. Mir obliegt die datenschutzrechtliche Aufsicht über Messengerdienste, die Telekommunikationsdienste sind, und solche, die von öffentlichen Stellen betrieben werden.

Aufgrund ihrer Bedeutung als Kommunikationsmittel habe ich mich in diesem Jahr intensiv mit datenschutzrechtlichen Fragen rund um das Thema Messengerdienste beschäftigt. Um sicherzustellen, dass persönliche Informationen in der vernetzten Welt angemessen geschützt werden, haben der europäische und der deutsche Gesetzgeber datenschutzrechtliche Regelungen für Telekommunikationsdienste geschaffen, die über das Internet bereitgestellt werden. Mittlerweile hat sich so ein komplexes Regelungsdickicht entwickelt.

99 Stellungnahme an den Deutschen Bundestag vom 16. Oktober 2023 abrufbar unter: www.bfdi.bund.de/stellungnahmen

Zur Aufklärung beleuchte ich in einem Fachbeitrag auf meiner Webseite verschiedene Aspekte des Daten- und Privatsphärenschutzes bei Messengerdiensten. Dafür gehe ich zunächst der Frage nach, was Messengerdienste sind. Sie können verstanden werden als Programme oder Apps, mit denen Nutzerinnen und Nutzer in Echtzeit Nachrichten über das offene Internet austauschen können. Um Messengerdienste von anderen Onlinekommunikationsdiensten und Telemedien abzugrenzen, bedarf es einer belastbaren Definition, die ich auf meiner Webseite darstelle. Dort zeige ich auch die rechtlichen Grundlagen und meine Zuständigkeit gegenüber Messengerdiensten auf.[100]

Wird ein nach der Definition als Messengerdienst identifizierter Dienst in der Regel gegen Entgelt erbracht, handelt es sich um einen Telekommunikationsdienst i. S. d. Telekommunikationsgesetzes (TKG). Für diesen Dienst gelten neben den Anforderungen der Datenschutz-Grundverordnung (DSGVO) auch die spezifischen telekommunikationsdatenschutzrechtlichen Regelungen des Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) und des TKG. Dies umfasst etwa das Fernmeldegeheimnis, besondere Anforderungen an die Verarbeitung von Verkehrs- und Standortdaten sowie technische und organisatorische Maßnahme oder besondere Meldepflichten bei Datenschutzvorfällen. Über die Einhaltung dieser Anforderungen habe ich nach der DSGVO und dem TTDSG die datenschutzrechtliche Aufsicht.

Im Oktober 2023 habe ich zum ersten Mal den „Jour fix Messenger“ ausgerichtet, in dem ich mit für Messengerdienste Verantwortlichen künftig regelmäßig zusammenkomme. Den ersten Jour fix habe ich bewusst zunächst auf einen kleineren Teilnehmerkreis begrenzt – nämlich die kleineren und mittelgroßen Anbieter im deutschsprachigen Raum – um mit ihnen in einen offenen und vertrauensvollen Austausch zu grundsätzlichen datenschutzrechtlichen Fragen zu kommen. Der Jour fixe wurde von den teilnehmenden Dienstanbietern durchweg äußerst positiv aufgenommen, weswegen ich den Termin künftig zunächst in einem halbjährigen Turnus plane.

Um die konkreten datenschutzrechtlichen Anforderungen an Messengerdienste systematisch zu evaluieren, rechtlich einzuordnen und für Dienstanbieter übersichtlich darzustellen, habe ich zunächst für das Frontend eines Messengerdienstes im Rahmen eines sogenannten SPE-Projekts in Zusammenarbeit mit einem Experten einen Prüfkatalog erarbeitet.

Neben der Aufklärungs- und Grundsatzarbeit habe ich in diesem Jahr drei Kontroll- und Beratungsbesuche bei Messengerdiensten durchgeführt (s. Nr. 9.2.2).

Ein Thema, das aktuell und sicherlich auch künftig, die Anbietenden von Messengerdiensten besonders beschäftigt, ist das der Interoperabilität. Der Digital Markets Act verpflichtet sogenannte Gatekeeper, Unternehmen mit erheblichem Einfluss, eine anbieterübergreifende Kommunikation zu ermöglichen. Diese Vorgabe ist aus Sicht der Marktregulierung und der Sicherstellung eines fairen Wettbewerbs begrüßenswert, bringt aber neben technischen Umsetzungsfragen zur Gewährleistung des Daten- und Datensicherheitsniveaus auch schwierige datenschutzrechtliche Fragestellungen mit sich.

Querverweise:

9.2.1 Beratungs- und Kontrollpraxis bei Messengerdiensten

8.5 Facebook-Seiten öffentlicher Stellen des Bundes

Im Februar dieses Jahres habe ich das Bundespresseamt (BPA) angewiesen, den Betrieb der Facebook-Seite der Bundesregierung wegen datenschutzrechtlicher Verstöße einzustellen. Das BPA ist meiner Anweisung nicht nachgekommen, sondern klagt dagegen vor dem Verwaltungsgericht Köln.

Letztes Jahr berichtete ich (31. TB Nr. 4.3.1) über die Einleitung eines Verfahrens zur Abhilfe wegen datenschutzrechtlicher Probleme im Zusammenhang mit dem Betrieb der Facebook-Fanpage/-Seite für die Bundesregierung gegen das BPA. Die Stellungnahme des BPA zu meiner Anhörung hat meine Überzeugung nicht ausgeräumt, dass das BPA mit dem Betrieb der Seite gegen das Datenschutzrecht verstößt. Nachdem die Taskforce Facebook-Fanpages der DSK ihr Kurzgutachten anlässlich von Änderungen der Datenschutzrichtlinie und der Nutzungsbedingungen sowie des Einwilligungs-Banners von Facebook überarbeitet hatte,[101] wies ich das BPA im Februar dieses Jahres an, den Betrieb der Facebook-Seite einzustellen.[102]

100 Siehe Beitrag „Messengerdienste und das Recht“, abrufbar unter https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/Messengerdienste.html

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

102 Bescheid vom 17. Februar 2023, abrufbar unter https://www.bfdi.bund.de/dokumente

Das BPA und Meta als Betreiber des sozialen Netzwerks Facebook sind meines Erachtens gemeinsam Verantwortliche für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Betrieb der Facebook-Seite. Dies gilt auch bei deaktivierter Insight-Funktion, mit der Meta den Betreibenden von Seiten Statistiken über die Nutzung bereitstellt. Diese gemeinsame Verantwortlichkeit ergibt sich bereits daraus, dass das BPA mit der Erstellung und dem Betrieb der Facebook-Seite die primäre Ursache setzt, die es Meta erlaubt, personenbezogene Daten der Benutzerinnen und Benutzer der Seite zu erheben. Und zwar unabhängig davon, ob es sich um bei Facebook registrierte Nutzer handelt. Das BPA hat ein eigenes Interesse an der Datenverarbeitung zu Zwecken der Profilerstellung und darauf aufbauend der gezielten Werbeansprache, da dieses Geschäftsmodell von Meta dem BPA eine kostenfreie Nutzung erlaubt. Zudem folgt ein Interesse des BPA daraus, dass es mit der Facebook-Seite durch dieses Geschäftsmodell eine große Anzahl an Nutzenden gezielt ansprechen kann.

Das BPA ist seiner Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO nicht nachgekommen, da es die Einhaltung der Grundsätze des Datenschutzrechts bei Nutzung der Facebook-Seite im Verwaltungsverfahren nicht nachweisen konnte. Zudem hat das BPA gegen § 25 TTDSG verstoßen, indem für auf der Fanpage gesetzte Cookies keine wirksamen, aber erforderlichen Einwilligungen eingeholt wurden. Schließlich hat das BPA personenbezogene Daten der Besucherinnen und Besucher verarbeitet, ohne dass dies nach meiner Auffassung durch eine Rechtsgrundlange erlaubt war. Die gesetzliche und wichtige Aufgabe der Öffentlichkeitsarbeit legitimiert keine Datenverarbeitungen zu Profiling- und Marketingzwecken für sich selbst oder Dritte. Einfach ausgedrückt: Der Zweck heiligt nicht die Mittel.

Das BPA hat gegen den Bescheid fristgerecht Klage vor dem Verwaltungsgericht Köln eingereicht. Die Klage ist derzeit anhängig und hat aufschiebende Wirkung. Das heißt, dass die Wirkung des Bescheides erst einmal aufgeschoben ist, bis die Gerichte abschließend über den Bescheid entschieden haben. Diese aufschiebende Wirkung könnte nur durch die zusätzliche Anordnung der sog. sofortigen Vollziehung verhindert werden. Gegenüber Behörden hat der deutsche Gesetzgeber mir in § 20 Abs. 7 BDSG die Befugnis zur Anordnung der sofortigen Vollziehung jedoch ausdrücklich entzogen. Hierdurch hat sich der Staat im Unterschied zu Unternehmen selbst das Privileg eingeräumt, meine Bescheide auch in eilbedürftigen Fällen für die Dauer eines Gerichtsverfahrens erst einmal nicht umsetzen zu müssen. Dies sehe ich äußerst kritisch. Die Regelung dürfte mit dem Äquivalenz- und Effektivitätsgebot des Unionsrechts kaum zu vereinbaren sein.

Das BPA hat angekündigt, bis zu einer abschließenden Gerichtsentscheidung über meinen Bescheid die Facebook-Seite weiterbetreiben zu wollen.

8.6 Beratungsresistenz der öffentlichen Stellen des Bundes am Beispiel Telemedien

Beratung führt leider nicht immer zum Erfolg.

Seit dem Inkrafttreten des Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) zum 1. Dezember 2021 habe ich die öffentlichen Stellen des Bundes mehrfach über die nunmehr geltende Rechtslage und die konkreten Auswirkungen für Telemedienangebote informiert. Technische Lösungen, wie das Tracking des Surfverhaltens zur Webseitenoptimierung, die nach Datenschutz-Grundverordnung (DSGVO) einwilligungsbefreit sein können, wurden mit dem TTDSG grundsätzlich einwilligungsbedingt. Hierzu hatte die DSK die Orientierungshilfe Telemedien erstellt. Zusätzlich habe ich gemäß meinem Auftrag aus Art. 57 Abs. 1 lit. d) DSGVO Rundschreiben versandt und veröffentlicht, die behördlichen Datenschutzbeauftragen in meinem regelmäßigen Austauschtreffen unterrichtet und zu konkreten Telemedienangeboten Hinweisschreiben an die jeweils zuständigen behördlichen Datenschutzbeauftragten übermittelt. Darüber hinaus wurden mit einzelnen öffentlichen Stellen des Bundes datenschutzrechtliche Mängel bei Telemedienangeboten in Beratungsterminen besprochen und Lösungsalternativen bzw. Schritte zur Behebung der Mängel aufgezeigt.

Trotz dieser umfangreichen Informations- und Beratungsaktivitäten sind einige der beaufsichtigten Stellen meinen Hinweisen nur sehr zögerlich oder unzureichend nachgekommen. Letztlich musste ich leider auch in diesem Jahr weiterhin bereits kommunizierte datenschutzrechtliche Mängel feststellen.

Da die eigenständige Herstellung eines datenschutzkonformen Zustands durch die jeweils Verantwortlichen in naher Zukunft für mich nicht mehr zu erwarten war, musste ich als letztes Mittel meiner Möglichkeiten in einigen Fällen Abhilfemaßnahmen nach Art. 58 Abs. 2 lit. d) DSGVO einleiten.

8.7 Streitbeilegung Facebook/ TikTok

In den diesjährigen Streitbeilegungsverfahren vor dem EDSA ging es insbesondere um Datenübermittlungen von Facebook in die USA, Altersverifikationsmaßnahmen durch TikTok und personalisierte Werbung durch Facebook und Instagram.

Nach Art. 44 DSGVO dürfen personenbezogene Daten in Staaten außerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR) nur unter bestimmten Voraussetzungen übermittelt werden. Drittstaatenübermittlungen sind zulässig, wenn die EU-Kommission in einem Angemessenheitsbeschluss festgestellt hat, dass der betreffende Staat ein angemessenes Datenschutzniveau bietet. Für Fälle in denen kein Angemessenheitsbeschluss vorliegt, sieht Art. 46 Abs. 1 DSGVO vor, dass ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten nur übermitteln darf, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Der EuGH hatte mit dem Schrems II Urteil[103] den US-Angemessenheitsbeschluss, das sogenannte „Privacy Shield", für ungültig erklärt, sodass Datenübermittlungen in die USA (zumindest bis Inkrafttreten des jüngsten Angemessenheitsbeschlusses) nicht auf einen Angemessenheitsbeschluss gestützt werden konnten.

Die irische Datenschutzbehörde stellte in ihrem Beschlussentwurf fest, dass Meta Platforms Ireland Limited (Meta Irland) hinsichtlich des sozialen Netzwerks Facebook die Bedingungen des Kapitels 5 der DSGVO nicht eingehalten hatte und die Datenübermittlungen in die USA rechtswidrig erfolgten. Meta Irland könne sich für die Drittlandübermittlungen mangels hinreichender zusätzlicher Maßnahmen nicht zulässigerweise auf die Standardvertragsklauseln stützen und es greife keine Ausnahme des Art. 49 DSGVO für die regelmäßigen Übermittlungen seitens Facebook. Der Entwurf enthielt weder ein Bußgeld gegenüber Meta Irland noch eine Entscheidung über die Zulässigkeit der Weiterverarbeitung bereits übermittelter Daten.

Die deutschen Aufsichtsbehörden forderten in dem Einspruch die Verhängung eines wirksamen, verhältnismäßigen und abschreckenden Bußgeldes gegen Meta Irland sowie den Erlass einer Anweisung gegenüber der Meta Irland, die Verarbeitung personenbezogener Daten europäischer Nutzender, die seit dem Schrems II-Urteil (Juli 2020) an Meta Platforms, Inc. in die USA übermittelt wurden, zu unterlassen. Beide Forderungen konnten in den Beratungen durchgesetzt werden.

Die irische Datenschutzbehörde verhängte daraufhin gegenüber Meta Irland das bislang höchste Bußgeld von 1,2 Milliarden Euro und wies Meta Irland an, seine Datenverarbeitungsvorgänge in Einklang mit der DSGVO zu bringen, indem es die unrechtmäßige Verarbeitung, auch die Speicherung, personenbezogener Daten von EEA-Nutzenden in den USA unterlässt.

Meta Ireland hat gegen den Beschluss der irischen Datenschutzbehörde vor dem irischen High Court und gegen den Beschluss des EDSA vor dem Gericht der Europäischen Union Klage eingereicht. Die Verfahren sind weiterhin anhängig.

In einem weiteren Verfahren ging es um die datenschutzrechtliche Bewertung des sozialen Netzwerks TikTok Technology Limited (TikTok Irland) mit Bezug auf Minderjährige. Die irische Datenschutzbehörde hatte in ihrem Beschlussentwurf mehrere Verstöße festgestellt. Im Einzelnen stellte sie fest, dass TikTok Irland gegen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO), gegen den Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO) und gegen Transparenzpflichten bezüglich des Anführens von Empfänger(kategorien) (Art. 13 Abs. 1 lit. e) DSGVO) verstoßen habe sowie, dass TikTok Irland dem Risiko für unter 13-jährige Nutzer nicht hinreichend Rechnung getragen habe (Art. 24 Abs. 1 DSGVO) und keine hinreichenden Maßnahmen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen getroffen habe (Art. 25 Abs. 1 und 2 DSGVO). Der Beschlussentwurf gegenüber TikTok Irland sah ein Bußgeld, eine Verwarnung und die Anordnung vor, Verstöße innerhalb von drei Monaten in Einklang mit der DSGVO zu bringen.

Die deutschen Aufsichtsbehörden forderten in ihrem Einspruch die Feststellung eines zusätzlichen Verstoßes gegen den Grundsatz von Treu und Glauben des Art. 5 Abs. 1 lit. a) DSGVO in Form sogenannter irreführender Designmuster[104] bei der Registrierung auf der Plattform und beim Posten von Videos. Die italienische Datenschutzbehörde forderte die zusätzliche Feststellung

103 „Schrems II" Urteil des EuGH vom 16. Juli 2020, Rechtssache C-311/18, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=40595668

104 Siehe dazu EDSA, Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

eines Verstoßes gegen Art. 25 DSGVO wegen unzureichender Altersverifikationsmaßnahmen.

Der deutsche Einspruch fand (mit Ausnahme eines zusätzlichen Bußgelds) Eingang in den verbindlichen Beschlussentwurf des EDSA. Es wurde festgestellt, dass TikTok Irland Minderjährige in unzulässiger Weise dazu bewegt hatte, ihre Profile und Videos „öffentlich zu stellen", d. h. auch für nicht registrierte Nutzende des Netzwerks zugänglich zu machen. Hinsichtlich des italienischen Einspruchs entschied der EDSA, dass keine ausreichenden Informationen vorlagen, um einen Verstoß gegen Art. 25 DSGVO festzustellen, weil nicht ermittelt werden konnte, welche konkreten, effektiveren (und gleichwohl selbst datensparsamen) Altersverifikationsmaßnahmen für TikTok Irland im Prüfungszeitraum Juli bis Dezember 2020 zur Verfügung standen. In dem finalen Beschluss stellte die irische Aufsichtsbehörde die oben genannten Verstöße fest und verhängte gegen TikTok Irland ein Bußgeld in Höhe von 345 Mio. Euro. TikTok Irland möchte den Beschluss der irischen Datenschutzbehörde vor dem irischen High Court gerichtlich überprüfen lassen.

Im Dringlichkeitsverfahren betreffend Facebook und Instagram befasste sich der EDSA erneut mit der Zulässigkeit verhaltensbezogener Werbung auf sozialen Netzwerken. Bereits in den verbindlichen Beschlüssen des 2/2022 u. 3/2022 vom 5. Dezember 2022 (31. TB Nr. 3.3.1) hatte der EDSA festgestellt, dass Art. 6 Abs. 1 lit. b) DSGVO (vertragliche Erforderlichkeit) keine taugliche Rechtsgrundlage für verhaltensbezogene Werbung darstelle. Die irische Datenschutzbehörde wies Meta Irland daraufhin an, den Verstoß gegen Art. 6 Abs. 1 DSGVO einzustellen. Meta Irland stützte die Datenverarbeitung zum Zwecke verhaltensbezogener Werbung daraufhin aber teilweise weiter auf Art. 6 Abs. 1 lit. b) DSGVO und überwiegend auf Art. 6 Abs. 1 lit. f) DSGVO (berechtigtes Interesse). In der Zwischenzeit bestätigte der EuGH eine Entscheidung des Bundeskartellamts,[105] wonach auch Art. 6 Abs. 1 lit. f) DSGVO keine taugliche Rechtsgrundlage für verhaltensbezogene Werbung ist. Nachdem Meta Irland der einstweiligen Anordnung der norwegischen Aufsichtsbehörde, verhaltensbezogene Werbung auf diesen Grundlagen einzustellen, nicht nachkam, beantragte diese bei dem EDSA einen Dringlichkeitsbeschluss. Dem Antrag folgend wies der EDSA die irische Aufsichtsbehörde an, Meta Irland endgültig und bezogen auf den ganzen Europäischen Wirtschaftsraum zu untersagen, persönliche Daten zur verhaltensbezogenen Werbung gestützt auf Art. 6 Abs. 1 lit. b) oder lit. f) DSGVO zu verarbeiten.

Querverweise:

3.5 EU-U.S. Data Privacy Framework – „Privacy Shield"-Nachfolge, 4.2.7 Streitbeilegungsverfahren im EDSA

8.8 Corona Warn App

Die Corona Warn App – Ein gelungener Abschluss.

Die Corona Warn App (CWA) gilt als eine der wichtigsten und erfolgreichsten Apps im Kampf gegen das Corona Virus. Zwar war die Entwicklung und die damit für mich verbundene, oftmals in hoher Schlagzahl und unter erheblichem Ressourceneinsatz erforderliche Beratung, nicht immer einfach. Doch rückblickend betrachtetet war dies ein sinnvolles Investment in ein sehr wirkungsvolles Werkzeug zur Pandemiebekämpfung.

Gleich zu Beginn galt es eine Abwägung zwischen zentralem und dezentralem Modell zu treffen. Dank internationaler Unterstützung von vielen Individuen und Gruppen, die sich intensiv mit den einzelnen Optionen, Vorteilen und Nachteilen dieser unterschiedlichen Methoden auseinandergesetzt und viel wegweisende Arbeit geleistet haben, hat man sich für eine dezentrale Architektur entschieden.

Neben der Festlegung und Anpassung der richtigen Parameter für die Kontaktverfolgung wurden nach und nach weitere Funktionen in die Anwendung aufgenommen, die stets ihre eigenen Fragestellungen und Herausforderungen für den Datenschutz mit sich brachten. Das umfasste Funktionen wie beispielsweise das Abrufen von Testergebnissen, die Speicherung von eigenen und fremden Impfzertifikaten, das Absetzen von Warnungen, die Aufnahme eines Kontakttagebuchs, optionale Nutzendenauswertungen oder Eventregistrierungen. Dabei mussten jedes Mal die Einführung der jeweiligen Funktion und die damit einhergehenden Risiken mit dem möglichen Nutzen aus datenschutzrechtlicher Sicht schnell und ohne Verzug in Einklang gebracht werden. Nicht zuletzt galt, es Gefahren zu verhindern und dafür zu sorgen, trotz gebotener Eile, Vorsicht und maßvolle Entwicklung nicht aus den Augen zu verlieren.

Nach fast drei Jahren wurde die CWA zum 1. Juni 2023 laut Bundesministerium für Gesundheit (BMG) in den Ruhemodus versetzt. Dem bisher guten Verlauf dieses Großprojektes folgend habe ich dieses Jahr eine Kon-

105 EuGH Urteil vom 04. Juli 2023, Az. C252/21

trolle bei einem der Dienstleister der App durchgeführt, um das ordnungsgemäße Einstellen des Betriebes zu kontrollieren und um zu überprüfen, ob die Systeme ordentlich zugedeckt wurden. Dabei habe ich zunächst festgestellt, dass die CWA entgegen der öffentlichen Verlautbarung des BMG nicht in einen Ruhemodus (Schlafmodus) versetzt, sondern eingestellt wurde. Bei meiner Kontrolle der damit einhergehenden vollständigen Löschung der Systeme und Daten, habe ich eine sehr gute Dokumentation des Prozesses und der Nachweisführung feststellen können, die keine datenschutzrechtlichen Mängel aufwies.

Es bleibt zu hoffen, dass die CWA diesen Zustand niemals wieder verlassen muss.

8.9 Authentifizierung im Bereich Telekommunikation

Eine sichere Kunden-Authentifikation spielt in vielen Wirtschaftsbereichen eine wichtige Rolle. Besonders brisant wird diese Frage im Telekommunikationsmarkt. Denn hier gibt es viele Geschäftsvorgänge mit schützenswerten Daten des privaten Lebens und finanziellen Risiken. Klar ist: Es bedarf risikoangepasster und praktisch umsetzbarer Lösungen, um eine sichere Authentifizierung zu realisieren. Welche Risiken bestehen und welche Parameter hierbei zu bedenken sind, habe ich in einem Arbeitspapier zusammengefasst.

Nach Art. 32 DSGVO sind verantwortliche Stellen dazu verpflichtet, zum Schutz von Kundendaten angemessene technische und organisatorische Maßnahmen umzusetzen. Ausgangspunkt der Überlegungen ist damit immer auch die Frage, welchen Geschäftsprozessen welche datenschutzrechtlichen Risiken innewohnen.

Näheres finden Sie im Arbeitspapier zur Authentifizierung im Bereich Telekommunikation

(QR-Code klicken oder scannen)

Die Bewertung der datenschutzrechtlichen Risiken ist komplex und variantenreich, mit Blick auf die Risiken und mögliche Schutzmaßnahmen. So hängen die Anforderungen an eine sichere Kunden-Authentifizierung maßgeblich davon ab, ob der Kunde im Shop vor Ort ist, es sich um einen Call-Center-Kontakt handelt oder die Interaktion mittels eines Online-Zugangs erfolgt.

Angemessener Schutz setzt eine Risikoanalyse voraus

Betrachtet man zunächst die datenschutzrechtlichen Risiken einer Kundeninteraktion im Telekommunikationsmarkt, so stellen sie sich holzschnittartig wie folgt dar:

Recht augenfällig ist (auch) im Telekommunikationsmarkt datenschutzrechtlich problematisch, wenn Unberechtigten personenbezogene Daten preisgegeben werden. Beispielsweise bei Stalking-Fällen, wenn eine unberechtigte Person an eine Adresse oder eine Telefonnummer gelangt, die geheim bleiben sollte. Das Risiko kann im Einzelfall sehr groß sein, etwa, wenn politisch engagierte Menschen ins Visier von Extremisten geraten und dadurch möglicherweise ihr Leben bedroht wird. Möglich sind aber auch familiäre Konstellationen, wenn Personen von ihrem Ex-Partner, ihrer Ex-Partnerin oder von deren Familie bedroht werden und möglicherweise Opfer eines Gewaltverbrechens werden können. Auch wenn durch Vertragsänderungen Vermögensschäden drohen, ist die Risikolage klar. Zu denken ist hier an Vertragsverlängerungen mit dem Ziel, ein neues Handy an der eigentlich berechtigten Person vorbei zu erlangen oder aber Fälle, in denen ein neuer Vertrag über eine Kontonummer einer anderen Person abgewickelt werden soll.

Andere Risiken zeigen sich aber erst auf den zweiten Blick. Dies gilt etwa für den Identitätsdiebstahl als mittelbares, aber ganz erhebliches Risiko. Klar wird dies, wenn man sich vor Augen führt, dass E-Mail-Adressen und Mobilfunknummern oft als Sicherheitsanker für andere digitale Dienste genutzt werden. Wenn es Betrügerinnen oder Betrügern gelingt, sich eine neue SIM-Karte für einen bestehenden Mobilfunkvertrag ausstellen zu lassen, ist es damit oft möglich, sich unerlaubt Zugang zu Betroffenen-Accounts von Diensten mit hohen monetären Risiken zu verschaffen (etwa Paypal- oder auch Bitcoin-Konten). Diese Risiken liegen zwar außerhalb des Einflussbereichs des Telekommunikationsanbieters, sind aus meiner Sicht dennoch mit in seine Risikobetrachtung einzubeziehen.

Verantwortliche Stellen müssen geeignete Sicherungsmechanismen etablieren

Wie dargelegt, gibt es bei Telekommunikationsunternehmen für Kundinnen und Kunden die typischen Zugangswege des Callcenters, der Shops und durch Online-Accounts. Bei allen Wegen manifestieren sich besondere Vorteile, aber auch Risiken, die jeweils für

die Wahl einer geeigneten Authentifikationsmethode zu beachten sind.

Gerade wenn der Kunde nicht selbst vor Ort im Shop ist, stellt sich die Frage, wie geeignete Sicherheitsmechanismen aussehen können. Die bisherigen Untersuchungen haben ergeben, dass ein Passwort, eine PIN oder ein anderes sicheres Verfahren hier der Regelfall für eine Authentifikation sein muss. Andere Möglichkeiten, wie die Abfrage von bestimmten Kriterien zum Beispiel Kundennummer, Vertragsnummer oder ähnliches kommen nur als Rückfall-Option in Betracht.

Insbesondere bei der Ausstellung von Ersatz-SIM-Karten ist wegen des erhöhten Gefährdungspotentials auf eine besonders sichere Authentifikation zu achten. Je nach Ausgestaltung der Standardprozesse können hierbei zusätzliche Sicherungsmechanismen erforderlich werden.

8.10 Von TrustPID zu Utiq

Das Pilotprojekt eines Joint-ventures zu personalisierter Werbung im Internet ist unter neuem Namen in den Regelbetrieb übergegangen.

Permission for BfDI to use cartoon in print/electronic.

In meinem 31. Tätigkeitsbericht (Nr. 8.11) habe ich bereits über das Projekt „TrustPID“ berichtet. Es handelte sich um einen Machbarkeitstest zur Wiedererkennung von Mobilfunk-Nutzenden auf Webseiten. Dabei werden die IP-Adressen und die Mobilfunknummern der Nutzenden verwendet, um eine pseudonyme Kennung zu generieren. Ziel ist das Ausspielen pseudonymisierter personalisierter Werbung ohne Drittanbieter-Cookies. Rechtliche Basis der Datenverarbeitung ist eine datenschutzrechtliche Einwilligung der Nutzenden, die von den Webseitenbetreibenden eingeholt wird.

Der Pilotbetrieb von TrustPID in Deutschland wurde im Mai 2023 eingestellt. Mit der europäischen Umsetzung der Projektidee beschäftigt sich nun ein neues Unternehmen namens Utiq aus Brüssel. Für dieses Unternehmen ist die belgische Datenschutzaufsichtsbehörde (APD) zuständig. Ich bin weiterhin allein für die Beteiligung der deutschen Mobilfunkanbieter zuständig. Auch zukünftig werde ich das Thema eng u. a. mit der APD begleiten und mich auf europäischer Ebene für eine datenschutzfreundliche Umsetzung einsetzen.

8.11 Kindergrundsicherung

Mit der Kindergrundsicherung ist auch die Einführung digitaler Verfahren geplant, mit denen in bislang nicht gekanntem Umfang bei verschiedenen Stellen bereits vorliegende sensible Daten ohne Zutun der Betroffenen verarbeitet werden. Den Ansatz, durch digitale und unbürokratische Verfahren den Bezug der Kindergrundsicherung für die Betroffenen zu erleichtern, begrüße ich. Hierbei muss auf die Einhaltung datenschutzrechtlicher Standards und eine umfassende Transparenz geachtet werden. Der Gesetzesentwurf wird dem nur zum Teil gerecht.

Die Bundesregierung verfolgt mit der Einführung der Kindergrundsicherung das Ziel, bessere Chancen für Kinder und Jugendliche zu schaffen, mehr Familien und ihre Kinder mit Unterstützungsbedarf zu erreichen sowie Kinderarmut wirksam zu bekämpfen. Neben einem einkommensunabhängigen Kindergarantiebetrag für alle Kinder und Jugendlichen (ehemals Kindergeld nach dem Bundeskindergeldgesetz) soll insbesondere ein einkommensabhängiger und altersgestaffelter Kinderzusatzbetrag (ehemals Kinderzuschlag) eingeführt werden. Die Kindergrundsicherung soll einfach und digital zu beantragen sein. So sollen bis zu 5,6 Millionen Kinder erreicht werden, davon fast zwei Millionen Kinder, die derzeit Bürgergeld beziehen. Bei meiner Prüfung des Gesetzentwurfs habe ich das besondere Gewicht der Zielsetzung berücksichtigt, Kinderarmut wirksam zu bekämpfen, soweit etwa Abwägungsentscheidungen zu treffen waren. Der Gesetzesentwurf zur Einführung einer Kindergrundsicherung enthält in datenschutzrechtlicher Sicht einige relevante Neuerungen. So sollen (teil-)automatisierte Datenabrufe aus verschiedenen Datenquellen, z. B. Steuerdaten oder Sozialversicherungs-

daten, in einem bisher noch nicht gekannten Umfang stattfinden. Außerdem sollen die Leistungsberechtigten so wenige Angaben wie möglich selbstständig erbringen müssen und damit die Leistungserbringung unbürokratischer erfolgen. Die insoweit geplanten Datenübermittlungen bedürfen in jedem Fall ausreichender Rechtsgrundlagen und müssen zudem technisch wie organisatorisch sicher gestaltet werden. Die vorliegend geplante Nutzung von Steuerdaten stellt insbesondere mit Blick auf das zu wahrende Steuergeheimnis eine besondere Herausforderung dar.

Vollständig neu konzipiert wurde der sog. **Kindergrundsicherungs-Check**. Hiernach sollen Daten, die in Behörden bereits in elektronischer Form vorliegen, für die Vorprüfung des Anspruchs auf den Kinderzusatzbetrag verwendet und potentielle Anspruchsberechtigte proaktiv zur Beantragung der Leistung angesprochen werden. Leistungen müssen im Falle der Bedürftigkeit also nicht mehr selbstständig ermittelt und nachgefragt werden, sondern werden aktiv angeboten, wenn die Bürgerinnen und Bürger darin eingewilligt haben. Damit wird im Hinblick auf den Unterstützungsbedarf von Kindern ein Paradigmenwechsel weg vom Prinzip der Holschuld hin zum Prinzip der Bringschuld angestrebt. Bei der Ausarbeitung des Kindergrundsicherungs-Checks wurde ich in erfreulicher Weise frühzeitig beteiligt. So konnten einige datenschutzrechtliche Probleme bereits im Vorfeld ausgeräumt werden. Ich begrüße, dass der Kindergrundsicherungs-Check nach dem Regierungsentwurf mit dem ausdrücklich erklärten Einverständnis der von der Datenerhebung Betroffenen erfolgen soll, und nicht, wie ursprünglich diskutiert, durch eine antragslose massenhafte Datenverarbeitung ohne Zustimmung oder Kenntnis der betroffenen Personen, von denen am Ende nur eine Minderheit tatsächlich Anspruch auf den Kinderzusatzbetrag hat. Es erfolgt außerdem eine umfangreiche Information im Vorfeld, auf welche Datenquellen zugegriffen werden kann. Die Betroffenen werden regelmäßig und transparent über die Ergebnisse des Checks informiert.

Im eigentlichen **Antragsverfahren** muss nach den Ausführungen in der Gesetzesbegründung davon ausgegangen werden, dass Nachweise zu Einkommen der Familiengemeinschaft im Regelfall ohne Mitwirkung der von der Datenverarbeitung betroffenen Personen entweder automatisiert über die DRV Bund abgerufen oder in Papierform unmittelbar bei den Arbeitgebern der Mitglieder der Familiengemeinschaft eingeholt werden sollen. Dagegen habe ich Bedenken. Die zwingende Offenbarung des Bezugs von existenzsichernden Sozialleistungen gegenüber den Arbeitgebern könnte Leistungsberechtige davon abhalten, einen Antrag auf den Kinderzusatzbetrag zu stellen, was der erklärten Zielsetzung des Gesetzes zuwiderlaufen würde. Aus den bei mir eingehenden Beschwerden ist mir bekannt, dass einige Bezieher von Sozialleistungen nicht wollen, dass ihre Arbeitgeber vom Bezug von bedürftigkeitsabhängigen Sozialleistungen, etwa „aufstockende SGB II-Leistungen“, wissen. Sie befürchten – ob berechtigt oder nicht – eine Stigmatisierung. Gleiches gilt für das unmittelbare Anfordern einer papiergebundenen Einkommensbescheinigung durch den Familienservice beim Arbeitgeber. Es sollte sichergestellt werden, dass Betroffene, die nicht wollen, dass ihre Arbeitgeber von der Bedürftigkeit ihrer Familie erfahren, gleichwohl den einkommensabhängigen Kinderzusatzbetrag beantragen können, vorzugsweise durch ein Widerspruchsrecht der Betroffenen („opt out“) gegen die Datenerhebung beim Arbeitgeber und die Möglichkeit, die erforderlichen Nachweise selbst beizubringen.

Den vorgesehenen digitalen Datenaustausch zwischen Behörden der Sozialverwaltung halte ich hingegen für vertretbar. Dies gilt auch für die damit verbundene Abkehr von dem Grundsatz der Direkterhebung beim Betroffenen. Hierbei muss das besondere Gewicht des Ziels, Kinderarmut wirksam zu bekämpfen, berücksichtigt werden. Dieser Datenaustausch steht im Einklang mit dem im Rahmen der Verwaltungsdigitalisierung insgesamt verfolgten „Once-Only-Prinzip“. Danach sollen Daten nur einmal bei den betroffenen Personen selbst erhoben werden und danach für mehrere Zwecke verwendet werden können. Hierbei müssen in besonderer Weise Transparenz, Kontrolle und strukturelle Hemmnisse der Zusammenführbarkeit mit anderen Mitteln gleichsam effektiv gewährleistet werden.

Problematisch ist jedoch in der vorgesehenen Form **die Verarbeitung der sog. Steuer-Identifikationsnummer** (Steuer-ID). Sie führt dazu, dass eine Behörde außerhalb der Steuerverwaltung – die Kindergrundsicherung soll zum besonderen Teil des Sozialgesetzbuchs gehören – die Steuer-ID ohne die Sicherungen aus dem Identifikationsnummerngesetz (IDNrG) und dem Onlinezugangsgesetz (OZG) verarbeiten darf. Dies ist nicht akzeptabel. Hier ist eine ausdrückliche Regelung zur Nutzung der Steuer-ID als Identifikationsnummer nach dem IDNrG unter Anerkennung der Schutzmechanismen des IDNrG sowie des OZG vorzusehen. Dazu gehört unter anderem die Anwendung des 4-Corner-Modells und des Datenschutzcockpits.

Querverweise:

8.2 Registermodernisierung

8.12 Beratung des RKI

Das Robert Koch-Institut (RKI) hat auch in diesem Berichtsjahr die Verantwortung für neue relevante Digitalisierungsprojekte für die öffentliche Gesundheit übernommen und mich um Beratung hierzu gebeten. Diese frühzeitige Information und Einbindung auch zum geplanten Forschungspanel ist ein positives Beispiel für konstruktive Zusammenarbeit, denn sie erleichtert die Berücksichtigung datenschutzrechtlicher Aspekte.

Im Berichtsjahr habe ich das RKI zu AGORA, einer Plattform für den Austausch von Gesundheitsämtern, beraten. Ich habe empfohlen über diese Plattform nur allgemein gefasste Informationen auszutauschen und Fälle nur in grundsätzlicher Form zu besprechen. Das bedeutet, dass auf die Verarbeitung fall- bzw. personenbezogener Daten verzichtet werden soll, die andernfalls Schutzmaßnahmen und zusätzliche Anforderungen bei Auftragungsverarbeitung erforderlich gemacht hätten. Für den Austausch von Falldaten kann, soweit erforderlich, auf DEMIS (Deutsches elektronisches Melde- und Informationssystem für Infektionskrankheiten) zurückgegriffen werden. Auf diese Weise würden bei AGORA ausschließlich dienstliche personenbezogene Daten erfasst.

Das RKI beabsichtigt, DEMIS weiter auszubauen, das nach einer langen Planungsphase seit 2013 zuletzt aufgrund der Erfordernisse der Pandemiebewältigung in grundlegenden Funktionalitäten technisch umgesetzt worden war. Hier werden weitere Stellen angebunden, die Meldungen über Infektionen und Ausbrüche abgeben oder empfangen. Wesentlich ist der Nachweis von Identität und Berechtigung, der je nach Art der Stelle unterschiedlich vorgesehen ist, um missbräuchliche Meldungen oder Abrufe zu verhindern. Krankenhäuser beispielsweise weisen sich über den „Authenticator“ der Telematik-Infrastruktur aus. Für meldepflichtige Einrichtungen, die nur selten den Ausbruch einer meldepflichtigen Infektion mitteilen müssen und die keinen eigene Berechtigung zum Zugang zu DEMIS haben, ist ein Portal auf Grundlage des Onlinezugangsgesetz (OZG) geplant, um die Identität der Einrichtung und der meldenden Person nachzuweisen und zu dokumentieren. Außerdem muss eine wirksame Pseudonymisierung und Verschlüsselung gewährleistet werden.

Aktuell ist geplant, zusätzliche Module zu integrieren und bundesweit für den öffentlichen Gesundheitsdienst zur Verfügung zu stellen. Ich begrüße die frühzeitige Information zum Planungsstand, da ich so Hinweise geben kann. Bei der Vielzahl der Beteiligten auf Bundes-, Landes- und kommunaler Ebene kommt es besonders auf die Klärung der Verantwortlichkeiten und die Steuerung über Berechtigungen und deren Nachweis an.

Das RKI hat außerdem die Planungen zum Aufbau eines weiteren Forschungspanels vorgestellt. Dabei werden aufgrund von repräsentativ ausgewählten Meldedaten mögliche Teilnehmerinnen und Teilnehmer angeschrieben, die sich dann bei Interesse für das Panel registrieren können. Diese erhalten in der Folge weitere Fragen. Daneben können sich weitere Interessierte aktiv für das Panel registrieren und an den Forschungsbefragungen teilnehmen. Die bei den Befragungen erhobenen Daten werden getrennt von den personenidentifizierenden Daten gespeichert. Diesbezüglich habe ich mich dafür ausgesprochen, nach Möglichkeit eine unabhängige Vertrauensstelle zu integrieren. Thema waren auch die Gewährleistung der Betroffenenrechte, z. B. auf Auskunft, einerseits sowie eine frühe Löschung der Erhebungsdaten oder die dauerhafte und irreversible Pseudonymisierung als Schutz vor Reidentifikation andererseits. Dabei ist dafür Sorge zu tragen, dass die Erhebungsdaten nicht selbst einen Rückschluss auf die Person zulassen. Das Panel ist ein positives Beispiel für einwilligungsbasierte Forschung, die einerseits durch eine repräsentative ausgewählte Gruppe ausgewogen und aussagekräftig ist, andererseits für alle Interessierten zur Teilnahme und Unterstützung dieser Forschung offensteht.

8.13 Sicherheitsvorfälle bei BITMARCK

Um den Anforderungen an zeitgemäße Arbeitsabläufe gerecht zu werden, digitalisieren gesetzliche Krankenkassen zunehmend ihre Prozesse. Die BITMARCK ist als eine Arbeitsgemeinschaft Dienstleister für eine Vielzahl gesetzlicher Krankenkassen im Bereich der Informationstechnologie. Zwei IT-Sicherheitsvorfälle haben jedoch gezeigt, dass so auch ein Single-Point-of-Failure entstehen kann.

Die BITMARCK Holding GmbH ist ein Dienstleister von Sozialversicherungsträgern gem. § 94 Abs. 1a Satz 1 SGB X (Arbeitsgemeinschaft), § 219 SGB V mit ausschließlicher Beteiligung von Krankenkassen(-verbänden). Sie unterliegt der staatlichen Aufsicht durch das Bundesamt für Soziale Sicherung und meiner datenschutzrechtlichen Aufsicht. Unterteilt in fünf Business-Units ist der Unternehmenszweck die „Entwicklung, Wartung, Überlassung und Betreuung von Informationssystemen in der gesetzlichen Krankenversicherung. So ver- und betreibt die BITMARCK Software für Krankenkassen, wie beispielsweise die GKV-Branchenlösung „BITMARCK_21c“, bietet Rechenzentrumsleistungen

sowie Leistungen aus den Bereichen Beratung und Service an. Zu den Kunden der BITMARCK zählen rund 80 gesetzliche Krankenkassen.

Zugriff über Login-Daten

Im Januar 2023 war es Unbekannten gelungen, mit den rechtswidrig angeeigneten Login-Daten eines Mitarbeitenden der BITMARCK rund 350.000 Datensätze (Name, Vorname, Geburtsdatum, Krankenversichertennummer und Seriennummer der elektronischen Gesundheitskarte) von Versicherten einzelner Mitgliedskassen zu entwenden und diese im Internet zum Kauf anzubieten. Dies war nur möglich, da die betreffenden Daten in Systemen (Projektmanagementtools) gespeichert und verarbeitet wurden, die mangels adäquater Sicherheiten nicht für die Verarbeitung von personenbezogenen Daten geeignet sind. Zudem waren diese Systeme nur durch Nutzername und Passwort geschützt. Eine Zwei-Faktor-Authentisierung hätte den Angriff aller Voraussicht nach verhindert.

Mittlerweile hat mir die BITMARCK versichert, alle personenbezogenen Daten aus den unsicheren Projektmanagementtools entfernt und ihre technischen und organisatorischen Maßnahmen (insb. Einführung der Zwei-Faktor-Authentisierung) angepasst zu haben. Die Prüfung und Durchsetzung aufsichtsrechtlicher Maßnahmen habe ich in diesem Fall noch nicht abgeschlossen.

Kompromittierung der Domaincontroller

Im April 2023 erreichte eine maliziöse E-Mail die Systeme der BITMARCK. Aufgrund dieser E-Mail wurde der Domaincontroller eines Rechenzentrums der BITMARCK kompromittiert. Mittels dieses Domaincontrollers hat ein Angreifer umfangreiche Rechte erlangt, die zur Ausbreitung im firmeninternen Netzwerk hätten genutzt werden können. Der Angriff konnte jedoch frühzeitig erkannt werden, sodass das Rechenzentrum kontrolliert vom Netz genommen werden konnte. Eine Folge dessen war, dass eine Vielzahl der Krankenkassen über unterschiedlich lange Zeiträume teilweise nur sehr eingeschränkt arbeitsfähig war.

Im Rahmen der Aufarbeitung dieses Sachverhaltes wurde deutlich, dass es der BITMARCK durch zeitnahe, aufwändige und zugleich auch effektive Gegenmaßnahmen gelungen ist, die Gefahren einzudämmen und größere Schäden zu verhindern. Ein konkreter Verstoß gegen datenschutzrechtliche Vorgaben kann in diesem zweiten Vorfall aus April 2023 weder der BITMARCK noch den auftraggebenden Krankenkassen vorgeworfen werden. Dennoch zeigt der Vorfall die Verwundbarkeit der IT-Infrastruktur – insbesondere bei gebündelten Abhängigkeiten verschiedener Verantwortlicher von einem Dienstleister.

8.14 Implantateregister

In diesem Berichtsjahr hat das Implantateregister (IRD) den Probebetrieb mit ersten Echtdaten aufgenommen. Ab Januar 2024 werden planmäßig im Regelbetrieb zunächst alle Brustimplantate an das Register gemeldet. Vor Betriebsbeginn habe ich das nötige Einvernehmen zum Pseudonymisierungsverfahren und zur Verschlüsselungstechnik gegeben und zu verschiedenen Einzelfragen beraten.

Mit dem EIRD[106] wurde das Implantateregistergesetz (IRegG) als Grundlage für das deutsche Implantateregister (IRD) geschaffen. Es handelt sich um das erste bundesweite Register mit Meldepflicht für die Gesundheitseinrichtungen und Teilnahmepflicht für die Patientinnen und Patienten (28. TB Nr. 4.2.2, 29. TB Nr. 7.3).

Die Betroffenenrechte auf Einschränkung der Verarbeitung und Widerspruch wurden in § 26 IRegG ausgeschlossen. Begründet wird dies mit dem Erfordernis der Vollständigkeit für eine wirksame Produktüberwachung/Pharmakovigilanz. Den ursprünglich vorgesehenen Ausschluss aller Betroffenenrechte hatte nicht nur ich heftig kritisiert.

Das Register soll sukzessive verschiedene Implantattypen erfassen, beginnend mit Brustimplantaten, und die Daten aus bestehenden einwilligungsbasierten Registern (Endoprothesenregister, Aortenklappenregister) integrieren. Es wird mit enormen Fallzahlen gerechnet, allein aus dem Bereich Endoprothesen jährlich mit ca. 500.000 Meldungen. Die für die jeweiligen Implantattypen vorgesehenen Datenkränze werden kleinteilig und umfangreiche medizinische Angaben auch aus Vorgeschichte und Nachsorge beinhalten (Anlage 2 zur IRegBV: Alter, Größe, Gewicht, allgemeiner Gesundheitszustand, diverse Diagnosen u. v. m.). Die Daten sollen zur Nutzung für fachliche Zwecke durch das BfArM sowie für wissenschaftliche Forschung zugänglich sein (§§ 27–31 IRegG).

Leider ist die Registerstelle noch immer provisorisch bei einer Projektgruppe im Bundesministerium für Gesundheit (BMG) selbst angesiedelt. Gerade bei einem Register, das eine enorme Fallzahl umfassen wird und jeweils

106 Implantateregister-Errichtungsgesetz vom 12. Dezember 2019, BGBl 2019, 2494 Gesetzentwurf BT-Drs 19/10523

hoch sensible Daten beinhaltet, sollte die Aufgabe der Registerstelle unbedingt sachgerecht und unabhängig wahrgenommen werden.

Bei den Beratungen war zu berücksichtigen, dass das IRD u. a. für Produktwarnungen, aber auch bei möglichen Fehlern/Implausibilitäten einen „Rückweg" zu den meldenden Gesundheitseinrichtungen benötigt. In der Abstimmung habe ich darauf hingewirkt, dass dieser aus datenschutzrechtlichen Gründen nicht direkt (unter Verwendung einer Fall-ID aus der Gesundheitseinrichtung), sondern immer nur über die Vertrauensstelle anzulegen ist. Die Fall-ID wird, wie im Gesetz vorgesehen, bei der Zulieferung pseudonymisiert und für einen Rück-Kontakt zur Gesundheitseinrichtung de-pseudonymisiert. Zudem speichert die Vertrauensstelle beim RKI die Krankenversichertennummer der Patienten zu den generierten Pseudonymen, um bei Bedarf (§ 9 Abs. 5 IRegG) eine De-Pseudonymisierung zu ermöglichen, u. a. um bei den Krankenkassen in Einzelfällen den Vitalstatus abzufragen oder um Sicherheitskorrekturmaßnahmen vorzunehmen.

Im Berichtsjahr habe ich auf Antrag des RKI das nötige Einvernehmen zum Pseudonymisierungskonzept und zum Verschlüsselungskonzept erteilt. Alle Pseudonyme werden nach demselben zufallsbasierten Verfahren ohne rechnerische Verbindung zu Fachdaten erzeugt. Die Pseudonyme werden mittels Zufallszahl erzeugt, die eine Länge von 32 Byte hat. Dabei ist entscheidend, dass diese Zufallszahl kryptografisch sicher erzeugt wird. Die eingesetzten kryptografischen Verfahren sind BSI-konform. Vor dem Beginn des Probebetriebs mit Echtdaten aus einzelnen Gesundheitseinrichtungen habe ich auch das Datenschutzkonzept und die Datenschutzfolgenabschätzung geprüft. Besonderes Augenmerk habe ich dabei auf die Berechtigungen der eingebundenen Auftragsverarbeiter gelegt.

In Anbetracht der unmittelbar bevorstehenden Aufnahme des Regelbetriebs empfehle ich der Bundesregierung, endlich eine unabhängige Registerstelle für das Implantateregister zu schaffen.

8.15 Gutachterliche Stellungnahmen in Verfahren der Berufsgenossenschaften

Teilweise haben Unfallversicherungsträger im Rahmen der Beauftragung von beratenden Ärztinnen und Ärzten personenbezogene Gesundheitsdaten ohne Rechtsgrundlage übermittelt. Mit einem Informationsschreiben an den Spitzenverband der gewerblichen Berufsgenossenschaften und der Unfallkassen (DGUV) habe ich auf den geänderten Übermittlungsbegriff hinwiesen und in einem Kriterienkatalog dargestellt, wann bei der Weiterleitung von personenbezogenen Daten an beratende Ärztinnen und Ärzte von einer Übermittlung i. S. d. DSGVO auszugehen ist.

In meiner Aufsichtspraxis habe ich festgestellt, dass meiner Aufsicht unterstehende Unfallversicherungsträger das Vorliegen einer Übermittlung i. S. d. DSGVO vielfach noch nach dem früheren Übermittlungsbegriff beurteilt haben. Dies hat sich darin gezeigt, dass sie zur Durchführung gutachtlicher Stellungnahmen personenbezogene Gesundheitsdaten an sogenannte beratende Ärztinnen und Ärzte übermittelt haben, ohne dass die betroffenen Versicherten hierin eingewilligt oder andere Rechtfertigungsgründe für die Übermittlung vorgelegen haben. Als Begründung haben Unfallversicherungsträger regelmäßig auf die Unterscheidung zwischen einem Gutachtenauftrag nach 200 Abs. 2 SGB VII und einer beratungsärztlichen Stellungnahme Bezug genommen. In diesem Zusammenhang haben sie die Auffassung vertreten, dass aus dem Nichtvorliegen eines Gutachtenauftrags i. S. d. § 200 Abs. 2 SGB VII auf das Fehlen einer Übermittlung nach Art. 4 Nr. 2 DSGVO geschlossen werden könne. Dies ist unter Zugrundelegung des neuen Übermittlungsbegriffs nach der DSGVO nicht mehr haltbar. Tatsächlich liegt eine Übermittlung gemäß Art. 4 Nr. 2 DSGVO bereits dann vor, wenn personenbezogene Daten gezielt an einen Empfänger i. S. d. Art. 4 Nr. 9 DSGVO weitergeleitet werden. Dies kann durchaus auch dann der Fall sein, wenn Unfallversicherungsträger personenbezogene Gesundheitsdaten von Versicherten an beratende Ärztinnen und Ärzte weiterleiten, auch wenn diese kein Gutachten nach § 200 Abs. 2 SGB VII erstellen, sondern „nur" eine beratungsärztliche Stellungnahme abgeben.

Ich habe daraufhin ein Informationsschreiben an die DGUV versandt, in dem ich den Übermittlungsbegriff nochmals eingehend erläutert habe. Außerdem habe ich in dem Informationsschreiben einen Kriterienkatalog aufgestellt, den Unfallversicherungsträger als Richtschnur für die Feststellung des Vorliegens einer Übermittlung im Fall einer Weiterleitung von personenbezogenen Daten an beratende Ärztinnen und Ärzte sowie sonstige gutachtlich Stellung nehmende Personen heranziehen können.

Die DGUV hat die Unfallversicherungsträger über mein Schreiben informiert und es außerdem auf seinem Internetportal veröffentlicht. Aus schriftlichen Eingaben und Telefonaten mit Beschwerdeführenden habe ich

erfahren, dass dieses Informationsschreiben in verschiedenen Internetforen lebhaft diskutiert und von betroffenen Versicherten sehr positiv aufgenommen worden ist. Dagegen habe ich an den Reaktionen von DGUV sowie verschiedenen Unfallversicherungsträgern bemerkt, dass die von mir beobachteten Unsicherheiten bei der Anwendung des Übermittlungsbegriffs immer noch nicht vollständig ausgeräumt sind, obwohl dieser Übermittlungsbegriff nun schon seit über fünf Jahren anzuwenden ist. Ich werde daher im Rahmen meiner Aufsichtspraxis weiterhin ein wachsames Auge auf die datenschutzkonforme Weiterleitung personenbezogener Gesundheitsdaten an beratende Ärztinnen und Ärzte durch Unfallversicherungsträger die meiner Aufsicht unterstehen haben.

8.16 Klage der Knappschaft gegen digitalen Auskunftsanspruch

Die Deutsche Rentenversicherung Knappschaft Bahn See verweigert den digitalen Auskunftsanspruch aus Art. 15 Abs. 3 Satz 3 der DSGVO.

Gemäß Art. 15 DSGVO hat jede betroffene Person nach Art. 4 Nr. 1 DSGVO, also jede durch personenbezogene Daten identifizierbare oder identifizierte Person, das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Im Falle des Art. 15 Abs. 3 Satz 3 DSGVO sind die Informationen im Rahmen des Auskunftsanspruchs in einem gängigen elektronischen Format zur Verfügung zu stellen, soweit die betroffene Person den Antrag auf Auskunft elektronisch gestellt hat und sich nichts Gegenteiliges ergibt.

Die Deutsche Rentenversicherung Knappschaft Bahn See (KBS) verweigert den digitalen Auskunftsanspruch aus Art. 15 Abs. 3 Satz 3 DSGVO mit Verweis auf einen unverhältnismäßig hohen Verwaltungsaufwand, sofern die entsprechenden Schriftstücke nicht ohnehin schon digitalisiert seien. So sei es nach Auffassung der KBS unverhältnismäßig, die Schriftstücke aus den einzelnen Sozialversicherungszweigen (Rentenversicherung, Krankenversicherung, Pflegeversicherung, Sozialmedizinischer Dienst, Minijob-Zentrale) zusammenzutragen und zu digitalisieren. Diese Argumentation wurde von der KBS wiederholt vertreten, sowohl im Rahmen des Aufsichts- und Kontrollbesuchs bei der Knappschaft vom 22.–25. Mai 2023 in Bochum, wie auch im Kontext eines zwischenzeitlich abgeschlossenen Beschwerdeverfahrens. In dem vorbenannten Beschwerdeverfahren nach Art. 77 Abs. 1 DSGVO habe ich gegenüber der KBS einen Maßnahmenbescheid gemäß Art. 58 Abs. 2 lit. d) DSGVO erlassen (Anweisung). Hiergegen hat die KBS Klage erhoben.

Im Kontext des derzeit anhängigen Klageverfahrens bleibt abzuwarten, inwieweit das zuständige Klagegericht (Sozialgericht Köln) meiner Rechtsauffassung folgt.

8.17 Weiterentwicklung der Protokollrecherche im Registerportal des Bundesverwaltungsamts

Das Bundesverwaltungsamt (BVA) entwickelt das sogenannte Registerportal fortlaufend weiter; auch mit dem Augenmerk auf die Protokollierung, die für meine Kontrollen unentbehrlich ist.

Das Registerportal wird durch das BVA als gemeinsame Plattform für den Zugang zu großen bundesweiten Registern betrieben. Es betrifft beispielsweise das Ausländerzentralregister (AZR), das Nationale Waffenregister (NWR) und das Visa-Informationssystem (VIS). Ich habe den gesetzlichen Auftrag zur datenschutzrechtlichen Kontrolle dieser Register. Obwohl der Gesetzgeber meine Kontrollrechte gerne als Gegengewicht zu weitergehenden Einschränkungen von Grundrechten bei Gesetzgebungsverfahren ins Feld führt, vor allem im Ausländerrecht und somit Regelungen betreffend das AZR, sind meine Kontrollmöglichkeiten in diesem Bereich beschränkt. Dies ist darauf zurückzuführen, dass die gespeicherten Protokolldaten bzgl. der Datenverarbeitung in den jeweiligen Registern nicht im notwendigen Umfang auswertbar sind bzw. die Darstellung der Ergebnisse nicht sachgerecht ist. Nachdem ich diesen Umstand bereits mehrfach bemängelt hatte und sich der Innenausschuss des Deutschen Bundestages auch für eine Anpassung ausgesprochen hat, soll nunmehr die Auswertbarkeit der Protokolldaten fortentwickelt werden. Ich hoffe, dass dem BVA die notwendigen finanziellen Mittel zur Verfügung stehen, um die erforderlichen Anpassungen vornehmen zu können.

8.18 Beschränkte Anbietungspflicht an das Bundesarchiv

Grundsätzlich sind die öffentlichen Stellen des Bundes verpflichtet, ihre Unterlagen dem Bundesarchiv zur Übernahme anzubieten. Dieser Grundsatz gilt nicht unbeschränkt.

Ich habe mich mit Vertretern des Bundesarchivs und dessen Aufsichtsbehörde, der Bundesbeauftragten für Kultur und Medien (BKM), bezüglich der Pflicht der Bundesbehörden zur Anbietung von Unterlagen gegenüber dem Bundesarchiv und Ausnahmen hiervon ausgetauscht. Eine solche Ausnahme von der grundsätzlichen Anbietungspflicht findet sich in § 6 Abs. 2 Nr. 2 Bundesarchivgesetz. Demnach sind solche Unterlagen nicht von der Anbietungspflicht umfasst, die nach gesetzlichen Vorschriften vernichtet oder gelöscht werden müssen und die nach diesen gesetzlichen Vorschriften nicht ersatzweise den zuständigen öffentlichen Archiven angeboten werden dürfen (sog. Löschungssurrogat). Solche Löschungssurrogate sollten laut dem im Zuge der letzten Reform des Bundesarchivgesetzes geäußerten Wunsch des Gesetzgebers in den jeweiligen Spezialgesetzen erfolgen. Die für die Rechtsmaterie zuständigen Ressorts sollten auf die erforderlichen gesetzlichen Regelungen hinwirken. Da dies in den seither vergangenen sechs Jahren lediglich punktuell gelungen ist, strebt die BKM nunmehr eine gesetzliche generelle Anbietungspflicht der öffentlichen Stellen an das Bundesarchiv an.

Ich stehe dem kritisch gegenüber und habe dies gegenüber der BKM und dem Bundesarchiv so kommuniziert. Der Gesetzgeber hat bewusst die oben geschilderte differenzierte gesetzliche Regelung getroffen, die ich unterstütze. Durch diese Regelung soll sichergestellt werden, dass spezifische Daten (zunächst) von der Anbietungspflicht ausgenommen sind, weil es sich bereits wegen ihres starken Personenbezugs um besonderes sensible Daten handelt. Die für die betreffende Materie jeweils zuständigen obersten Bundesbehörden sollen deshalb den archivarischen Bedarf selbst prüfen und auf dahingehende Regelungen in ihren Spezialgesetzen hinwirken, wenn sie zu dem Ergebnis kommen, dass die Archivierung entsprechender Unterlagen im Bundesarchiv zugunsten von Wissenschaft und Forschung erstrebenswert und erforderlich ist.

8.19 Informationsangebot für kleine und mittlere Postdienstleister

Bei meinen Kontrollen kleiner und mittlerer Unternehmen der Postbranche habe ich einen großen Informations- und Aufklärungsbedarf zu datenschutzrechtlichen Themen festgestellt. Daher habe ich ein spezielles Informationsangebot für diese Zielgruppe entwickelt und veröffentlicht.

Seit dem Jahr 2021 führt mein Haus regelmäßig Beratungs- und Kontrollbesuche bei kleineren Postdienstleistern durch. Wie in meinem 30. Tätigkeitsbericht (Nr. 8.2.10) berichtet, nimmt die Beratung zu grundsätzlichen Datenschutzfragen dabei einen großen Raum ein. Aktuell sind rund 68.000 Postdienstleister bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen als zuständigem Marktregulierer angezeigt. Die Mehrzahl dieser Unternehmen sind kleine und mittlere Betriebe wie Paketshops und Transport- und Beförderungsunternehmen, die z. B. die Zustellung auf der sogenannten letzten Meile zwischen Depot und Haustüre verantworten.

Um diese Unternehmen für die datenschutzrechtlichen Grundlagen ihrer Tätigkeit zu sensibilisieren und in Fragen der praktischen Umsetzung zu beraten, habe ich am Weltposttag, dem 9. Oktober 2023, den Flyer „Datenschutz und Postdienstleister“ veröffentlicht, der durch umfangreichere Textbeiträge auf meiner Internetseite ergänzt wird. Hier wird das Wichtigste zum Thema Datenschutz für Postdienstleister kurz und prägnant erläutert. Zu Fragen wie: „Was muss ich als Postdienstleister beim Datenschutz beachten?“ „Braucht mein Unternehmen einen Datenschutzbeauftragten?“ oder „Wann wende ich mich an welche Aufsichtsbehörde?“ finden sich Antworten und praktische Umsetzungstipps.

Link zum Flyer in deutscher und englischer Sprache

(QR-Code scannen oder klicken)

Neu angezeigte Postdienstleister erhalten den Flyer „Datenschutz und Postdienstleister“ künftig mit der Bestätigung der Anzeige ihrer Postdienstleistungen durch die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen.

Ich bin nach dem ersten Feedback auf die Veröffentlichung zuversichtlich, dass das neue Informationsangebot dazu beitragen wird, bei kleinen und mittleren Unternehmen der Postbranche weiter für Datenschutzfragen zu sensibilisieren und einen guten Datenschutzstandard sicherzustellen.

9 Kontrollen und Beratungsbesuche

9.1 Kontrollen und Beratungsbesuche Sicherheitsbereich

Zu meinen wesentlichen Aufgaben gehört die Durchführung von Kontrollen bei den meiner Zuständigkeit unterliegenden datenverarbeitenden Stellen. Kontrollen erfolgen oftmals anlassbezogen – so zum Beispiel aufgrund von Hinweisen auf problematische Datenverarbeitungen in schriftlichen Unterlagen, aufgrund von Medienberichten oder auch von Hinweisen von Bürgerinnen und Bürgern. Daneben führe ich eine Vielzahl von Kontrollen anlasslos durch.

Besonders im Sicherheitsbereich, wo Betroffene oftmals keine Kenntnis von Eingriffen in ihr Grundrecht auf informationelle Selbstbestimmung haben, kommt Datenschutzkontrollen als Ausfluss meiner Kompensationsfunktion eine herausragende Bedeutung zu. Aus diesem Grund sehen viele Gesetze in diesem Bereich auch sogenannte Pflichtkontrollen vor. Diese verpflichten mich von Gesetzes wegen, in regelmäßigen Abständen besonders eingriffsintensive Datenverarbeitungen zu kontrollieren. Wesentliches Element meiner Kontrollen ist immer auch die Beratung der Verantwortlichen. Auf diese Weise lassen sich oftmals Datenschutzverstöße bereits im Vorfeld vermeiden. Denn Ziel ist es nicht, möglichst viele Datenschutzverstöße aufzudecken und zu sanktionieren. Stattdessen soll durch eine regelmäßige Kontrollpraxis das Datenschutzbewusstsein bei den Sicherheitsbehörden gefestigt und dadurch dazu beigetragen werden, die von der Datenverarbeitung betroffenen Personen nachhaltig zu schützen. Mit diesem Ziel habe ich auch in diesem Berichtszeitraum wieder eine Vielzahl von Kontrollmaßnahmen durchgeführt.

9.1.1 Kontrolle der Zugriffe der Sicherheitsbehörden des Bundes auf das Visainformationssystem, Eurodac und das Schengener Informationssystem

Die Kontrollen der Zugriffe der Polizeibehörden des Bundes auf das Visainformationssystem (VIS), das Schengener Informationssystem (SIS) und die Datei Eurodac (European Dactyloscopy) führten zu keinen Beanstandungen. Gleiches gilt für Zugriffe des Bundesnachrichtendienstes (BND) auf VIS und das SIS. Zur Dokumentation der Gründe für den Zugriff ergingen in meinen Kontrollberichten Hinweise. Weitere datenschutzrechtliche Eigenkontrollen habe ich empfohlen.

Im Berichtsjahr habe ich mehrere bereits im Vorjahr begonnene Kontrollen abgeschlossen. Im Einzelnen handelt es sich um die beim Bundeskriminalamt (BKA) begonnenen Kontrollen der dortigen Zugriffe auf VIS und die Datei Eurodac sowie die ebenfalls beim BKA vorgenommene Prüfung der Rechtmäßigkeit der Datenverarbeitungsvorgänge im nationalen System des Schengener Informationssystems der zweiten Generation (N.SIS II). Zudem habe ich im Jahr 2023 eine weitere Kontrolle zur Nutzung der Datei Eurodac beim Zollkriminalamt (ZKA) durchgeführt. Im Rahmen dieser Kontrolle habe ich festgestellt, dass das ZKA in dem zuvor festgelegten Prüfzeitraum keine Eurodac-Abfragen getätigt hat, so dass diese Prüfung ohne Folgemaßnahmen abgeschlossen werden konnte. Die drei bereits im Jahr 2022 begonnenen Prüfungen führten zu keiner Beanstandung. Die Kontrolle des SIS ergab allerdings über das SIS hinausgehende Fragen hinsichtlich der IT-Infrastruktur des BKA, denen ich zu einem späteren Zeitpunkt gesondert nachgehen werde.

Zudem habe ich im Ergebnis der Kontrolle der VIS-Zugriffe des BKA nochmals den Hinweis zur Dokumentation aus meinem Kontrollbericht vom 13. September 2019 in Erinnerung gerufen. Im Rahmen der Prüfung der Datenverarbeitungsvorgänge im N.SIS II habe ich eine Verstärkung der Eigenkontrolle empfohlen.

Beide von mir im Jahr 2023 durchgeführten Kontrollen beim BND zum SIS und VIS hatten zum Ergebnis, dass der BND seine Zugriffe (besser) dokumentieren muss. Insbesondere die Dokumentation des Zugriffsgrundes war in der Vielzahl der von mir geprüften Einzelfälle ungenügend. Gleichwohl konnten mir in den Kontrollen sämtliche Zugriffe auf die Systeme nachvollziehbar dar-

gelegt werden. Rechtsverstöße habe ich in den von mir geprüften Einzelfällen nicht festgestellt. Soweit das VIS betroffen ist, bedarf es einer grundsätzlichen Klärung, ob der nationale Gesetzgeber dem BND zu Recht ein Zugriffsrecht auf dieses eingeräumt hat. Hintergrund dieser Frage sind die europarechtlichen Regelungen, die polizeirechtlich und nicht nachrichtendienstrechtlich ausgestaltet sind.

9.1.2 Beanstandungen betroffener Personen im Bundeszentralregister

Die Bearbeitung sogenannter Beanstandungen von Registereintragungen durch betroffene Personen im Bundeszentralregister (BZR) war Gegenstand eines Kontrollbesuchs. Dabei stand vor allem der Umgang mit festgestellten Datenschutzverletzungen im Zentrum meines Interesses.

Unter dem Begriff der Beanstandungen werden im BZR sämtliche Eingaben von betroffenen Personen verstanden, die Einwendungen gegen Registereintragungen zu ihrer Person vorbringen. Dies können ganz verschiedene Sachverhalte sein. Die meisten Eingaben beziehen sich in Unkenntnis der nicht unkomplizierten Regelungen im Bundeszentralregistergesetz darauf, dass Eintragungen bezüglich kleiner Geldstrafen oder weit in der Vergangenheit liegender Verurteilungen vermeintlich nicht mehr im Führungszeugnis erscheinen dürften. Mitunter wird aber auch behauptet, es läge gar keine Straftat vor oder das Strafverfahren sei fehlerhaft geführt worden. Bei der Bearbeitung solcher Beanstandungen konnte ich keine datenschutzrechtlichen Probleme feststellen.

Mein Fokus bei der Kontrolle lag auf berechtigten Beanstandungen. Dies sind in der Regel Fälle, in denen bei der Erteilung eines Führungszeugnisses einer Person Registereintragungen zugeordnet wurden, die zu einer anderen Person mit sehr ähnlichen oder gar identischen Personendaten gehören. Solche Falschauskünfte kommen hin und wieder vor und sind bei einem Massenverfahren wie dem BZR auch kaum vermeidbar. Problematisch stellte sich für mich allerdings dar, wie lange nach dem Erkennen einer solchen Datenschutzverletzung die entsprechende Meldung der Sachbearbeitung braucht, um hausintern bei der für den administrativen Datenschutz zuständigen Stelle anzukommen. Hier vergehen im Schnitt fast zwei Wochen, was meines Erachtens einen Verstoß gegen die Unverzüglichkeit nach Art. 33 Abs. 1 Satz 1, Art. 34 Abs. 1 DSGVO darstellt. Ansonsten wurden kleinere Probleme bei der Abfrage des Meldeportals und der Aktenführung identifiziert. In einem Einzelfall wurde meiner Meinung nach zu Unrecht auf die Meldung nach Art. 33 DSGVO verzichtet. Nach dieser Vorschrift sind Datenschutzverletzungen unverzüglich an die Datenschutzaufsichtsbehörde zu melden.

9.1.3 Kontrolle des Zeugenschutzes im Bundeszentralregister

Bei einem Kontrollbesuch habe ich Zeugenschutzfälle im Bundeszentralregister (BZR) geprüft. Dies ist ein nicht nur datenschutzrechtlich sehr sensibler Teil des Bundeszentralregisters.

Die gesetzliche Regelung zum Umgang mit Zeugenschutzfällen im BZR findet sich in § 44a Bundeszentralregistergesetz. Sinn der Vorschrift ist es, dass bezüglich Personen, die in ein Zeugenschutzprogramm aufgenommen wurden, nicht ohne weiteres Registerauskünfte erteilt werden. Auskünfte zu den Echtdaten der geschützten Person sollen nur erteilt werden, wenn die zuständige Zeugenschutzstelle dies für unproblematisch erachtet.

Die Zeugenschutzstellen sind bei den Polizeibehörden angesiedelt und haben nach dem Zeugenschutzharmonisierungsgesetz weitgehende Befugnisse. Falls die Person im BZR vorher nicht bekannt war, wird ein spezieller Datensatz angelegt, um auf Auskunftsbegehren zu der Person aufmerksam zu werden, ohne aber gleichzeitig deren Schutz zu unterlaufen.

In der Kontrolle wurden bezüglich der Standardfälle keine Probleme gefunden. Bei einigen Spezialfällen wurden jedoch problematische Sachverhaltskonstellationen identifiziert. Bezüglich einer dieser Konstellationen habe ich eine Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO ausgesprochen. Hier wurden nach meiner Auffassung die gesetzlichen Befugnisse in Zeugenschutzsachen deutlich überschritten. Details dazu kann ich aufgrund der Sensibilität des Gegenstandes an dieser Stelle nicht schildern.

9.1.4 Speicherungen von ermittlungsunterstützenden und personengebundenen Hinweisen im Bundeskriminalamt

Bereits vor dem Berichtsjahr 2023 hatte ich meinen umfangreichen Beratungs- und Kontrollbesuch beim Bundeskriminalamt (BKA) begonnen. Gegenstand waren die Speicherungen von personengebundenen Hinweisen (PHW) gemäß § 16 Abs. 6 Nr. 1 BKAG und ermittlungsunterstützenden Hinweisen (EHW) gemäß § 16 Abs. 6 Nr. 2 BKAG durch das BKA. Die sogenannte PHW vergibt das BKA, wenn dies zum Schutz der betroffenen Person oder zur Eigensicherung von Polizeibeamtinnen und -beamten erforderlich ist. EHW werden vergeben, wenn Hinweise vorliegen, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen.

Im Vorfeld der Kontrolle teilte mir das BKA mit, insgesamt 64.850 PHW und 10.562 EHW gespeichert zu haben. Die PHW und EHW werden durch das BKA im bundesweiten zentralen polizeilichen Informationssystem (INPOL-Z) in der sogenannten W-Gruppe gespeichert. Neben den Polizeien des Bundes speichern auch die Landespolizeibehörden in INPOL-Z PHW bzw. EHW. Um eine bundesweit einheitliche Vergabe sicherzustellen, werden die PHW und EHW auf Grundlage von gemeinsamen Leitfäden vergeben. Der Leitfaden zur Vergabe der PHW ist nicht mehr als Verschlusssache nur für den Dienstgebrauch (VS-NfD) eingestuft. Derzeit prüft das BMI, ob an der Einstufung des Leitfadens zur Vergabe der EHW weiter festgehalten wird.

In meiner Kontrolle habe ich in Stichproben unter anderem die PHW „Betäubungsmittelkonsument" (BTMK) und „Psychische- und Verhaltensstörung" (PSYV) sowie ausgewählte EHW geprüft.

Zunächst möchte ich besonders positiv erwähnen, dass mich das BKA bei meinem Kontrollbesuch sehr gut und kooperativ unterstützt hat. Dies hat mir die datenschutzrechtliche Prüfung erheblich erleichtert. Insbesondere durch die Bereitstellung eines separaten Büros für die Kontrolldurchführung und eigene lesende Zugriffe auf die polizeilichen Systeme konnte ich die ausgewählten Stichproben mit der erforderlichen Tiefe prüfen. Das BKA zeigt sich mir als datenschutzrechtliche Aufsicht gegenüber sehr transparent. Das wirkt sich entsprechend positiv auf meine Kontrollmöglichkeiten aus.

In meiner Kontrolle bin ich auf mindestens 3.035 Fälle gestoßen, in denen das BKA PHW vergeben hat, ohne über notwendige Belege, bzw. einen Aktenrückhalt zu verfügen und zuvor geprüft zu haben, ob der Hinweis zum Schutz der betroffenen Person oder zur Eigensicherung von Polizeivollzugsbeamtinnen und -beamten erforderlich ist. In diesen Fällen war ein Freitextfeld mit „ALTBESTAND BESITZER NICHT GEPRÜFT" bezeichnet. Dies verstößt gegen § 16 Abs. 6 Nr. 1 BKAG. Diesen Verstoß habe ich beanstandet. Das BKA teilte mir bereits während der Kontrolle mit, an einem Bereinigungsprozess zu arbeiten. Dieser sei voraussichtlich Ende 2023 abgeschlossen. Obgleich sich das BKA sehr kooperativ verhalten hat, konnte ich von einer Beanstandung nicht absehen, weil es sich weder um einen unerheblichen noch um einen inzwischen beseitigten Mangel gehandelt hat.

Kurz vor Redaktionsschluss teilte mir das BMI mit, der Bereinigungsprozess der 3.035 unreferenzierten W-Gruppen sei nunmehr abgeschlossen. Ich begrüße, dass das BKA meine Beanstandung zum Anlass genommen und die angekündigte Überprüfung umgehend durchgeführt hat.

Das BKA vergibt den PHW PSYV regelmäßig auf Grundlage der Angabe „Mentally Ill" in den Fahndungsersuchen (Notices) der International Criminal Police Organisation (INTERPOL). In diesen Fällen liegt regelmäßig kein ärztliches Attest oder Gutachten vor, obwohl dies Voraussetzung nach dem Leitfaden zur Vergabe personengebundener Hinweise ist. Eine abschließende rechtliche Bewertung dieser Praxis war für mich zum Zeitpunkt der Kontrolle nicht möglich. Es stellt sich die Frage, welche Tatsachengrundlage den jeweiligen Fahndungsersuchen zu Grunde liegt bzw. welche Standards bei Interpol einzuhalten sind. Damit das BKA die Angabe „Mentally Ill" ungeprüft übernehmen kann, müsste geklärt sein, welche Gründe die Interpolteilnehmenden zur Vergabe der Bezeichnung veranlasst haben und ob die Interpolteilnehmenden einen Nachweis über eine solche Erkrankung vorlegen, bevor ein Fahndungsersuchen ausgesprochen wird. Mit Blick darauf und um die Rechtmäßigkeit der Speicherung prüfen zu können, hatte ich mich im Mai dieses Jahres an die unabhängige Kontrollkommission bei Interpol gewandt und um Stellungnahme gebeten, auf welcher Tatsachengrundlage die Angaben der Teilnehmerstaaten beruhen, die eine Bezeichnung wie „Mentally Ill" rechtfertigen. Interpol teilte nun Ende September mit, mir gegenüber keine Stellungnahme abzugeben. Das BKA sei als Nationales Zentralbüro für Deutschland einziger zuständiger Kommunikationspartner für Interpol. Gerade mit Blick darauf, dass Interpol die Achtung der Grundrechte und Qualität der internationalen polizeilichen Zusammenarbeit betont,[107] hätte ich eine andere Reaktion auf meine Anfrage erwartet. Ich werde nun das BKA in seiner Funktion als Nationales Zentralbüro bitten, den klärungsbedürftigen Fragen nachzugehen.

In dem Kontrollbesuch habe ich zudem festgestellt, dass die Dokumentation der PHW und EHW nicht den Anforderungen an eine ordnungsgemäße Dokumentation polizeilichen Handelns entspricht und insofern nach § 16 Abs. 2 BDSG als Verstoß gegen § 6 Satz 3 EGovG bzw. § 23 BKAG in Verbindung mit den durch Art. 20 Abs. 3 Grundgesetz vorgegebenen allgemeinen Grundsätzen der Aktenführung zu beanstanden ist. Vor diesem Hintergrund habe ich an meinem Prüfergebnis zur Aktenführung beim BKA festgehalten (29. TB Nr. 9.5.3). Die Dokumentation der Rechtmäßigkeit polizeilichen Handelns in

107 Hinweise von Interpol zum Datenschutz, abrufbar unter: https://www.interpol.int/en/Who-we-are/Legal-framework/Data-protection

Bezug auf die Speicherung von personengebundenen und ermittlungsunterstützenden Hinweisen ist in einem erforderlichen Mindestmaß sicherzustellen.

Das BMI hat zu meinem Prüfbericht Stellung genommen, sich inhaltlich aber nicht vollständig meinen Ausführungen angeschlossen. Insbesondere zu den Anforderungen an die Dokumentation polizeilichen Handelns wird eine andere Auffassung vertreten.

9.1.5 Datei „Gewalttäter Sport“

Die Datei „Gewalttäter Sport“ ist gemäß § 29 Abs. 1 bis 5 Bundeskriminalamtgesetz (BKAG) eine Verbunddatei, die es den Polizeien der Länder sowie des Bundes ermöglicht, sportspezifische Personenerkenntnisse zu speichern und im Fahndungssystem des bundesweiten zentralen polizeilichen Informationssystems (INPOL) abzubilden.

In Vorbereitung auf die Kontrolle hat mir das Bundeskriminalamt (BKA) alle Speicherungen nach den jeweiligen Teilnehmenden der Datei aufgeschlüsselt und übermittelt. Gleichzeitig teilte mir das BKA mit, dass es selbst keine Speicherungen in der Datei „Gewalttäter Sport“ vornehme und diese als Zentralstelle auch nicht pflege. Lediglich die technische Aufbereitung der Datei werde durch das BKA realisiert. Nach Auskunft des BKA erfolgen die Datenpflege, Speichervoraussetzungen und Anlieferung der Daten über die Zentrale Informationsstelle für Sporteinsätze (ZIS). Die geplante Vorort-Kontrolle beim BKA wurde deshalb nicht fortgeführt.

Die ZIS ist beim Landesamt für Zentrale Polizeiliche Dienste in Nordrhein-Westfalen eingerichtet. Sie nimmt Aufgaben in Zusammenhang mit Sportgroßveranstaltungen (insbesondere Fußballspielen) sowohl im Inland als auch Ausland wahr. Die Stelle sammelt, bewertet, steuert und bereitet die anlassbezogenen Informationen auf. Nach wie vor ist nicht geklärt, auf welcher rechtlichen Grundlage die ZIS errichtet und ihr die länderübergreifende Aufgabenkompetenz übertragen worden ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte die Innenministerkonferenz bereits im Jahr 2021 gebeten, hierzu Stellung zu nehmen. Dazu hatte sie dies an den in der Innenministerkonferenz zuständigen „AK II“ weitergeleitet. Auf Nachfrage teilte die Geschäftsstelle der IMK nunmehr mit, dass der Prüfauftrag, „… ob die Beschlüsse (…) noch aktuell sind oder ob sie ggf. einer Anpassung bedürfen, (…) noch nicht beratungsreif“ sei. Daraus schließe ich, dass dieses Thema in der Innenministerkonferenz nicht mit Nachdruck bearbeitet wird.

9.1.6 Kontrollen zum Sicherheitsüberprüfungsgesetz

Damals wie heute gilt: Vorbeugen ist besser als Heilen. Auch meine Kontrollbesuche zeigen zunehmend präventive Wirkung, denn die kontrollierten Stellen nehmen diese immer mehr als Chance zur datenschutzrechtlichen Beratung an. Und der Bedarf ist groß, denn wie meine Kontrollergebnisse zeigen, bestehen nach wie vor Unsicherheiten in Bezug auf den datenschutzkonformen Umgang mit personenbezogenen Daten im Sicherheitsüberprüfungsverfahren.

Im Berichtsjahr führte ich erstmals einen Informationsbesuch bei zwei – hinsichtlich der Anzahl an Sicherheitsüberprüfungsverfahren – repräsentativen Patentanwaltskanzleien zu den Besonderheiten des Sicherheitsüberprüfungsverfahrens in diesem Tätigkeitsfeld durch und erörterte meine Erkenntnisse anschließend gemeinsam mit dem Deutschen Patent- und Markenamt als zuständige Stelle. Meine weitere Beratung bei der Fortentwicklung des Verfahrens und Unterstützung bei der Durchführung von Fortbildungsangeboten habe ich angeboten.

Außerdem kontrollierte ich bei 15 Stellen die Einhaltung der datenschutzrechtlichen Vorgaben des Sicherheitsüberprüfungsgesetzes. Im öffentlichen Bereich betraf dies acht Behörden und sieben geheim- und sabotageschutzbetreute Unternehmen. Bei den kontrollierten Behörden handelte es sich um

- das Bundesministerium für Gesundheit,
- die Bundestagspolizei,
- die Bundesanstalt für Landwirtschaft und Ernährung,
- den Dienstältesten Deutschen Offizier Deutscher Anteil 1st NATO Signal Battaillon in Wesel,
- die Bundespolizeiakademie,
- eine mitwirkende Behörde i. S. d. § 3 Abs. 2 und 3 SÜG,
- die Generalzolldirektion in Neustadt a. d. W und
- das Bundespresseamt.

Bei den kontrollierten Wirtschaftsunternehmen handelte es sich um Unternehmen aus den Branchen der Rüstung, IT (2x), Luftfahrt (2x), Personen- und Objektschutz (2x).

Soweit die Kontrollberichte veröffentlicht werden konnten, finden Sie diese auf meiner Webseite.

(QR-Code klicken oder scannen)

Gegenüber zwölf kontrollierten Stellen habe ich Beanstandungen aufgrund datenschutzrechtlicher Verstöße im Anwendungsbereich des SÜG ausgesprochen. Diese richteten sich gegen das Bundesministerium für Gesundheit, die Bundestagspolizei, die Bundesanstalt für Landwirtschaft und Ernährung, die Bundespolizeiakademie, die mitwirkende Behörde, die Generalzolldirektion in Neustadt a. d. W., das Bundespresseamt und fünf Unternehmen, die der Geheimschutzbetreuung des Bundesministeriums für Wirtschaft und Klimaschutz unterliegen. Die Beanstandungen betrafen:

- fehlende organisatorische Maßnahmen in Form unzureichender Personalausstattung in den Organisationsbereichen des personellen Geheim- und Sabotageschutzes (2 Fälle),
- fehlende organisatorische Maßnahmen zur Sicherstellung eines ausreichenden Informationsflusses seitens der Personalstelle an den Bereich Geheimschutz, zur Dokumentation der Aufnahme und des Ausscheidens von (Fremd-)Personal aus der sicherheitsempfindlichen Tätigkeit sowie zur Verwaltung der entsprechenden Informationen durch ein funktionierendes Wiedervorlagesystem (6 Fälle),
- Verstöße gegen Löschvorschriften (6 Fälle),
- Mängel im Wiedervorlagesystem in Gestalt von Abweichungen zwischen Akte und elektronischer Wiedervorlage (2 Fälle),
- Datenübermittlungen im Besuchskontrollverfahrens ohne Nachweis der erforderlichen Zustimmung (2 Fälle),
- das Eröffnen einer zweiten Sicherheitsakte für dieselbe betroffene Person (1 Fall) sowie das Führen einer Sicherheitsakte ohne Ausübung einer sicherheitsempfindlichen Tätigkeit (1 Fall),
- die unzulässige systematische Speicherung personenbezogener Daten in Dateien in großem Umfang (1 Fall),
- die Übermittlung von personenbezogenen Daten an unberechtigte Dritte (1 Fall),
- die Speicherung personenbezogener Daten Dritter ohne Rechtsgrundlage, um diese von VS-NfD-Belehrungen auszuschließen (1 Fall),
- die fehlende Dokumentation der Zustimmung der betroffenen oder mitbetroffenen Person in älteren Sicherheitserklärungen (1 Fall).

Über die ausgesprochenen Beanstandungen hinaus haben meine Mitarbeitenden bei allen kontrollierten Stellen Datenschutzverstöße oder Mängel festgestellt. Zu den häufigsten Fehlern gehörten unzulässige Angaben in der Sicherheitserklärung, die Verarbeitung personenbezogener Daten Dritter ohne Rechtsgrundlage, die Verarbeitung unzulässiger Unterlagen in der Sicherheitsakte und unzulässige Speicherungen in Dateien. Hinzu kamen auch in diesem Berichtsjahr oft Defizite bei der Sicherstellung der rechtzeitigen Vernichtung von Sicherheitsakten und korrespondierenden Datensätzen in Dateien. Nahezu ebenso häufig gab es Mängel bei technisch-organisatorischen Maßnahmen zur Sicherstellung einer ordnungsgemäßen Datenverarbeitung, beispielsweise eine fehlende Protokollierung bei Dateien, die ungeschützte Zugriffsmöglichkeit auf die eigene Sicherheitsakte seitens der/des Geheimschutzbeauftragten oder der Mitarbeitenden, die fehlende Sicherstellung des Abschottungsgebotes zwischen den Bereichen Geheimschutz und Personal sowie die unverschlüsselte Nutzung elektronischer Kommunikationswege.

Eines wird daraus sehr deutlich: Die zahlreichen Defizite sind überwiegend auf bestehende Rechtsanwendungsunsicherheiten seitens der verantwortlichen Stellen zurückzuführen. Gerade deshalb messe ich der datenschutzrechtlichen Beratung in meinen Kontrollen stets einen sehr hohen Stellenwert bei. Immer häufiger nutzen die kontrollierten Stellen die Gelegenheit und treten mit Beratungsanfragen an mich heran. Anregungen und Verbesserungsvorschläge meinerseits werden dankend angenommen und umgesetzt. Auf positive Resonanz stoßen auch meine Schulungsangebote bei der Bundesakademie für öffentliche Verwaltung, dem Sicherheitsseminar des Bundesministeriums für Wirtschaft und Klimaschutz sowie bei Arbeitskreisen der Sicherheitsbevollmächtigen in der Wirtschaft als Multiplikatoren für die nichtöffentlichen Stellen. Die Veröffentlichung von Arbeitshilfen und Kontrollberichten meiner Homepage nutze ich als weiteres Mittel, um den verantwortlichen Stellen aufzuzeigen, wie sie personenbezogene Daten in Sicherheitsüberprüfungsverfahren gesetzeskonform verarbeiten und Datenschutzverstößen vorbeugen können.

So gab es auch in diesem Jahr wieder einige Positivbeispiele, insbesondere im nichtöffentlichen Bereich. Diese zeigen, dass man mit den entsprechenden technischen Ressourcen und organisatorischen Maßnahmen trotz vergleichsweise geringen Personaleinsatzes auch ein sehr hohes, vierstelliges Fallaufkommen beherrschen und sehr gute Arbeitsprozesse etablieren kann.

9.1.7 Kontrollen beim Bundesamt für den Verfassungsschutz

Im Berichtszeitraum habe ich erneut diverse Kontrollen sowie Beratungs- und Informationsbesuche beim Bundesamt für Verfassungsschutz (BfV) durchgeführt. Neben u. a. der Fortsetzung der Kontrolle und auch Beratung zu der elektronischen Akte beim BfV hat sich ein weiterer Schwerpunkt in Bezug auf die Beobachtung im Internet herauskristallisiert.

Internetbeobachtung

Verfassungsfeindliche und staatsgefährdende Aktivitäten verlagern sich seit Jahren zunehmend ins Internet. Das Gefährdungspotential steigt durch die größere Reichweite und die tatsächliche oder vermeintliche Anonymität der Akteure. Es ist daher zwingend notwendig, dass der Verfassungsschutz auch im digitalen Raum mit wirksamen Mitteln seinen Aufgaben nach dem Verfassungsschutzgesetz nachkommt.

Soweit das BfV personenbezogene Daten in neuen Dateien speichert, bin ich im Rahmen einer Dateianordnung vor Inbetriebnahme der Datei anzuhören. In diesem Zusammenhang bin ich im Berichtszeitraum mehrfach beteiligt worden. Hierbei habe ich zwei Dateien noch einmal einer gesonderten datenschutzrechtlichen Prüfung unterzogen.

Bei einer der Dateien musste ich feststellen, dass diese zwar dem Grunde nach rechtmäßig betrieben werden könnte, die tatsächliche Umsetzung jedoch erhebliche Defizite aufwies. Nach zweijährigem Betrieb existierte beispielsweise keine ordnungsgemäße Dokumentation der Datenverarbeitung. Die festgestellten Mängel führten zu mehreren Beanstandungen.

Teile der Beanstandungen hat das Bundesministerium des Innern und für Heimat (BMI) als zuständige oberste Bundesbehörde zurückgewiesen. So argumentiert das BMI, es existiere keine (einfach-)gesetzliche Pflicht zur Dokumentation, weshalb sich ein Dokumentationsmangel nicht auf Art. 20 Abs. 3 GG stützen lasse bzw. ein Verstoß nicht beanstandungsfähig sei. Diese Argumentation habe ich wiederum zurückgewiesen. Die Dokumentation des Verwaltungshandelns ist Grundlage für eine rechtstaatliche und überprüfbare Verwaltung. Ohne Dokumentation ist mir eine Erfüllung meiner Aufgaben nicht möglich. Zudem hat das BMI bereits an früherer Stelle gegenüber dem Bundestag in einer Antwort auf eine Kleine Anfrage zur ordnungsgemäßen Aktenführung selbst auf Art. 20 Abs. 3 GG verwiesen. Und auch das Bundesverwaltungsgericht leitet die Dokumentationspflicht mittelbar aus Art. 20 Abs. 3 GG her. Wie das BMI als Rechtsaufsicht des BfV zu der Einschätzung gelangt ist, dass eine fehlende Dokumentation kein beanstandungswürdiges Problem darstellt, entzieht sich meiner Kenntnis und meinem Verständnis.

Bei der anderen Datei bin ich bereits frühzeitig im Rahmen des Beschaffungsprozesses eingebunden worden. Bedauerlicherweise war es mir im konkreten Fall allerdings nicht möglich, meiner Beratungsfunktion vollumfänglich nachzukommen. Dies lag vor allem daran, dass einige Sachverhaltsfragen, die für eine datenschutzrechtliche Bewertung zwingend erforderlich sind, mit dem BfV nicht geklärt werden konnten. Ich habe mich daher zunächst auf die Kontrolle des so genannten „Proof of Concept“, also die Testphase der Datei, beschränkt. Diese Kontrolle war zum Redaktionsschluss noch nicht abgeschlossen. Ich werde den laufenden Prozess im kommenden Jahr weiter begleiten und ggfs. eine Folgekontrolle der Datei im Wirkbetrieb durchführen.

Eine weitere neu geschaffene Datei, die als Verbunddatei die Ergebnisse von Internetbeobachtungen zu Dokumentationszwecken entgegennimmt, wurde von mir kontrolliert. Trotz eines grundsätzlich guten Eindrucks habe ich kritisiert, dass der Verwendungszweck zu unspezifisch und die Zugriffsmöglichkeiten zu weit gefasst waren. Das BfV will hier im Detail nachbessern.

Verletzung meiner Kontrollkompetenz wegen verweigerter Aktenübersendung

In zwei Fällen von Bürgereingaben wollte ich vom BfV die entsprechenden Akten, die das BfV über die Personen angelegt hat, als Kopie übersendet haben, um mögliche Datenschutzverletzungen detailliert prüfen zu können. In beiden Fällen konnte ich die Akte zwar vor Ort umfänglich einsehen. Meiner Bitte, mir die Akte als Ganzes zuzusenden, wurde aber im Ergebnis nach Rücksprache mit dem BMI nicht entsprochen. Zur Begründung hieß es, dass das BfV gesetzlich zwar zur Mitwirkung bei der Kontrolle durch den BfDI verpflichtet sei. Dies beinhalte aber nur die Einsichtnahme vor Ort, also beim BfV, nicht aber die Übersendung von Akten. Auszüge aus Akten oder Dateien habe ich in der Vergangenheit in der Regel unproblematisch erhalten. Hier hatte ich aber auf die Übersendung der gesamten Akte bestanden, weil ich bei der Einsichtnahme vor Ort bereits Hinweise auf mehrere mögliche Datenschutzverletzungen fand,

die ich detailliert in meinem Hause überprüfen wollte. Interessanterweise hat mich das BfV nicht daran gehindert, im Rahmen der Einsichtnahme vor Ort notwendige Notizen zu fertigen.

Auch wenn § 28 Abs. 3 BVerfSchG bei der Mitwirkungspflicht festlegt, dass das BfV mir „insbesondere […] Einsicht in alle Unterlagen […] zu gewähren hat", spricht dies nach meiner Auffassung keineswegs dafür, dass ich auf die Einsichtnahme vor Ort beschränkt bin. Die Einsichtnahme ist vielmehr nur als eine der möglichen Konkretisierungen der Mitwirkungspflicht anzusehen. Mir obliegt – bestätigt durch das Bundesverfassungsgericht – eine Kompensationsfunktion zugunsten der von nachrichtendienstlichen Maßnahmen Betroffenen aufgrund des schwachen Individualrechtsschutzes in diesem Bereich. Damit bin ich im Ergebnis Anwalt der Betroffenen und muss auch schon deswegen wie ein Anwalt im Gerichtsverfahren im Rahmen des Akteneinsichtsrechts behandelt werden.

Insbesondere die Frage nach dem Einsichtsrecht im Zusammenhang mit Aktenübermittlungen wurde in der ständigen Rechtsprechung zum Verwaltungsverfahren zu § 29 Verwaltungsverfahrensgesetz (VwVfG) hinreichend entschieden. Das festgeschriebene Akteneinsichtsrecht (vor Ort) kann im Rahmen der pflichtgemäßen Ermessensausübung der Behörde auch mittels einer im Ausnahmefall gestatteten Übersendung der Akten erfolgen. Eine solche Ausnahme wird u. a. bei der Übermittlung der Akten in die Kanzleiräume eines Rechtsanwaltes angenommen.[108] Soweit die Erfüllung der Aufgaben der Behörde nicht beeinträchtigt wird und auch sonstige Gesichtspunkte nicht entgegenstehen, ist die Verweigerung einer Ausnahme nach § 29 Abs. 3 Satz 2 VwVfG ermessensfehlerhaft. Etwaige berechtigte Interessen des BfV, die einer Aktenübersendung im Rahmen einer Güterabwägung entgegenstehen könnten, sind mir nicht ersichtlich. Daher muss das Einsichtsrecht mittels Übermittlung mindestens analog für § 28 Abs. 3 BVerfSchG und auch § 36a Abs. 3 Satz 1 Sicherheitsüberprüfungsgesetz ausgelegt werden. Dies ist bei einer grundsätzlichen Gefahr von rechtswidrigen Grundrechtseingriffen zwingend geboten.

Ich werde mich weiter mit allen erforderlichen Mitteln für die Übermittlung von Akten einsetzen, um den Anliegen der Bürgerinnen und Bürger gerecht werden zu können.

Elektronische Akte beim BfV

Die im vorangegangenen Berichtszeitraum durchgeführte Kontrolle der elektronischen Akte hat die Notwendigkeit einer Folgekontrolle ergeben, die ich in diesem Jahr, wie geplant, gemeinsam mit dem behördlichen Datenschutz des BfV durchgeführt habe (vgl. 31. TB Nr. 9.4.9). Dabei stand insbesondere die Geeignetheit des vom BfV intern entwickelten Kontrollkonzepts im Fokus. Die Kontrolle ist zum Redaktionsschluss noch nicht abgeschlossen. Zum jetzigen Zeitpunkt kann jedoch bereits positiv hervorgehoben werden, dass die im Rahmen der vorangegangenen Kontrolle von mir geforderten organisatorischen Maßnahmen zur Sensibilisierung der Mitarbeitenden überwiegend umgesetzt wurden. Beispielsweise die Bereitstellung von anwenderfreundlich gestaltetem Informationsmaterial trägt dazu bei, dass die vielseitig bestehenden Unklarheiten bei der Anwendung der Suche nach personenbezogenen Daten in der elektronischen Akte abgebaut werden. Die Geeignetheit des BfV-intern entwickelten Kontrollkonzepts sowie die turnusmäßige Durchführung dieser Kontrollen stehen noch auf dem Prüfstand und zeigten in den ersten Kontrollteilen bereits positive Ergebnisse. In dem Kontext habe ich auch die Beratung zu der zukünftigen elektronischen Akte, dem Dokumentenmanagementsystem im Verfassungsschutzverbund (Verbund-DMS), fortgesetzt. Neben der laufenden schriftlichen Beratung habe ich in diesem Berichtsjahr einen Informationstermin vor Ort wahrgenommen, um mir ein besseres Bild von dem aktuellen Verfahrensstand zu machen und einen ersten Einblick in das neue System zu erhalten. Mein Fokus liegt hierbei insbesondere darauf, die geforderten Maßnahmen, die sich aus der Kontrolle der aktuellen elektronischen Akte ergeben und aus datenschutzrechtlicher Sicht als notwendig herauskristallisiert haben, auch beim Verbund-DMS zu implementieren. Neben den o. g. erforderlichen organisatorischen Maßnahmen bleibt es mir weiterhin ein Anliegen, laufend zu prüfen, ob auch technische Maßnahmen entsprechend Abhilfe schaffen können. Zudem erachte ich es als unbedingt erforderlich, frühzeitig und auch regelmäßig verpflichtende Schulungen für die Mitarbeitenden, die alltäglich mit der elektronischen Akte arbeiten, anzubieten. Nur durch die Sensibilisierung der Nutzenden können Unklarheiten, wie sie bereits bei der Personensuche in der aktuellen elektronischen Akte teilweise vorherrschen, in dem neuen System direkt von Beginn an vermieden werden. Die Kontrolle im Nachgang ist wichtig, aber allein kein ausreichendes Mittel, um die datenschutzkonforme Nutzung zu gewährleisten. In Bezug auf das

108 OVG Münster, Urteil vom 3. September 1979 – VI A 2223/78

künftige Verbund-DMS werde ich meine Beratung auch im nächsten Jahr fortsetzen.

Querverweise:

7.3 Internetrecherche für die nationale Sicherheit – Auch hier gibt es Grenzen!, 9.1.9 Kontrolle des Gemeinsamen Terrorabwehrzentrums

9.1.8 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst

Im Berichtsjahr habe ich beim Bundesamt für den Militärischen Abschirmdienst (BAMAD) die Datenverarbeitung im Rahmen des Visa-Konsultationsverfahrens (ViKon) kontrolliert. Ein weiteres Thema meiner Kontroll- und Beratungstätigkeit war der Umfang der Vollanbindung des BAMAD an das Nachrichtendienstliche Informationssystem (NADIS) des Verbundes der Verfassungsschutzbehörden von Bund und Land. Die Fortführung meiner intensivierten Kontrolltätigkeit zeigt mir, dass es auch beim dritten Nachrichtendienst des Bundes einen umfangreichen Reformbedarf im Bereich der Gesetzgebung und Prozessabläufe gibt.

Kontrolle des ViKon beim BAMAD

Ich habe die Verarbeitung von personenbezogenen Daten durch das BAMAD im Zusammenhang mit dem ViKon inklusive der damit beim BAMAD verbundenen Dateien geprüft. Das ViKon gemäß § 73 Abs. 1, 3 Aufenthaltsgesetz (AufenthG) dient dazu, deutschen Auslandsvertretungen eine sicherheitsbehördliche Überprüfung von Visumantragstellern bestimmter Staatsangehörigkeiten im Vorfeld der Visumerteilung zu ermöglichen. Dazu werden durch das Bundesverwaltungsamt (BVA) die Daten der antragstellenden Person an die im Gesetz benannten Sicherheitsbehörden übermittelt, die dann das Vorliegen von Ausschlussgründen und/oder sonstiger Sicherheitsbedenken prüfen. Das BVA übermittelt die Rückmeldung der Behörden zu ggf. vorliegenden Erkenntnissen zu der Person an die Auslandsvertretungen, die über die Erteilung des Visums entscheiden.

Neben den technischen Zusammenhängen, den Grundsätzen der Datenübermittlungen zwischen den am Visumverfahren beteiligten sog. Zentralbehörden (BVA, Bundesamt für Migration und Flüchtlinge, Auslandsvertretungen, Ausländerbehörden) und dem Realeinsatz des Verfahrens vor Ort lag ein weiterer Schwerpunkt der Kontrolle auf der Prüfung, ob datenschutzrechtliche Mängel und/oder Verstöße bei der Annahme von Versagungsgründen oder sonstige Sicherheitsbedenken i. S. d. § 73 Abs. 1 AufenthG durch die Fachabteilungen des BAMAD bestehen. Ich musste feststellen, dass mehrere Verarbeitungen von personenbezogenen Daten gegen datenschutzrechtliche Vorschriften verstoßen. Die fehlende Möglichkeit, eine Verarbeitungssperre in einer Datei des BAMAD zu setzen, die dazu führen soll, dass löschreife Daten nicht mehr durch die operative Fachabteilung verarbeitet werden können, habe ich beanstandet. Zudem habe ich wegen der zu langen Speicherdauer der Daten in den verschiedenen Dateien des BAMAD eine Beanstandung ausgesprochen. Des Weiteren habe ich verschiedene Defizite festgestellt, die das ViKon im Allgemeinen betreffen und die ich an das BVA berichten werde, welches die zentrale Rolle in diesem Verfahren spielt. Positiv hervorzuheben ist, dass aufgrund meines Kontrollberichtes bereits kurzfristig einige datenschutzrechtliche Mängel und Verstöße abgestellt worden sind. Im Übrigen hat das zuständige Bundesministerium der Verteidigung zugesichert, weitere Maßnahmen zur Umsetzung meiner Verbesserungsvorschläge zu prüfen.

Anbindung des BAMAD an NADIS

Das NADIS ist (bislang) eine gemeinsame Datei des Verbundes aus Bundesamt für Verfassungsschutz und Landesbehörden für Verfassungsschutz (VS-Verbund). Es dient der gegenseitigen Unterrichtung der Verfassungsschutzbehörden untereinander. NADIS steht den Behörden zur Verfügung, um Speicherungen und Verknüpfungen der gewonnenen und ausgewerteten Informationen vorzunehmen. Daneben spielt das NADIS auch eine große Rolle bei der Auswertung der vorliegenden Informationen, da oftmals erst durch die hier erkennbaren Verbindungen einzelner Informationen Zusammenhänge offenbar werden. Im Rahmen der Anhörungsverfahren zur Änderung der zum Verfahren gehörigen Dateianordnungen (31. TB Nr. 9.4.10) habe ich den vorgesehenen Umfang der Vollanbindung des BAMAD an das NADIS kritisiert. Hierdurch würde das BAMAD Zugriff auf den gesamten Datenbestand des VS-Verbundes erhalten. Eine solche vollständige Öffnung aller Datensätze des VS-Verbundes ist meiner Ansicht nach auf der Grundlage der im Jahr 2021 hierfür geschaffenen Vorschriften nicht möglich: Ich vertrete die Auffassung, dass in der Eingabe eines Datensatzes mittels einer Speicherung in NADIS bereits eine Offenlegung in der Form der Übermittlung an die an NADIS teilnehmenden Behörden zu sehen ist. Das Bundesverfassungsgericht (BVerfG) hat in seiner jüngsten Rechtsprechung konkret definierte Schwellen in den Rechtsgrundlagen gefordert, welche die Übermittlungen durch die Nachrichtendienste ermöglichen. An solchen fehlt es aber meiner Meinung nach in den dem NADIS zugrundeliegenden Vorschriften der § 6 Bundesverfassungsschutzgesetzes und § 3 des Gesetzes über den Militärischen Abschirmdienst (MADG). Neben dem Umfang der im NADIS vorhandenen Daten

ist auch zu berücksichtigen, dass mittels NADIS automatisierte Analysen über alle eingespeicherten Daten durchgeführt werden können. Bei einem Verfahren des automatisierten Abrufs kann der Nutzende letztlich auf den gesamten vorhandenen Datenbestand zugreifen und zusammenhängend analysieren. Ein solcher Vorgang stellt einen solch intensiven Eingriff in das Recht auf informationelle Selbstbestimmung dar, dass dieser allenfalls unter bestimmten engen formalen und inhaltlichen Grenzen zugelassen werden kann, die wiederum in einer gesetzlichen Grundlage definiert sein müssen. Entsprechende Anforderungen hierzu hat das BVerfG in seiner Entscheidung vom 16. Februar 2023 zu polizeilichen Datenanalysen formuliert. Die Bundesregierung hat die Vollanbindung des BAMAD an das NADIS trotz meiner vorgebrachten Bedenken umgesetzt und auch die Chance, die notwendigen Anpassungen der Vorschriften im aktuellen Gesetzgebungsverfahren vorzunehmen, ungenutzt verstreichen lassen. Ich habe daher die Gelegenheit genutzt, meine Kritik in eine Stellungnahme an das BVerfG, bei dem derzeit eine Verfassungsbeschwerde u. a. gegen die Rechtsgrundlagen zum NADIS anhängig ist, einzubringen.

Umfangreicher Reformbedarf auch beim BAMAD

Im Rahmen meiner datenschutzrechtlichen Beratung hinsichtlich der Datenverarbeitung zu Reservistinnen und Reservisten hatte ich eine gesetzliche Klarstellung hinsichtlich der Zuständigkeit von Reservistinnen und Reservisten zwischen BAMAD und BfV empfohlen. Ferner hatte ich in meiner Kontrolle im Bereich der Observation des BAMAD (31. TB Nr. 9.4.10) die Verbesserung von Prozessabläufen angeregt. Aufgrund der Rechtsprechung des BVerfG stehen für die Nachrichtendienste des Bundes insbesondere auch im Bereich der Observation umfangreiche Reformen an, in deren Rahmen auch meine Empfehlungen Berücksichtigung finden sollen. Ich werde daher im zweiten Teil der Reform des Nachrichtendienstrechts diese Empfehlungen einbringen und auch für die Schaffung eines eigenständigen MADG werben, um eine bessere Verständlichkeit und Normenklarheit des Gesetzestextes zu erreichen.

Querverweise:

3.3 Gesetzgebung im Sicherheitsbereich

9.1.9 Kontrolle des Gemeinsamen Terrorismusabwehrzentrums

Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) ist eine behördenübergreifende Kooperationsplattform. In unterschiedlichen Formaten finden sich dort teilweise täglich Vertreterinnen und Vertreter von 40 Sicherheitsbehörden zusammen. Eine eigene gesetzliche Grundlage für diesen Austausch von Informationen gibt es nicht. Der Informationsaustausch wird auf die allgemeinen Übermittlungsregelungen gestützt.

Im Rahmen einer Kontrolle habe ich geprüft, ob sich die im GTAZ vertretenen Bundesbehörden (Bundeskriminalamt, Bundesamt für Verfassungsschutz, Bundesnachrichtendienst, Bundesamt für den Militärischen Abschirmdienst, Bundespolizei, Zollkriminalamt, Generalbundesanwalt und Bundesamt für Migration und Flüchtlinge) an die bestehenden Übermittlungsvorschriften halten und ob der Informationsaustausch im GTAZ von diesen Übermittlungsvorschriften umfasst ist.

Für meine Kontrolle habe ich ein Kontrollteam gebildet, welches aus Mitarbeitenden der für die betroffenen Bundesbehörden zuständigen Referate bestand. Dieses Kontrollteam hat im Rahmen von mehreren Vorortbesuchen an vielen Sitzungen des GTAZ teilgenommen, wozu auch kurzfristig einberufene Sitzungen zu operativen Gefährdungslagen zählten.

Die Kontrolle hat ergeben, dass nicht jedes Arbeitsformat mit den datenschutzrechtlichen Bestimmungen in Einklang zu bringen ist. So habe ich die Konzeption einer Arbeitsgruppe beanstandet. Diese sieht vor, dass sich täglich alle 40 im GTAZ vertretenen Behörden zu Sachverhalten austauschen, ohne dass bei den einzelnen Beiträgen explizit geprüft wird, ob die Weitergabe der Informationen und insbesondere der personenbezogenen Daten aufgrund der bestehenden gesetzlichen Übermittlungsvorschriften zulässig ist. Darüber hinaus habe ich Praxisempfehlungen zur Stärkung des Datenschutzes in den anderen Arbeitsgruppen ausgesprochen. So habe ich die Erstellung eines einheitlichen Datenschutzkonzeptes empfohlen, die Etablierung einer weisungsunabhängigen Ansprechperson für den Datenschutz in den Arbeitsgruppen des GTAZ und eine Erhöhung des Dokumentationsstandards in den Sitzungen der Arbeitsgruppen.

Gegenüber der Bundesregierung, die die Schaffung von expliziten Rechtsgrundlagen für die Gemeinsamen Zentren wie u. a. das GTAZ in den Koalitionsvertrag aufgenommen hat, habe ich mich ausdrücklich für die Schaffung eigener klarer gesetzlicher Regelungen ausgesprochen und ein entsprechendes datenschutzrechtliches Beratungsangebot unterbreitet. Mit einer Fraktion der Bundesregierung habe ich diesbezüglich auch bereits Gespräche geführt. Leider hat die Bundesregierung Abstand davon genommen, im Rahmen der aktuellen Novellierung der Sicherheitsrechtslage entsprechende Regelungen für die Gemeinsamen Zentren zu schaffen.

9.1.10 Kontrolle des Bereichs Auswertung im BND

Die neue Struktur des Bundesnachrichtendienst (BND) bündelt die gesamte nachrichtendienstliche Auswertung der erhobenen Erkenntnisse in einem eigenen Organisationsbereich. Ich habe unterschiedliche Organisationseinheiten dieses Bereichs kontrolliert und überprüft, ob bei den dortigen Tätigkeiten die Datenschutzregelungen eingehalten werden.

In dem Organisationsbereich Auswertung des BND laufen alle erhobenen Informationen zusammen. Aufgabe der Auswertenden ist es, die Informationen in Bezug auf ihren Erkenntnisgehalt zu sichten, einzuordnen und zu bewerten. Sodann werden die Informationen zu eigenen Produkten weiterverarbeitet. So werden beispielsweise umfassende Analysen erstellt, Meldungen an das Bundeskanzleramt und weitere Ressorts verfasst, aber auch Schreiben an andere Stellen gefertigt. Bei den Schreiben handelt es sich regelmäßig um Erkenntnismitteilungen zu vorliegenden Sachverhalten oder um die Beantwortung von an den BND gerichteten Erkenntnisanfragen.

Mit meiner Kontrolle habe ich einen Schwerpunkt auf die Facharbeit des BND gelegt, um mir einen Überblick über die Prozesse bei der Verarbeitung von personenbezogenen Daten in diesem wichtigen Bereich zu verschaffen. Zudem diente die Kontrolle dem Zweck, gegebenenfalls bestehende datenschutzrechtliche Missstände zu detektieren und eine Abschaltung dieser herbeizuführen. Hierzu habe ich mir zunächst in einem Informationstermin alle Abläufe sowie verwendeten Verarbeitungssysteme vorstellen lassen. In einem Kontrolltermin habe ich mir sodann von der Auswertung erstellte Produkte vorlegen lassen und geprüft, ob die hierin verwendeten personenbezogenen Daten in rechtmäßiger Art und Weise verarbeitet wurden. Zusätzlich habe ich auch Speicherungen zu in den Produkten genannten Personen in Systemen des BND überprüft.

Meine Kontrolle hat ergeben, dass derzeit keine datenschutzrechtlichen Defizite bei der Arbeit der Auswertung vorliegen. Ich habe lediglich drei Praxisempfehlungen ausgesprochen und meine Kontrolle ohne Beanstandungen abgeschlossen.

9.1.11 Europaweit koordinierte Kontrolle – Übermittlungen an Europol zu Minderjährigen im Fokus

Auf Basis der Europol-Verordnung können die Polizeibehörden der Mitgliedstaaten Informationen an Europol übermitteln. Wenn dies Minderjährige betrifft, ist dieser Vorgang besonders sensibel. Das Coordinated Supervision Committee (CSC) hat daher eine länderübergreifende Überprüfung dieser Übermittlungen angestoßen. Ich habe hierbei wesentliche Beiträge zur europäischen und deutschen Koordinierung von Kontrollmaßnahmen geleistet.

Strafverfolgungsbehörden können unter sehr spezifischen Voraussetzungen Daten Minderjähriger an Europol übermitteln. In Deutschland ist die zentrale Schnittstelle zu Europol die deutsche Europol National Unit beim Bundeskriminalamt. Der Europäische Datenschutzbeauftragte stellte bei einer Kontrolle von Europol fest, dass die Übermittlungen von Daten Minderjähriger an Europol Anlass zur Überprüfung gaben.

Das CSC hat daraufhin beschlossen, europaweite Kontrollen anzustoßen und zu koordinieren. Wie bereits in meinem 31. Tätigkeitsbericht (Nr. 3.3.4) mitgeteilt, arbeiten meine Mitarbeitenden im CSC intensiv mit, insbesondere als stellvertretender Vorsitz. Europaweit sind derzeit zahlreiche Datenschutzaufsichtsbehörden mit der Kontrolle von Übermittlungen von Daten Minderjähriger an Europol befasst.

Für Deutschland wurde das Thema durch mich zusammen mit der Ländervertretung in die Datenschutzkonferenz eingebracht. Ziel dabei war, nicht nur auf europäischer Ebene, sondern auch auf nationaler Ebene ein koordiniertes Vorgehen und vergleichbare Ergebnisse zu ermöglichen. Um die Durchführung der Kontrollen in Deutschland zu ermöglichen, wurde beispielsweise ein gemeinsamer Fragebogen zur Nutzung durch die Aufsichtsbehörden entwickelt. Derzeit werden europa- und deutschlandweit – so auch durch mich – entsprechende Prüfungen durchgeführt und die Ergebnisse zusammengetragen.

Querverweise:

4.2.1 Allgemeiner Bericht

9.2 Allgemeine Kontrollen und Beratungsbesuche

Kontroll- und Beratungsbesuche sind ein wesentliches Element der datenschutzrechtlichen Aufsichtstätigkeit, da sie einen wichtigen Einblick in die Praxis der Datenverarbeitung ermöglichen. Um einen unmittelbaren Eindruck von den tatsächlichen Abläufen und Gegebenheiten zu bekommen, kontrollieren meine Mitarbeiterinnen und Mitarbeiter daher oft direkt vor Ort. Dies gilt auch, wenn der Weg mal etwas weiter ist, wie z. B. bei den deutschen Auslandsvertretungen.

Unabhängig von der kontrollierten Stelle werden Kontrollen teilweise als allgemeine Querschnittskontrollen durchgeführt, oft aber auch schwerpunktbezogen mit Blick auf besondere datenschutzrechtliche Fragestellun-

gen. Teilweise erfolgen Kontrollen aber auch anlassbezogen, z. B. nach Hinweisen von Bürgerinnen und Bürgern oder nach Medienberichten.

Immer sollte eine Kontrolle die datenverarbeitende Stelle auch ganz generell hinsichtlich eines datenschutzfreundlichen Umgangs mit personenbezogenen Daten sensibilisieren. Daher verbinde ich alle Kontrollen auch immer mit einem Beratungsangebot für die kontrollierten Stellen. Damit trage ich dazu bei, dass diese noch besser von sich aus in die Lage versetzt werden, bereits eingerichtete Prozesse kontinuierlich auf ihre Datenschutzfreundlichkeit zu überprüfen. Dies trägt nachhaltig zu einem Schutz von personenbezogenen Daten bei.

9.2.1 Beratungs- und Kontrollpraxis bei Messengerdiensten

Messengerdienste haben sich in den letzten Jahren zu einem der meist genutzten Kommunikationsmittel entwickelt. Sie vereinfachen die Kommunikation im Privaten und der Arbeitswelt erheblich, bringen aber auch Herausforderungen für den Datenschutz und die Privatsphäre der Nutzenden mit sich. In diesem Jahr habe ich Kontroll- und Beratungsbesuche durchgeführt, um die Diensteanbieter gezielt für die datenschutzrechtlichen Herausforderungen zu sensibilisieren.

Messengerdienste sind aus unserem Alltag nicht mehr wegzudenken und gewinnen auch im Umfeld der Bundesverwaltung an Bedeutung. Angesichts dessen habe ich in diesem Jahr meine Aufsichtstätigkeit im Bereich der Messengerdienste verstärkt (Nr. 8.4). Wesentlicher Teil dieser Tätigkeit sind Beratungs- und Kontrollbesuche bei in Deutschland niedergelassenen Unternehmen und öffentlichen Stellen des Bundes, die Messengerdienste erbringen.

Bei den Besuchen kontrolliere ich gezielt technische oder rechtliche Schwerpunkte. In drei Beratungs- und Kontrollbesuchen habe ich mich in diesem Jahr in rechtlicher Hinsicht insbesondere mit der Frage möglicher Rechtsgrundlagen des freiwilligen Einsatzes von Messengerdiensten als Kommunikationsmittel innerhalb öffentlicher Stellen des Bundes beschäftigt. Ebenso spielte die Richtigkeit und Vollständigkeit datenschutzrechtlich erforderlicher Dokumentationen, wie Datenschutzerklärungen, eine wichtige Rolle. In technischer Hinsicht habe ich insbesondere das Bestehen geeigneter und hinreichender technischer und organisatorischer Maßnahmen zum Umgang mit einem Ransomware-Befall geprüft.

Ich konnte feststellen, dass die kontrollierten hiesigen privaten Diensteanbieter datenschutzrechtlich gut aufgestellt sind. Gleichwohl habe ich in meinen Beratungs- und Kontrollbesuchen einige datenschutzrechtliche Mängel aufgedeckt, die bei den Diensteanbietern durch Anpassungen zu Verbesserungen des Datenschutzes führten.

Im direkten Anschluss an die Kontrollen habe ich den Unternehmen und öffentlichen Stellen bei meinen Besuchen im Rahmen eines offenen Austauschs die Möglichkeit gegeben, auch über die Kontrollgegenstände hinausgehende Fragen zu besprechen. Dabei konnte ich auch erfahren, welche Themen und Fragestellungen die Marktteilnehmer aktuell bewegen.

Meine Beratungspraxis habe ich im Rahmen des diesjährig erstmalig durchgeführten „Jour fixe Messenger“ weiter ausgebaut und verstärkt.

Darüber hinaus habe ich im Rahmen des europäischen Projektes „Support Pool of Experts“ zusammen mit einem externen Experten einen standardisierten Prüfkatalog zur einheitlichen Evaluation von Frontendsystemen von Messengerdiensten entwickelt.

Querverweise:

8.4 Messengerdienste, 9.2.2 Kontrolle als Chance – Aus der Beratungspraxis der Telekommunikations- und Postanbieter

9.2.2 Kontrolle als Chance – Aus der Beratungspraxis der Telekommunikations- und Postanbieter

Ich möchte Datenschutz in die Fläche tragen und vor Ort präsent sein. Mein Leitgedanke ist: Wo entfalte ich einen bestmöglichen Wertbeitrag für mehr Datenschutz?

Die Kontrolle und Beratung bei Unternehmen sind wichtige Teile meiner Aufsichtstätigkeit. Bei großen Unternehmen kontrolliere ich meist gezielt bestimmte Schwerpunkte. Dies gilt besonders, wenn es Hinweise auf datenschutzrechtliche Defizite gibt. Mir ist aber wichtig, mich nicht allein auf einige wenige Unternehmen zu konzentrieren, sondern auch in der Breite zu wirken. Deshalb achte ich darauf, zusätzlich auch bei kleinen und mittleren Unternehmen und in verschiedenen Regionen vor Ort zu sein – auch ganz ohne besonderen Anlass. Ich möchte damit zeigen, dass mein Haus, obwohl nur an zwei Standorten beheimatet, in ganz Deutschland präsent ist.

Insbesondere im Postbereich sind viele regionale Unternehmen tätig – vom alternativen Briefdienstleister bis zum Fahrradkurier. Allerdings gelten für diese Unternehmen bis auf wenige Ausnahmen die gleichen datenschutzrechtlichen Vorgaben wie für ihre großen Pendants. Bei einem kontrollierten Fahrradkurier

konnte ich einen guten Eindruck von der oft schnell auszuführenden Tätigkeit und der damit verbundenen Datenverarbeitung gewinnen. Dabei habe ich einen Schwerpunkt auf die Sensibilisierung der Beschäftigten für datenschutzrechtliche Themen gelegt, was sehr gut angenommen wurde.

Diese Kontroll- und Beratungstermine sind für mich essentiell. Sie sind aber auch für die verantwortlichen Stellen ein wichtiger Ankerpunkt für eigene unternehmensinterne Prüfungen. Unternehmen müssen sich fragen: Wo stehen wir im Datenschutz? Was können wir besser machen? Eine Kontrolle kann bestenfalls auch die Bestätigung sein, dass man gut aufgestellt ist und sich die Investition in den Datenschutz gelohnt hat.

Kontrollen müssen nicht immer „weh tun“ – ganz im Gegenteil werden fast alle Kontrollen von den kontrollierten Stellen rückblickend als hilfreich wahrgenommen. Ich möchte ein starker Beratungspartner für Unternehmen sein. Mir ist wichtig, dass meine Mitarbeiterinnen und Mitarbeiter mit ihrer Expertise unterstützen und konkrete Empfehlungen aussprechen. Sensibilisierung und Verbesserung des Status Quo stehen hier also im Vordergrund. Klar ist aber auch, dass erkannte datenschutzrechtliche Defizite schnellstmöglich behoben werden müssen.

Oft führt bereits die Ankündigung einer Kontrolle dazu, dass sich Unternehmen (erneut) sehr intensiv mit dem Datenschutz beschäftigen. So erhielt ich just wenige Tage vor einem angekündigten Kontrollbesuch zwei meldepflichtige Datenschutzvorfälle nach § 169 Telekommunikationsgesetz. Schon die seriöse Kontroll-Vorbereitung förderte hier also Mängel zutage, die dem Unternehmen vorher unbekannt waren. In meinem Kontrollbericht musste ich dann keine weiteren schwerwiegenden Defizite feststellen.

Soweit die Kontrollberichte veröffentlicht werden konnten, finden Sie diese auf meiner Webseite.

(QR-Code klicken oder scannen)

Besonderen Fokus lege ich bei Kontrollen regelmäßig auf die Umsetzung der Betroffenenrechte wie z. B. Auskunft, Berichtigung oder Löschung. In einem Fall konnten meine Hinweise auf kleine, aber notwendige Anpassungen bei einem Bestellformular und den Datenschutzhinweisen von einem Telekommunikationsunternehmen schnell und einfach umgesetzt werden. Bei einem Postdienstleister bin ich ausgehend von einer Vor-Ort-Kontrolle etwas tiefer in die Prüfung der Kommunikation des Unternehmens mit den betroffenen Personen eingestiegen. In einem kooperativen Abstimmungsprozess konnten die verwendeten Dokumente verbessert werden. Kundinnen und Kunden können sich in diesen Fällen nun besser informieren und ihre Betroffenenrechte gut wahrnehmen.

Querverweise:

9.2.1 Beratungs- und Kontrollpraxis bei Messengerdiensten

9.2.3 Kontrolle der steuerlichen Identifikationsnummer beim Bundeszentralamt für Steuern

In einer zunehmend digitalen Welt wird auch die Frage der eindeutigen Personenidentifizierbarkeit immer wichtiger. In Deutschland ist insoweit das Steuerrecht Vorreiter: Bereits seit mehr als 15 Jahren steht mit der Steuer-ID ein einheitliches und dauerhaftes Merkmal zur Verfügung, mit dem Bürgerinnen und Bürgern gegenüber Steuerbehörden identifiziert werden. Durch das Registermodernisierungsgesetz wurde nun die Voraussetzung geschaffen, die Steuer-ID in vielfältiger Weise auch außerhalb des Steuerrechts als einheitliches, bereichsübergreifendes Personenkennzeichen im Sinne des Identifikationsnummerngesetzes in diversen nationalen Registern einzusetzen. Umso wichtiger ist es, dass die Steuer-ID datenschutzkonform verarbeitet wird.

Die Nutzung des steuerlichen Identifikationsmerkmals (kurz Steuer-ID) außerhalb des Steuerrechts beschäftigt mein Haus bereits seit Jahren. Immer wieder habe ich mich kritisch in datenschutzrechtliche Diskussionen und in Stellungnahmen zu Gesetzesvorhaben eingebracht und auf die verfassungsrechtlichen Probleme hingewiesen. Zudem habe ich intensiv auf die Einführung notwendiger Schutzmechanismen gedrängt. Insbesondere das sogenannte Datencockpit soll Transparenz schaffen und allen Bürgerinnen und Bürgern die Möglichkeit geben, die Verwendung ihrer Steuer-ID und die hiermit einhergehenden Datenübermittlungen nachzuvollziehen (29. TB Nr. 5.1 und 31. TB Nr. 8.6). Nun war es an der Zeit, einen weiteren Fokus auf die Datenbank zu richten, in der die Steuer-ID seit dem Jahr 2007 durch das Bundeszentralamt für Steuern (BZSt) vergeben und gespeichert wird. Insbesondere die Fragen, zu welcher Zeit und unter welchen Voraussetzungen eine Steuer-

ID wieder gelöscht wird, wurden im Berichtszeitraum durch mein Haus geprüft.[109]

Das zuständige BZSt löscht eine Steuer-ID derzeit nur, wenn festgestellt wird, dass eine Befugnis zu deren Vergabe und Speicherung zu keiner Zeit bestanden hat. Darüber hinaus sind regelmäßige Löschungen nur vorgesehen, sobald die betroffene Person verstirbt. In Anknüpfung an § 4 der Verordnung zur Vergabe steuerlicher Identifikationsnummern (kurz StIdV) soll eine Löschung spätestens 20 Jahre nach dem Versterben des Steuerpflichtigen erfolgen. Diese restriktive Sichtweise des BZSt lässt meiner Einschätzung nach Zweifel aufkommen, dass die Steuer-ID-Datenbank dem allgemeinen Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO) und im Speziellen dem Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO) entspricht. Danach dürfen personenbezogene Daten nur solange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dementsprechend regelt § 4 StIdV bereits heute, dass die beim BZSt nach § 139b Abs. 3 AO gespeicherten Daten zu löschen sind, wenn sie zur Erfüllung der gesetzlichen Aufgaben der Finanzbehörden nicht mehr erforderlich sind.

Dies kann meiner Einschätzung nach insbesondere dann der Fall sein, wenn der Steuerpflichtige ins Ausland verzieht, ohne zukünftig zumindest der beschränkten Steuerpflicht in Deutschland zu unterliegen. Auch unter Berücksichtigung steuerlicher Nachbearbeitungsfristen entfällt die Erforderlichkeit der Steuer-ID in diesem Fall absehbar. Dabei ist entscheidend, dass die in Art. 5 Abs. 1 lit. e) DSGVO benannte „Erforderlichkeit" der fortdauernden Datenspeicherung für die legitimen Verarbeitungszwecke positiv festgestellt werden muss. Die bloße Möglichkeit, dass der ins Ausland Verziehende früher oder später nach Deutschland zurückkehren könnte, reicht insoweit für ein Vorhalten seiner Steuerdaten, auch der für ihn vergebenen Steuer-ID, nicht aus. Vielmehr ist in diesem Fall eine unzulässige Vorratsdatenspeicherung anzunehmen.

Zudem ist bei der Entscheidung über die fortdauernde Erforderlichkeit der Speicherung einer Steuer-ID zu berücksichtigen, dass diese schon lange nicht mehr nur steuerrechtlich genutzt wird. Mit der Registermodernisierung geht absehbar die Hinzuspeicherung der Steuer-ID in diversen nationalen Registern einher. Die dortigen und nicht harmonisierten Löschfristen bilden zusätzliche Herausforderungen für die Bestimmung einer allgemeinen Frist zur Löschung der Steuer-ID. Hierzu befinde ich mich weiterhin im konstruktiven Austausch mit dem BZSt und werde auf die zeitnahe Einführung einer datenschutzkonformen Regelung dringen. Insoweit erscheint eine Überarbeitung der StIdV erforderlich, welche weiterhin nur auf die steuerliche Nutzung der Steuer-ID abstellt und daher insbesondere einer Anpassung an die Entwicklungen zur Registermodernisierung bedarf. Ungeachtet der inzwischen heterogenen Anwendungsfälle der Steuer-ID dürfen die datenschutzrechtlichen Grundsätze des Art. 5 DSGVO und hier insbesondere der Grundsatz der Speicherbegrenzung nicht unterlaufen werden.

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.

Querverweise:

8.2 Registermodernisierung

9.2.4 Datenschutzrechtlicher Beratungs- und Kontrollbesuch bei den Auslandsvertretungen in Kasachstan

Im September 2022 haben meine Mitarbeitenden die Auslandsvertretungen in Astana und Almaty besucht, insbesondere um die Datenverarbeitungsvorgänge nach der europäischen Visa-Verordnung zu überprüfen. Nach weiteren sich dem Besuch anschließenden Gesprächen mit dem Auswärtigen Amt (AA) wurde die Kontrolle im Berichtsjahr abgeschlossen.

Zum Zweck der Visabearbeitung bestehen mehrere IT-Systeme nebeneinander. So erfolgt die Eingabe an den Auslandsvertretungen im System RK-Visa. Im Rahmen des automatisierten Visumverfahrens werden die Daten an das Bundesverwaltungsamt (BVA) übermittelt, das als nationale Kopfstelle das nationale Visa-Informationssystem (VIS) und den Knotenpunkt zum EU-VIS bereitstellt.

Durch diese Verzahnung konnte während der Vor-Ort-Kontrolle die genaue datenschutzrechtliche Verantwortlichkeit nicht geklärt werden, da sowohl das AA als auch das BVA an verschiedenen Stellen im Verfahren als Verantwortliche auftreten. Ich habe daher dem AA aufge-

109 Kontrollbericht vom 2. August 2023, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Kontrollberichte/Allgemeine-Verwaltung/Kontrolle-BZSt.html

tragen, die Verantwortlichkeit im Sinne von Art. 4 Nr. 7 DSGVO zu klären. Letztendlich gaben das AA und das BVA an, dass es sich um eine gemeinsame Verantwortlichkeit im Sinne des Art. 26 DSGVO handele und eine entsprechende Vereinbarung ausgearbeitet werde.

Da bei der Visabearbeitung unterschiedliche Systeme zum Einsatz kommen, erfolgte im Rahmen der Kontrolle auch eine differenzierte Betrachtung der Protokollierung innerhalb dieser Systeme. Die vom BVA vorgenommene Protokollierung entspricht den Vorgaben des Art. 34 VIS-Verordnung. Die Aufzeichnungen beim AA wiesen hingegen Mängel auf, die im Rahmen einer Systemüberarbeitung behoben werden sollen.

Während meiner Kontrolle vor Ort stellte ich an beiden Auslandsvertretungen fest, dass Maßnahmen zur Sicherheit der Verarbeitung personenbezogener Daten zu verstärken sind, um einen unbefugten Zutritt und Zugriff zu vermeiden. Beide Auslandsvertretungen setzten dies durch geeignete technisch-organisatorische Maßnahmen umgehend um. Weiterhin machte ich auf einen Sensibilisierungsbedarf der Beschäftigten aufmerksam, der insbesondere die lokalen Ortskräfte betrifft, da das Datenschutzniveau der DSGVO deutlich über dem Datenschutzverständnis in Kasachstan liegt.

Das AA hat auf meine Empfehlung seit einigen Jahren einen Datenschutzbeauftragten für das gesamte Haus und sogenannte Datenschutzansprechpersonen an den einzelnen Auslandsvertretungen etabliert. Da diese Rolle an den besuchten Vertretungen u. a. aufgrund einer Vielzahl weiterer Aufgaben nach meinen Feststellungen in nicht ausreichendem Maße ausgefüllt wurde, soll das AA künftig auf ein aktiveres Rollenverständnis hinwirken, um den Datenschutz an den Auslandsvertretungen zu gewährleisten.

Neben den Auslandsvertretungen besuchte ich auch das Visazentrum des für die deutschen Auslandsvertretungen in Kasachstan tätigen externen Dienstleisters in Almaty. Hier fiel insbesondere die fehlende Kennzeichnung der durchgeführten Videoüberwachung auf. Dieser Mangel wurde abgestellt. Die pandemiebedingt ausgefallenen regelmäßigen Inspektionen der externen Dienstleister durch die Auslandsvertretung sollen wieder aufgenommen werden, um die Einhaltung des Datenschutzes zu überprüfen und sicherzustellen.

Externer Dienstleister

Der europäische Visakodex (dort Art. 43) sieht vor, dass die Mitgliedstaaten bestimmte Aufgaben im Rahmen der Beantragung eines Visums zusammen mit einem externen Dienstleister erbringen können. Dies betrifft insbesondere die Erfassung der Daten und Entgegennahme der Anträge (einschließlich der biometrischen Identifikatoren) und Weiterleitung der Anträge an die Konsulate. Deutschland macht davon in verschiedenen Ländern Gebrauch. Als Ausgleich für die damit einhergehenden datenschutzrechtlichen Risiken sind die Mitgliedsstaaten (in Deutschland das AA) verpflichtet, die Maßnahmen zur Einhaltung der Datenschutzbestimmungen beim externen Dienstleister zu überwachen. Ob diese Verpflichtung ordnungsgemäß wahrgenommen wird, werde ich weiter in regelmäßigen Abständen überprüfen.

9.2.5 Datenschutzrechtlicher Beratungs- und Kontrollbesuch an der Auslandsvertretung Dakar

Der Einsatz sog. „Kooperationsanwälte“ im Rahmen von Ermittlungen deutscher Behörden in Ländern außerhalb der EU bedarf einer sorgsamen Abwägung zwischen dem damit verfolgten Zweck und den dadurch für die jeweils betroffenen Personen entstehenden Risiken. Diese Thematik und weitere datenschutzrelevante Sachverhalte habe ich im Rahmen eines Kontroll- und Beratungsbesuchs der deutschen Botschaft in Dakar überprüft.

Die deutschen Auslandsvertretungen können in Einzelfällen Kooperationsanwälte zur Aufklärung der örtlichen Rechts- und Tatsachenlage (§ 3 Abs. 3 Konsulargesetz) beauftragen. Der sorgsame Umgang mit den Daten betroffener Personen ist in einigen Fallgestaltungen (z. B. bei der Überprüfung von Fluchtgründen bei der Asylbeantragung) besonders wichtig. Einerseits kann die Offenbarung bestimmter personenbezogener Daten sowohl die betroffene Person als auch deren Verwandte und Bekannte im Drittland gefährden. Außerdem kann die Offenbarung auch dem eigentlichen Zweck der Aufklärung entgegenlaufen, z. B. indem dadurch die Gründe für einen sonst nicht bestehenden Asylanspruch erst geschaffen werden. Die Einhaltung des europäischen Datenschutzstandards ist auch aus diesen Gründen bei der Beauftragung der Anwälte zu gewährleisten. Ob dies der Fall ist, habe ich exemplarisch in der deutschen Botschaft in Dakar untersucht. Die Botschaft bearbeitet neben entsprechenden Fällen den Senegal betreffend auch zahlreiche Fälle aus dem Nachbarland Gambia, wo nur ein unzureichendes Urkundswesen besteht. Zur Überprüfung des Inhalts entsprechender Urkunden greift die Botschaft unter anderem auf die Dienstleistungen einer gambischen Anwältin zurück. Meine Mitarbeitenden haben hierzu auch Gespräche mit Kooperationsanwälten in Dakar führen können. Hinsichtlich der rechtlichen Ausgestaltung der Beauftragung der Anwälte vor Ort und der Wahl der Kommunikationsmittel befinde ich mich mit dem Auswärtigen Amt im Austausch.

Darüber hinaus erfolgte bei meinem Besuch eine allgemeine Betrachtung der Verarbeitung personenbezogener Daten in der Auslandsvertretung. Hierzu gehören u. a. die technisch-organisatorischen Maßnahmen oder der Umgang mit Datenschutzverletzungen und Betroffenenrechten.

Der Kontrollbericht wird aktuell noch abgestimmt, sodass der formelle Abschluss der Kontrolle erst im Jahr 2024 erfolgen wird.

9.2.6 Fingerabdrucknahme von Asylbewerbenden und Geflüchteten

Mit dem europäischen IT-System Eurodac werden Fingerabdrücke von Asylbewerbenden und Geflüchteten europaweit erhoben, zentral gespeichert und abgeglichen. Ob dies datenschutzkonform geschieht, haben meine Mitarbeitenden beim Bundesamt für Migration und Flüchtlinge (BAMF) geprüft.

Die Verarbeitung biometrischer Daten, wie Fingerabdrücken, kann ein effektives Mittel der Identifizierung darstellen, bedeutet aber andererseits einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung. Die Verordnung (EU) Nr. 603/2013 (sog. EURODAC-VO) sieht daher verschiedene datenschutzrechtliche Schutzmaßnahmen vor, um eine rechtskonforme Verarbeitung der Fingerabdruckdaten zu gewährleisten.

Was ist Eurodac?

Eurodac ist eine biometrische Datenbank in der Europäischen Union (EU), in der die Fingerabdruckdaten von Personen, die Asyl beantragen, sowie Staatsangehörigen von Nicht-EU-Ländern bzw. Ländern des Europäischen Wirtschaftsraums zum Abgleich zwischen den Mitgliedstaaten der EU gespeichert werden.

Ob und wie diese Maßnahmen in der Praxis umgesetzt werden, unterliegt – soweit Bundesbehörden diese Daten verarbeiten – meiner Aufsicht. Das BAMF als in Deutschland zentral für das Asylverfahren zuständige Behörde hat mir dazu schriftlich einen Fragenkatalog beantwortet. Danach sind die Verantwortlichkeiten für die Rechtmäßigkeit der Datenverarbeitungen in dem Verfahren zwischen einer Vielzahl von Behörden aufgeteilt. Das BAMF, die Grenzbehörden, die Ausländerbehörden, die Aufnahmeeinrichtungen sowie die Polizeidienststellen der Länder nehmen die Fingerabdrücke ab. Über das Bundeskriminalamt als nationale Schnittstelle werden die Daten zur Speicherung für spätere Abgleiche an das EU-Zentralsystem übermittelt.

Im Ergebnis meiner Prüfung habe ich keine wesentlichen Mängel festgestellt.[110] Ich habe jedoch bemerkt, dass die vom BAMF verwendeten Merkblätter zur Information der betroffenen Personen unvollständige Angaben über die zuständige Datenschutzaufsichtsbehörde enthalten. Da auch biometrische Daten von Minderjährigen verarbeitet werden, ist es besonders wichtig, den betroffenen Personen die korrekte Stelle zur Wahrnehmung ihrer Rechte zu nennen. Das BAMF hat mir nun zugesagt, die entsprechenden Merkblätter im ersten Quartal des Jahres 2024 entsprechend anzupassen.

110 Kontrollbericht vom 20. Dezember 2023, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Kontrollberichte/Allgemeine-Verwaltung/Kontrolle-BAMF.html

10 BfDI Intern

10.1 Personalentwicklung in meiner Behörde

Meine Behörde ist weiterhin im Aufwuchs. Obwohl im Berichtsjahr viele Stellen besetzt wurden, wird die Personalgewinnung auch künftig von zentraler Bedeutung sein.

Dankenswerterweise wurden mir vom Haushaltsgesetzgeber auch für das Berichtsjahr 2023 zusätzliche Stellen bewilligt. Insgesamt konnte ich einen Stellenzuwachs von 30,6 Stellen verzeichnen. Unter Berücksichtigung der von meiner Behörde im Haushaltsjahr 2022 zu erbringenden Stellenkürzung sowie Umsetzungen an das Bundesverwaltungsamt zur dortigen Aufgabenwahrnehmung ist mein Personalhaushalt auf insgesamt 424 Stellen gewachsen. Davon entfallen 403,5 Planstellen auf Beamtinnen und Beamte sowie 20,5 Stellen auf Tarifbeschäftigte.

Zu meinem Bedauern musste ich im vergangenen Jahr eine kleine Zahl von Personalabgängen verzeichnen. Darunter waren neben geplanten auch ungeplante Abgänge, was ich auf den allgemeinen Fachkräftemangel sowie auf die Konkurrenzsituationen der Behörden untereinander, aber auch mit anderen Branchen, zurückführe. Da wir eine Behörde mit einem ungewöhnlich niedrigen Altersdurchschnitt sind, wird mein Haus – anders als andere Behörden – in den nächsten Jahren nur wenige Mitarbeiterinnen und Mitarbeiter durch Erreichen des Renten- bzw. Pensionsalters verlieren.

Im Berichtsjahr konnte ich 38 neue Kolleginnen und Kollegen im Haus begrüßen. In absehbarer Zeit rechne ich noch mit 17 weiteren Neuzugängen aus bereits abgeschlossenen Bewerbungsverfahren. Insgesamt verfügte meine Behörde zum Stichtag 31. Dezember 2023 über eine Personalstärke von 327 Personen.

Als moderne Behörde möchte ich meine Mitarbeiterinnen und Mitarbeiter auf ihrem individuellen beruflichen Weg unterstützen und Möglichkeiten zur Weiterentwicklung anbieten. Um diese Entwicklung aktiv zu begleiten, habe ich im Berichtsjahr ein Personalentwicklungskonzept etabliert.

Auch das Jahr 2023 stand wieder im Zeichen der Ausbildung und Nachwuchskräftegewinnung. Im vergangenen Jahr haben insgesamt zehn Studierende, acht Referendarinnen und Referendare sowie fünf Anwärterinnen und Anwärter in meinem Hause ihre jeweilige Station absolviert. Über die rege Inanspruchnahme meines Angebots freue ich mich ganz besonders, denn die Ausbildung und Nachwuchskräftegewinnung liegt mir sehr am Herzen!

Ich bin bestrebt, ein diverses, vielfältiges und tolerantes Arbeitsumfeld zu schaffen. Anfang des Jahres unterzeichnete ich die sogenannte Charta der Vielfalt. Hierbei handelt es sich um eine Selbstverpflichtung, die das Voranbringen der Anerkennung, Wertschätzung und Einbeziehung von Vielfalt in der Arbeitswelt in Deutschland zum Ziel hat. Alle Beschäftigten sollen Wertschätzung unabhängig von Alter, ethnischer Herkunft und Nationalität, Geschlecht und geschlechtlicher Identität, körperlichen und geistigen Fähigkeiten, Religion und Weltanschauung, sexueller Orientierung und sozialer Herkunft erfahren. Am 23. Mai 2023, dem Diversity Tag, organisierte ich in meinem Haus eine Veranstaltung zu diesem Thema. Anhand von Postern, Flyern, einem Quiz sowie einer Mitarbeiterbefragung konnten sich die Beschäftigten meines Hauses intensiv mit den Themen Vielfalt, Toleranz und Diversität auseinandersetzen.

Die Gewinnung neuer Mitarbeiterinnen und Mitarbeiter ist weiterhin eine meiner Prioritäten. Der bundesweite Fachkräftemangel sowie die Konkurrenz durch Behörden und Unternehmen im Raum Bonn stellt eine Herausforderung bei der Suche nach guten Bewerberinnen und Bewerbern dar. Durch die Teilnahme an Karrieremessen, z. B. in Frankfurt, Bonn, Köln und Brühl konnte ich mein Haus bekannt machen und mit vielen Personen ins Gespräch kommen.

Im Berichtsjahr 2023 habe ich 32 Stellenbesetzungsverfahren (sowohl Einzel- als auch Sammelbesetzungsverfahren) durchgeführt. Insgesamt habe ich 587 Bewer-

bungen erhalten. Von diesen wurden 312 Bewerberinnen und Bewerber zu Vorstellungsgesprächen eingeladen. 61 Personen konnte ich eine Einstellungszusage geben.

10.2 Im Umbau – Das neue Verbindungsbüro in Berlin steht kurz vor der Fertigstellung

Die bisherige Liegenschaft des Berliner Verbindungsbüros in der Friedrichstraße reichte für den Raumbedarf und die gestiegene Aktivität meiner Behörde nicht mehr aus. Dies erforderte die Anmietung einer größeren Liegenschaft. Sie befindet sich am Spittelmarkt und wird derzeit den Bedarfen entsprechend baulich angepasst. Ziel der laufenden mehrmonatigen intensiven Umbauphase, die kurz vor ihrem Abschluss steht, sind die Vereinigung moderner Arbeitsplätze, optimierte Veranstaltungsmöglichkeiten sowie verbesserte Barrierefreiheit und Sicherheit.

Das neu angemietete Berliner Verbindungsbüro bietet langfristig ausreichend Platz, damit alle meine Organisationseinheiten bedarfsgerecht auch in Berlin vertreten sind und in der Hauptstadt alle administrativen und politischen Schnittstellenaufgaben optimal erfüllen können. Bonn wird dabei eindeutiger Hauptstandort der Behörde bleiben.

Vor Einzug in die neue Liegenschaft am Spittelmarkt sind intensive und umfangreiche Umbauten notwendig, die kurz vor ihrer Fertigstellung stehen. Bei der Ausstattung des Gebäudes steht zum einen die Einhaltung notwendiger Sicherheitsstandards im Vordergrund. Zum anderen wird bei den Umbauarbeiten ein besonderes Augenmerk auf die Barrierefreiheit gelegt. Hierdurch erhalten Beschäftigte ebenso wie Besuchende bestmögliche Voraussetzungen für das Arbeiten und den Aufenthalt in der Dienststelle. Ein weiterer Schwerpunkt bei der Ausstattung des Gebäudes liegt auf moderner Informations- und Kommunikationstechnik. Berlin soll zudem künftig über moderne variable Besprechungs- und Konferenzräume – ausgerüstet mit zeitgemäßer Präsentations-, Ton- und Videotechnik – für kleinere Veranstaltungen verfügen. Alle veranlassten Maßnahmen tragen zu sehr guten und zukunftsfähigen Arbeitsbedingungen für meine Beschäftigten bei, damit wir weiterhin eine moderne, dynamische und zukunftsorientierte Behörde bleiben.

Ich bin optimistisch, dass meine Behörde im Frühjahr 2024 das neue Berliner Verbindungsbüro am Spittelmarkt beziehen kann.

10.3 Presse- und Öffentlichkeitsarbeit

Nach wie vor stellt die Presse- und Öffentlichkeitsarbeit eine meiner wichtigsten Aufgaben dar, um die mir gesetzlich zugewiesene Aufgabe zu erfüllen, die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung von personenbezogenen Daten zu sensibilisieren und zu informieren. Dabei achte ich darauf, nicht nur für Medienschaffende und Fachleute, sondern auch für die breite Bevölkerung und hier insbesondere für Kinder und Jugendliche ein entsprechendes Angebot zur Verfügung zu stellen. Der Erfolg und die Qualität dieser Arbeit lässt sich nicht nur in Zahlen ablesen, sondern wurde im Berichtszeitraum auch explizit von der Global Privacy Assembly (GPA) ausgezeichnet.

Pressearbeit

Für das Jahr 2023 gibt es kein einzelnes Thema, das bei den Anfragen an meine Pressestelle heraussticht. Vielmehr lassen sich innerhalb eines sehr breiten Spektrums der Anfragen zumindest drei Themenblöcke identifizieren. Dazu gehört, dass viele Anfragen der Medien weiterhin die Digitalisierung des Gesundheitswesens betrafen, insbesondere die elektronische Patientenakte und das elektronische Rezept. Gerade zur konkreten Funktionsweise der technischen Lösungen und den Rechten der Betroffenen erhalte ich viele Fragen.

Ein zweiter Themenbereich war die datenschutzrechtliche Regulierung von Künstlicher Intelligenz. Hier erhielt ich vermehrt Anfragen, als das Unternehmen OpenAI sein Produkt ChatGPT für eine breite Öffentlichkeit verfügbar gemacht hat. Ich konnte hierzu allerdings nur auf die Landesbeauftragten für den Datenschutz und die zwischenzeitlich gegründete Arbeitsgruppe der Datenschutzkonferenz verweisen. Meine Behörde hat aufgrund der föderalen Organisation des Datenschutzes in Deutschland mit Ausnahme der Telekommunikations- und Postdienstleister grundsätzlich keine Zuständigkeit für Unternehmen und Vereinigungen des nicht-öffentlichen Bereichs.

Das dritte Thema umfasste meine Anweisung an das Bundespresseamt (BPA), den Betrieb seiner Facebook-Fanpage einzustellen. Hier erläuterte meine Pressestelle häufig, wie die Verwaltungsverfahren und Abläufe in einem solchen Fall aussehen. Nach Klage des BPA gegen den Bescheid liegt der Fall mittlerweile beim Verwaltungsgericht Köln, auf das ich bei weiteren Anfragen verweise.

Neben diesen größeren Themen erreichte mich von Journalistinnen und Journalisten eine große Bandbreite an Fragen, beispielsweise zur Verarbeitung von Positivdaten bei Telekommunikationsdienstleistern, dem EU-US Data Privacy Framework, TrustPID, der BundID und zu der von mir betriebenen Mastodon-Instanz social.bund.de.

Ich habe im Berichtszeitraum 21 Pressemitteilungen herausgegeben und war einmal zu Gast in der Bundespressekonferenz. Außerdem habe ich neun Gastbeiträge und Aufsätze für verschiedene Medien verfasst. Meine Pressestelle hat 364 Anfragen per Mail und 370 telefonische Anfragen beantwortet.

Social Media und Webauftritt

Die von mir betriebene Mastodon-Instanz social.bund.de wächst immer weiter. Mittlerweile gibt es über 100 aktive Accounts von Bundesinstitutionen. Immer wieder muss ich leider Anfragen von öffentlichen Stellen aus den Bundesländern ablehnen, die ebenfalls gerne einen Account auf meiner Instanz hätten. Das kann ich jedoch mit meinen vorhandenen personellen und technischen Kapazitäten nicht leisten. Ausnahmen auf Ebene der Länder mache ich nur für die Landesbeauftragten für den Datenschutz und die Parlamente. Umso mehr freut es mich, dass immer mehr Bundesländer, wie beispielsweise Hessen und Sachsen, eigene Projekte im Fediverse verwirklichen.

Dem Account meiner Behörde social.bund.de/@bfdi folgen mittlerweile mehr als 44.000 andere Accounts. Ich freue mich sehr über das große Interesse der Öffentlichkeit. Dieses ist sicher auch darin begründet, dass mein Social Media Team und ich mit der Community im Fediverse konstant im aktiven Austausch sind und Fragen beantworten.

Auch jenseits von Statistiken erhält meine Öffentlichkeitsarbeit immer wieder viel positives Feedback. Als großen Erfolg und Bestätigung meiner Arbeit sehe ich deshalb die Auszeichnung der GPA aus dem Oktober 2023 für meine Pixi-Videos an. Der Preis wurde in der Kategorie „Education and public awareness“ vergeben. Die Videos basieren auf den erfolgreichen Pixi Büchern zu den Themen Datenschutz und Privatsphäre. Seit 2022 sind sie auf meiner Webseite zu finden und wurden im Berichtsjahr auch in einer englischsprachigen Version veröffentlicht.

Daneben konnte ich auf der Internetseite meiner Behörde eine entscheidende qualitative Verbesserung des Angebots erreichen. Dieser betrifft den Bereich „Dokumente“, in dem ich seit mehreren Jahren proaktiv Kontrollberichte, Stellungnahmen, Reden und vieles mehr veröffentliche. Dieser Bereich war bisher nach Dokumententyp getrennt aufgebaut. Mit der Zeit wurde das Angebot immer schwerer durchsuchbar. Dieses Problem konnten wir nun mit einer neuen Suchmaske lösen. Hierdurch wird eine sinnvolle Filterung, Suche und damit Auffindbarkeit für die große Anzahl der Dokumente ermöglicht.

Besuchergruppen

Meine Mitarbeiterinnen und Mitarbeiter des Berliner Verbindungsbüros betreuten wieder Besuchergruppen von Mitgliedern des Deutschen Bundestages. Insgesamt sechs Gruppen mit bis zu 50 Teilnehmenden wurden empfangen. Darüber hinaus waren drei weitere Besuchergruppen von Universitäten und Bildungsträgern in der Bonner Liegenschaft zu Gast.

Diese Termine zeigen, dass das Thema Datenschutz auch in der allgemeinen Bevölkerung als interessant und wichtig wahrgenommen wird. Daher schätze ich auch die in diesem Rahmen möglichen Diskussionen sowie die Chancen, sowohl Fragen zu beantworten, als auch mit „Mythen“ und „Fake News“ um das Thema Datenschutz im direkten Gespräch mit Bürgerinnen und Bürgern aufräumen zu können und würde mich freuen, wenn das Angebot, als Besuchergruppe in den Austausch mit mir und meinen Mitarbeiterinnen und Mitarbeitern zu kommen, auch weiterhin rege angenommen wird.

Informationsmaterial

In 2023 lag der Schwerpunkt in der Entwicklung neuer Informationsmaterialen. Zum einen habe ich in Zusammenarbeit mit dem Bundesarchiv (BArch) eine Broschüre entwickelt. Die Publikation befasst sich mit dem Ausgleich zwischen Archiv- und Datenschutzrecht.

Des Weiteren entwickelte mein Haus zwei neue Flyer. Einmal die Information zu Datenschutz-Rechten für Geflüchtete und Asylsuchende und weiterhin Hinweise für kleine und mittlere Postdienstleister, was beim Datenschutz zu beachten ist. Beide Flyer biete ich auch in Englisch an, um möglichst viele Interessierte zu erreichen.

Um meine Informationen gezielt zur Verfügung stellen zu können, habe ich mit der Bundesagentur für Arbeit (BA) sowie dem Bundesamt für Migration und Flüchtlinge (BAMF) Vereinbarungen geschlossen. Allen zuständigen Jobcentern der BA sowie Außenstellen des BAMF stelle ich kostenfrei meine Flyer „Datenschutz im Jobcenter“ sowie „Datenschutz-Rechte für Asylsuchende und Geflüchtete“ in der notwendigen Anzahl bereit.

Eine weitere umfangreiche Aufgabe meiner Öffentlichkeitsarbeit lag in der Bewältigung der anhaltend hohen

Nachfrage zu meiner Pixi-Buch-Reihe. Insgesamt über 430.000 Pixi Bücher wurden im Jahr 2023 durch Privathaushalte sowie von Schulen, Kitas, öffentlichen Einrichtungen, Vereinen und vielen anderen deutschlandweit sowie aus dem Ausland bestellt.

Querverweise:

8.5 Facebook-Seiten öffentlicher Stellen des Bundes

Die Aufzeichnungen aller Veranstaltungen die per Livestream übertragen wurden, finden Sie hier:

(QR-Code scannen oder klicken)

10.4 Veranstaltungen des BfDI

Auch in diesem Berichtszeitraum habe ich wieder eine Vielzahl an Veranstaltungen ausgerichtet. Wie auch bei der sonstigen Öffentlichkeitsarbeit versuche ich hier eine Balance zwischen Angeboten für Fachpublikum und der breiten Öffentlichkeit zu schaffen. Um möglichst vielen Menschen Zugang zu ermöglichen, biete ich für die meisten Veranstaltungen zusätzlich einen Livestream an, der zudem auch nachträglich kostenlos auf meiner Webseite abgerufen werden.

5 Jahre DSGVO

Ein Highlight unter den Veranstaltungen war sicherlich die am 23. Mai 2023 gemeinsam mit dem Europäischen Datenschutzbeauftragten und dem Bayerischen Landesbeauftragten für den Datenschutz in der Vertretung des Freistaates Bayern bei der Europäischen Union in Brüssel durchgeführte Veranstaltung zum Thema „5 Jahre DSGVO: Immer noch ein Maßstab in der digitalen Landschaft der EU?“. Hier bot sich die Gelegenheit, die Auswirkungen der DSGVO und die neuen Herausforderungen nach fünf Jahren ihrer Anwendung aus der Perspektive unterschiedlicher Akteure zu reflektieren.

Ich hatte dabei u. a. die Gelegenheit, auf dem Panel gemeinsam mit den hochrangigen Gästen aus europäischer Kommission, Parlament, Rat und Gerichtshof die DSGVO im Hinblick auf ihre praktische Funktionsweise und ihre Durchsetzung im Lichte der jüngsten Initiative der Europäischen Kommission zur Harmonisierung bestimmter Aspekte des Verwaltungsverfahrens in grenzüberschreitenden Fällen zu analysieren. Weiter erörterten wir, welchen Platz die DSGVO innerhalb des neuen Rechtsrahmens einnehmen wird, dem sogenannten Digital Rulebook (einschließlich des Digital Markets Acts, des Digital Services Acts und der zukünftigen Verordnung zur Künstlichen Intelligenz) und der EU-Datenstrategie (Data Governance Act, Data Act und der künftige Europäische Raum für Gesundheitsdaten).

Alle Teilnehmenden betonten die Rolle der DSGVO als wertvollen Meilenstein im Datenschutz und die Tatsache, dass die DSGVO international als eine Art „Goldstandard“ der Datenschutzgesetzgebung wahrgenommen wird. Es bestand in der Diskussion weitgehend Einigkeit dahingehend, dass die Durchsetzung der DSGVO in den letzten fünf Jahren bereits gut funktioniert hat, aber signifikante weitere Schritte für eine breite und effektive Durchsetzung notwendig sind.

Weltkindertag

Gemeinsam mit der Stadtbibliothek Bonn habe ich am 21. September 2023 zum Weltkindertag zwei Veranstaltungen durchgeführt. Am Vormittag trafen meine Mitarbeitenden und ich dort zwei vierte Klassen einer Bonner Grundschule. Neben einer kleinen Lesung aus unseren Pixi-Büchern gab es viele Informationen rund um das Thema Datenschutz. Hier konnten die Kinder unter anderem lernen, wie man ein leicht zu merkendes, aber trotzdem sicheres Passwort erstellt. Die Veranstaltung bestätigte mich zudem einmal mehr darin, dass auch schon Kinder im Grundschulalter ein nicht zu unterschätzendes Verständnis für die Wichtigkeit des Schutzes ihrer Daten mitbringen. Deshalb ist es richtig und wichtig, bereits in diesem Alter erste Grundlagen insbesondere im Umgang mit modernen Medien zu legen.

Nachmittags veranstalteten wir ein Familienfest, bei dem wir uns insbesondere über kleine Besucherinnen und Besucher sowie viele interessierte Eltern freuen konnten. Hier zeigte sich, dass wir mit unseren Angeboten auch für kleinere Kinder nicht nur diese, sondern mittelbar immer wieder auch viele Erwachsene erreichen, die sich sonst vermutlich keine größeren Gedanken über das Thema Datenschutz gemacht hätten. Entsprechend planen wir auch für 2024 wieder Veranstaltungen mit und für Kinder.

Politische Foren

Ein mittlerweile etabliertes Format, dessen besondere Zielgruppe Akteure und Stakeholder des politischen Berlins sind, stellen meine Politischen Foren dar. Auch in

diesem Jahr habe ich daher wieder zwei entsprechende Veranstaltungen durchgeführt.

Mit meinen Gästen sind wir beim Frühjahrsforum den Fragen „Endet Datenschutz am Werkstor? – Wie steht es um den Beschäftigtendatenschutz?“ nachgegangen. Aus ihrer gewerkschaftlichen Erfahrung insbesondere bezogen auf einen großen Onlineversandhändler berichtete Frau Monika Di Silvestre, Landesfachbereichsleiterin Handel bei ver.di. In einer spannenden Diskussion gemeinsam mit Ana Dujic, Abteilungsleiterin im Bundesministerium für Arbeit und Soziales (BMAS), Roland Wolf von der Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA) und Prof. Dr. Gregor Thüsing, Arbeitsrechtler an der Universität Bonn, bestand trotz unterschiedlicher Positionen zumindest Einigkeit, dass die Digitalisierung die Arbeitswelt vor neue Herausforderungen stellt. Die Veranstaltung war ein wertvoller Beitrag im Vorfeld der bevorstehenden Gesetzgebungsaktivität zum Beschäftigtendatenschutz.

Beim Politischen Herbstforum ging es unter dem Titel „Demokratie und Persönlichkeitsrecht gefangen im Metaversum?“ um die facettenreichen Entwicklungen des Metaversums und seine Chancen sowie Risiken gerade unter dem Blickwinkel der Persönlichkeitsrechte und des demokratischen Gemeinwesens. Mit ihrem Eingangsimpuls beleuchtete Frau Prof. Dr. Carolin Wienrich, Professorin am Institut für Mensch-Computer-Medien der Universität Würzburg, Potentiale sowie Risiken des Metaversums, insbesondere aus psychologischer Sicht und ging auf Sicherheitsaspekte bezüglich Identität und Identifizierbarkeit ein. Im Anschluss diskutierten Susanne Dehmel von Bitkom e. V., Paul Nemitz, Berater der EU-Kommission und Mitglied der Datenethikkommission der Bundesregierung, Dorothea Winter, Philosophin und Autorin, gemeinsam mit mir über die unter den Begriff Metaversum fallenden Entwicklungen. Hier zeigte sich, dass das Metaversum wohl weder eine Dystopie, noch eine Verheißung ist. Angesichts möglicher Gefahren für Freiheiten und Demokratie gilt es allerdings, wachsam zu bleiben.

Weitere Veranstaltungen

Zum Abschluss meines Vorsitzes der Datenschutzkonferenz habe ich im Januar Expertinnen und Experten zum Gespräch mit dem Schwerpunktthema „Der Data Act und die Zukunft des Datenschutzes“ ins Europäische Haus nach Berlin eingeladen. Dabei standen die Fragen zur Nutzung industrieller Daten und die Zukunft des transatlantischen Datenverkehrs im Mittelpunkt.

Anlässlich des Grundrechtetags organisierte ich im Mai eine Diskussionsveranstaltung zum Thema „Meinungsfreiheit versus digitale Gewalt im Netz“ in Bonn, zu der zahlreiche interessierte Bürgerinnen und Bürger willkommen waren. Diskutiert wurde, wie man im Zeitalter von Fake News, Hassrede und digitaler Gewalt im Netz die Meinungsfreiheit auch im Internet schützen kann.

Im September lud ich zu einer Konsultationsveranstaltung zum Thema „Wieviel Künstliche Intelligenz verträgt unsere Gesellschaft?“ nach Berlin, um gemeinsam mit Zivilgesellschaft, Politik, Forschung und Wirtschaft über Datenschutz, Künstliche Intelligenz und die Auswirkungen auf unsere Gesellschaft zu diskutieren. Die Kernfragen waren: Wie geht man bei der datenschutzrechtlichen Beurteilung derart komplexer Sachverhalte vor? Wie können die allgemeinen Datenschutzgrundsätze eingehalten werden? Wie ist die effektive Datenschutzaufsicht zu gewährleisten?

Über das Jahr verteilt gehören vier datenschutzrechtliche Themenworkshops zu den regelmäßigen Angeboten meines Hauses für parlamentarisch Tätige. Dadurch besteht Gelegenheit für einen informellen Austausch über aktuelle Fragen des Datenschutzes und der Informationsfreiheit nach den Chatham House-Regeln. Zudem habe ich für diese Zielgruppe auch in diesem Jahr einen Workshop zu den Grundlagen des Datenschutzes angeboten. Er dient dazu, Einsteigern in die Thematik Basiswissen zu vermitteln.

Zudem stehe ich regelmäßig mit zivilgesellschaftlichen Organisationen in einem Austausch. Bestandteil der Kontakte sind zwei jährliche „NGO-Treffen“, anlässlich derer ich auch in diesem Jahr spannende Diskussionen zu diversen datenschutzrechtlichen Themen führen durfte. So ging es u. a. um aktuelle Datenschutzfragen im Kontext der Digitalisierung des Gesundheitswesen, TrustPID, das Nachrichtendiensterecht sowie Auskunfteien.

Querverweise:

6.2.1 Konferenz der Informationsfreiheitsbeauftragten, 6.3.2 Case Handling Workshop, 6.1.3 7. Fachsymposium zur Informationsfreiheit

10.5 Projektgruppe KI-Strategie

Die raschen Entwicklungen im Bereich der KI haben auch Auswirkungen auf die Arbeit der Datenschutzbehörden. Je nach Einsatzart können KI-Anwendungen zu intensiven Eingriffen in die Grundrechte der betroffenen Personen führen. Um sicherzustellen, dass die

datenschutzrechtlichen Bestimmungen dabei eingehalten werden, habe ich eigens eine Projektgruppe eingerichtet, die Grundlagen für den Umgang mit KI-Anwendungen im Bereich der Aufsichtstätigkeit erarbeitet.

Der Einsatz von KI wird unsere Gesellschaft tiefgreifend zu verändern. Aus Datenschutzsicht sind die Herausforderungen, die KI-Anwendungen mit sich bringen, dabei erheblich. Die Aufsichtsbehörden werden durch die hochdynamischen technologischen Entwicklungen in diesem Bereich mit neuen Fragestellungen konfrontiert: Wie geht man bei der datenschutzrechtlichen Beurteilung derart komplexer Sachverhalte vor? Wie können die allgemeinen Datenschutzgrundsätze eingehalten werden? Wie ist die effektive Datenschutzaufsicht zu gewährleisten? – um nur einige Beispiele zu nennen.

KI und Aufsichtstätigkeit

Damit ich meiner Aufsichts- und Beratungsaufgabe in diesem sich schnell wandelnden Umfeld auch künftig gerecht werden kann, habe ich im Berichtsjahr eine Projektgruppe eingerichtet, die Grundlagenarbeit für die Kontrolltätigkeit auf diesem Gebiet leistet. Die Projektgruppe setzt sich interdisziplinär aus Mitgliedern ganz verschiedener Fachreferate meines Hauses zusammen. Dort werden jetzt bereits aus unterschiedlichen Perspektiven KI-Anwendungen kontrolliert und die von uns beaufsichtigten Stellen dazu beraten. Auf diese Weise können Erfahrungen aus der bisherigen Aufsichtspraxis mit in die Weiterentwicklung der Kontrolltätigkeit eingebracht werden. Ziel der Projektgruppe ist es, Möglichkeiten und gegebenenfalls auch Grenzen der Aufsicht auszuloten, Fragen zu stellen, die sich im Angesicht der neuen Herausforderungen ergeben und Handlungsperspektiven zu erarbeiten, um weiterhin eine effektive Datenschutzaufsicht zu gewährleisten. Bestimmte Instrumente, die uns als Datenschutzaufsicht bereits jetzt zur Verfügung stehen, werden auch künftig nicht an Bedeutung verlieren und genauso für den Einsatz von KI Anwendung finden. Gleichzeitig gilt es aber auch das bestehende Selbstverständnis der Aufsichtsbehörden mit Blick auf die rasanten Entwicklungen zu hinterfragen und neue fachliche Gesichtspunkte, Herangehensweisen und Expertisen mit einzubeziehen. So erarbeitet die Projektgruppe auch Kriterien, die anwendungsbezogen bei der Prüfung von KI eingesetzt werden können. Dabei soll unter anderem ein einheitliches Verständnis für das Thema KI im Bereich der Aufsicht entwickelt werden, welches Maßstab und Leitlinie für die Arbeit der Datenschutzbehörden werden und als Grundlage für die so wichtige Teilnahme am gesellschaftlichen Diskurs dienen kann.

Konsultationsveranstaltung: Wieviel KI verträgt unsere Gesellschaft?

Die gesellschaftlichen und rechtlichen Rahmenbedingungen rund um das Thema KI werden aktuell auf ganz unterschiedlichen Ebenen diskutiert und gestaltet. Insbesondere hier sehe ich eine wichtige Aufgabe für den Datenschutz, sich aktiv in diesen Prozesseinzubringen. Zu diesem Zweck hat die Projektgruppe KI-Strategie im September zu einer Konsultationsveranstaltung zum Thema „Wieviel KI verträgt unsere Gesellschaft“ eingeladen. Gemeinsam mit Vertreterinnen und Vertretern aus Zivilgesellschaft, Politik, Forschung und Wirtschaft, haben wir uns in Berlin vor allem zu drei Fragekomplexen ausgetauscht: Fragestellungen aus den Kontexten „KI und die Rolle der Datenschutz-Aufsichtsbehörden“, „Blackbox KI – wie kann der Datenschutz den Transparenzherausforderungen begegnen?“, „KI und Verantwortlichkeit: Wer verantwortet hier eigentlich was?“.

Die Idee dieser Veranstaltung war es, Expertinnen und Experten aus ganz unterschiedlichen Bereichen zusammenzubringen, miteinander ins Gespräch zu kommen, Positionen auszutauschen und zu diskutieren. Das positive Fazit der Teilnehmerinnen und Teilnehmer, dass ein derartiger Austausch auch künftig hilfreich sein könne, um Datenschutz nicht an der KI-Realität vorbei zu betreiben, teile ich. Mein Ziel ist es, weiterhin in engem Austausch mit allen Stakeholdern zu bleiben und durch guten Datenschutz die mit KI verbundenen Risiken zu reduzieren, damit die unstrittig vorhandenen positiven Potentiale zum Wohle aller eingesetzt werden können.

Die Herausforderungen, die sich aus den Entwicklungen im KI-Bereich ergeben, gehen mit einer großen Verantwortung einher. Das gilt nicht nur, aber auch für die Aufsichtsbehörden. Die von mir eingesetzte Projektgruppe ist ein wichtiger Beitrag der notwendigen Auseinandersetzungen zu diesem Thema. Die Ergebnisse ihrer Arbeit sollen einerseits in die praktische Arbeit meiner Mitarbeiterinnen und Mitarbeiter einfließen, aber auch Grundlage für weitere Schritte und Entwicklungen bilden. Auf Basis der Arbeiten der Projektgruppe plane ich zukünftig anlassbezogen Prüfschwerpunkte im Bereich KI zu setzen.

10.6 Future Foresight beim BfDI

Der (wahlweise Karl Valentin, Mark Twain, Winston Churchill oder Niels Bohr zugeschriebene) Satz „Prognosen sind schwierig, besonders wenn sie die Zukunft betreffen“ mag zutreffen. Für die Arbeit meiner Behörde ist eine gewisse Prognosefähigkeit in Bezug auf künftig relevant werdenden Technologien dennoch

unabdingbar. Daher habe ich begonnen, ein „Future Foresight“ mit Blick auf datenschutzrelevante technologische Entwicklungen aufzubauen.

Die Datenschutz-Grundverordnung ist technologieneutral. Dies hat den Vorteil, dass neue Technologien erstmal keine neue Rechtssetzung erfordern. Auf der anderen Seite müssen Spezifika immer wieder anhand der Maßstäbe der DSGVO einzeln bewertet werden, weil es gerade keine speziellen Vorgaben in Bezug auf konkrete Technologien gibt.

Eine Betrachtung neuer Technik unter Datenschutzgesichtspunkten erfolgt oft erst, wenn diese öffentliche Aufmerksamkeit erfährt. Dann ist es aber meist zu spät, um noch in der Entwicklungsphase die Anforderungen des Datenschutzes, etwa die Betroffenenrechte der Nutzer, von Beginn an zu berücksichtigen. Eine frühzeitige Einbeziehung von Datenschutzfragen schon bei der Entwicklung neuer Technologien ist jedoch essentielle Voraussetzung für den in der DSGVO verankerten Grundsatzes des „Data Protection by Design“.

Ziel des Future Foresight – oder Technologieradar – ist es, neue technische Themen bereits zu erkennen, bevor diese in den Fokus öffentlicher Wahrnehmung geraten, in der Regel also auch vor einem breiten Markteintritt. Dies ermöglicht eine frühzeitige Analyse und Bewertung aus Datenschutzsicht sowie eine konstruktive konzeptionelle Zusammenarbeit mit Entwicklern und Protagonisten. Dabei sollen neue Technologien so begleitet werden, dass es zu realistischen Einschätzungen kommt und überzogene Erwartungen vermieden werden. Wenn Anforderungen des Datenschutzes von vornherein Berücksichtigung finden, können Fehlentwicklungen (und damit Aufwände für spätere Nachbesserungen) vermieden werden.

Daher hat mein Haus begonnen, entsprechende Kapazitäten und Fähigkeiten für ein datenschutzbezogenes Future Foresight aufzubauen. Ähnliche Aktivitäten gibt es auch auf europäischer und internationaler Ebene, z. B. beim Europäischen Datenschutzbeauftragten, bei der britischen Datenschutzaufsichtsbehörde ICO oder in übergreifenden Gremien wie der von mir geleiteten Berlin Group und den G7. Eine Zusammenarbeit unter den Aufsichtsbehörden bei Zukunftsthemen und neuen Technologien kann dabei zu einer frühzeitigen Abstimmung und einheitlichen Bewertung beitragen.

Querverweise:

4.4 Berlin Group, 4.5.1 G7 DPA Roundtable

10.7 Technische Laborumgebung

Im Berichtsjahr wurde die Laborumgebung meiner Behörde zur technischen Untersuchung von IT-Anwendungen, -Diensten und Apps weiter ausgebaut und steht nun allen Mitarbeitenden zur Verfügung. Existierende Erfahrungen mit eigenen Laboruntersuchungen im Bereich der Telemedien wurden um technische und methodische Kompetenzen zur Durchführung größerer Untersuchungen erweitert.

Infolge fortschreitender Digitalisierung alltäglicher Lebensbereiche wie auch bei der Arbeit der Bundesbehörden spielen technische Aspekte des Datenschutzes eine immer stärkere Rolle. Ob digitale Gesundheitsanwendungen oder Nutzung digitaler Identitätsdokumente, ob Einsatz von smarten Stromzählern oder Web-Portalen zu Fachanwendungen in Bundesbehörden – es kommen zunehmend browsergestützte Verfahren, Smartphone-Apps und smarte Geräte zum Einsatz.

Um prüfen zu können, ob entsprechende Dienste, Apps, IoT-Geräte und -Sensoren die gesetzlichen Anforderungen des Datenschutzes berücksichtigen, müssen deren technischen Eigenschaften noch genauer und vor allem „unabhängig“ durch meine Behörde untersucht werden können.

Zu diesem Zweck nahm im Berichtsjahr ein neues Referat seine Arbeit auf, das für den Betrieb der Laborumgebung zuständig ist. Die Anforderungen an die Laborumgebung wurden in einem Anforderungsmanagementprozess erhoben und mit den Stakeholdern im Haus abgestimmt. Der so erarbeitete Anforderungskatalog dient als Basis für die nächste Stufe des Laborausbaus. Neben den funktionalen und nicht funktionalen Anforderungen wurden Prozesse zum Betrieb der Laborumgebung definiert und mit der Umsetzung der Kriterien des IT-Grundschutzes (BSI) begonnen.

In der Laborumgebung können die Mitarbeitenden meiner Behörde durch den Einsatz geeigneter Untersuchungswerkzeuge die Datenflüsse von Produkten – wie Apps, Anwendungen oder Geräte– untersuchen. Dazu werden mit entsprechenden Werkzeugen vorkonfigurierte virtuelle Maschinen automatisiert erstellt und benötigte Ausstattung, wie Smartphones, zur Verfügung gestellt. Auf den virtuellen Maschinen können unterschiedliche Betriebssysteme zum Einsatz kommen, um dort lauffähige Produkte zu untersuchen. Es können damit verschiedene Szenarien nachgestellt und untersucht werden, etwa zu Abhängigkeiten und Zusammenarbeit von Produktbestandteilen auf mehreren Systemen. Im Berichtsjahr konnten erste Erfahrungen zu geeigneten Untersuchungswerkzeugen und -methoden mit einzel-

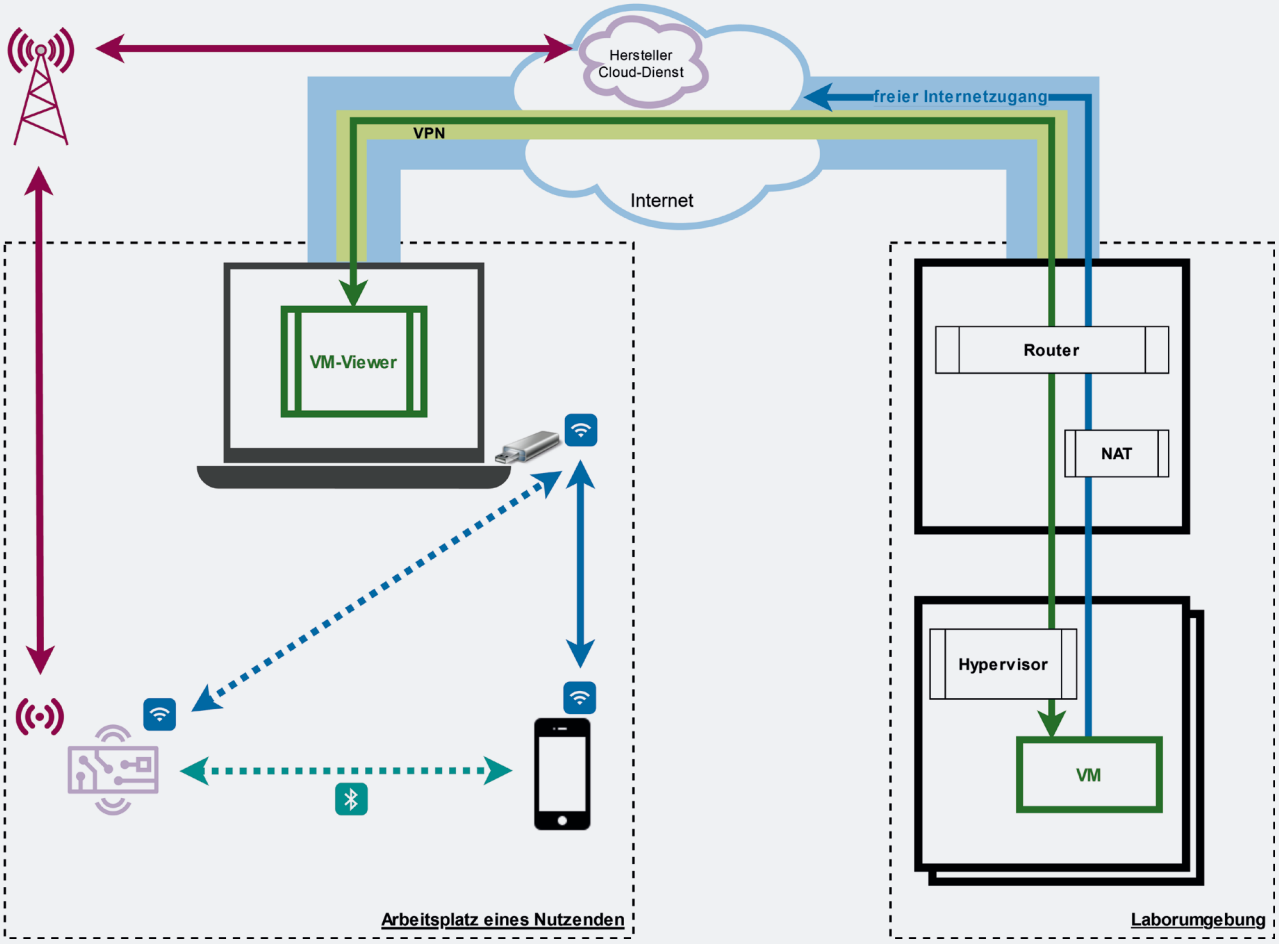
nen Untersuchungen von Webseiten und Apps gesammelt werden.

Um bereits in der Datenschutz-Community vorhandenes Wissen zu Untersuchungswerkzeugen und –methoden zu nutzen und eigene Ergebnisse und Erkenntnisse zu streuen, stehe ich im aktiven Austausch mit anderen Behörden. Der Austausch mit Nicht-Regierungsorganisationen ist ebenfalls geplant.

Folgende Abbildung stellt schematisch die Gesamtarchitektur der Laborumgebung inklusive der Kommunikation mit dem Untersuchungsarbeitsplatz dar.

Auf der linken Seite ist der Arbeitsplatz eines Nutzenden dargestellt, der ortsunabhängig von der Laborumgebung aufgebaut ist und exemplarisch aus einem Laptop, dem zu untersuchenden IoT-Gerät und einem Smartphone besteht. Der Zugriff auf die Laborumgebung erfolgt durch den Aufbau einer sicheren VPN-Verbindung (hellgrüner Tunnel) über das Internet (hellblauer Tunnel). Die Steuerung der eigenen virtuellen Maschine (VM) in der Laborumgebung und die Darstellung der VM auf dem Laptop erfolgt über ein entsprechendes Protokoll (grüne Verbindung). Über dieses Protokoll lassen sich an den Laptop angeschlossene USB-Geräte in die VM übermitteln; der freie Internetzugang der VM (blaue Verbindung) kann so über den angeschlossenen USB-WLAN-Stick am Arbeitsplatz zur Verfügung gestellt werden.

Die rechte Seite bildet beispielhaft die Server der Laborumgebung ab. Ein Server stellt sicher, dass nur VPN-Verbindungen zur Laborumgebung erlaubt sind und ermöglicht den freien Internetzugang der VM über das NAT-Verfahren (blaue Verbindung). Die Kommunikation verläuft dann über einen Router zur Virtualisierungsumgebung (Hypervisor), die den Betrieb und den Zugriff auf die VM gewährleistet (grüne Verbindung).



10.8 Aufbau eines strukturierten Notfall- und Krisenmanagements

Als richtungsweisender Schritt zu einer krisenfesten Behörde konnte in meinem Haus das Projekt zum Aufbau eines internen strukturierten Notfall- und Krisenmanagements mit einem Sollkonzept weiter forciert werden. Die sich aus diesem ergebenen Maßnahmen werden nun sukzessive umgesetzt und das Konzept kontinuierlich evaluiert.

Zur Stärkung der Resilienz meiner Behörde gegenüber Krisen ist der Auf- und Ausbau eines strukturierten Krisenmanagements unerlässlich. Hierzu hatte ich bereits in meinem letzten Tätigkeitsbericht ausgeführt, dass sich dieses mit zusätzlicher externer Unterstützung im Aufbau befindet. Wie sich im Laufe des Projekts zeigte, sind die Übergänge zwischen einem Notfall und einer Krise fließend. Daher habe ich um die ganzheitliche Erarbeitung eines strukturierten Notfall- und Krisenmanagement gebeten. Aufgrund der Komplexität konnte das Projekt noch nicht vollumfänglich abgeschlossen werden.

Darüber hinaus beteiligt sich meine Behörde seit kurzem am nationalen Krisenmanagement und der zivilen Alarmplanung. Zudem konnte meine Behörde an der länder- und ressortübergreifenden Krisenmanagementübung LÜKEX aus organisatorischer Sicht beobachtend teilnehmen, um Erkenntnisse für den Fall einer möglichen Krisenbewältigung zu gewinnen. Das alles wird zukünftig dazu beitragen, meine Behörde für den Fall der Fälle notfall- und krisenfest zu machen.

10.9 Aufbau eines zentralen Wissensmanagements

Nach Durchführung mehrerer Workshops und einer Zukunftswerkstatt schreitet der Aufbau eines zentralen, strukturierten Wissensmanagements weiter voran. Hierdurch soll meine Behörde personenunabhängig und zukunftsorientiert aufgestellt werden.

Wie im letzten Tätigkeitsbericht berichtet, habe ich als Projekt den Aufbau eines zentralen, strukturierten Wissensmanagements in meiner Behörde angestoßen und konnte dies im vergangenen Berichtszeitraum entscheidend vorantreiben. Die mit dem Wissensmanagement betrauten Mitarbeitenden aus allen Organisationseinheiten wurden in zwei Workshops in den fachlichen Grundlagen des Wissensmanagements geschult, wobei sich diese Schulungen inhaltlich an der Ausbildung der Industrie- und Handelskammer zur Wissensmanagerin bzw. zum Wissensmanager orientiert haben.

Im Rahmen einer sogenannten Zukunftswerkstatt haben 40 Mitarbeitende danach die Eckpfeiler für das Konzept zum Aufbau eines zentralen, strukturierten Wissensmanagements in meiner Behörde erarbeitet. Die daraus gewonnenen Erkenntnisse wurden in einen Maßnahmenkatalog überführt. Dieser stellt die Grundlage für die weitere strategische Ausrichtung des Wissensmanagements dar. Das wesentliche Ziel ist, das Bewusstsein für Wissensmanagement zu schärfen und die Vorteile der Anwendung in den Vordergrund zu stellen. Die Umsetzung der Maßnahmen führen zu einer gestärkten Effektivität und höheren Effizienz in Bezug auf meine Aufgaben im Datenschutz und der Informationsfreiheit. Dies gilt auch insbesondere für die Einarbeitung neuer Beschäftigter. Mit einem ganzheitlichen Ansatz möchte ich den Wissenstransfer, die Wissensentwicklung und die Wissensbewahrung optimieren. Ich plane, diesen Prozess fortzuführen, um diese Ziele zu erreichen.

10.10 Statistik für das Jahr 2023

Auch aus der Statistik lassen sich Einblicke in die Arbeit meiner Behörde gewinnen. Es zeigt sich insbesondere, dass die Arbeit beim Thema Datenschutz nicht ausgeht.

Anfragen, Beschwerden und Meldungen zu Datenschutzverstößen

Im Berichtsjahr wurden insgesamt 7.782 Beschwerden und Anfragen an mich gerichtet. Hier zeigt sich eine Trendumkehr zu den beiden Vorjahren. Bei den schriftlichen Anfragen schließt das Jahr 2023 auf dem Niveau des Pandemiejahres 2020 ab. Lediglich zur Einführung der DSGVO konnte meine Behörde höhere Eingangszahlen verzeichnen. Der Hintergrund für diese Entwicklung ist insbesondere im Bereich des Gesundheitsdatenschutzes zu finden, in dem z. B. die elektronische Patientenakte oder das E-Rezept große öffentliche Aufmerksamkeit generierten. Neben den schriftlichen Anfragen und Beschwerden habe ich auch in 5.506 Fällen Personen telefonisch beraten.

Auf hohem Niveau rückläufig zeigte sich jedoch die Anzahl der Meldungen von Datenschutzverstößen. Im Berichtsjahr habe ich 9.263 Meldungen entgegengenommen.

Beschwerden und Anfragen	2020	2021	2022	2023
Allgemeine Anfrage	4897	4329	4434	5162
Beschwerde Art. 77 DSGVO	2861	2383	2115	2513
Beschwerde Art. 80 DSGVO	25	19	3	11
Beschwerde § 60 BDSG	56	54	29	50
Eingabe gegen Nachrichtendienste	39	44	38	46

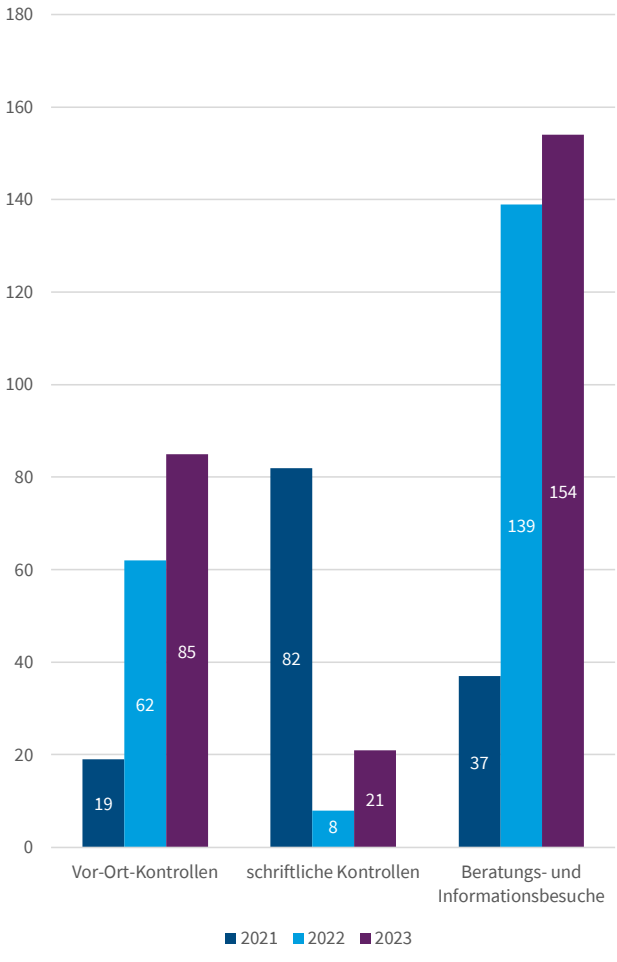
Meldungen von Datenschutzverstößen	2020	2021	2022	2023
Meldungen nach Art. 33 DSGVO	9987	10106	10614	9234
Meldungen nach § 169 TKG	37	51	44	29

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. Der Trend zurück zum persönlichen Gespräch nach der Corona-Pandemie ist ungebrochen. Auch im Berichtsjahr 2023 konnte ich meine Beratungs- und Kontrolltätigkeit weiter steigern. Das Instrument der schriftlichen Kontrolle hat dabei aber nicht komplett ausgedient, sondern wird dort, wo es sich als sinnvoll erwiesen hat, weiterhin eingesetzt.

Es ist außerdem erfreulich, dass meine Behörde auch von den beaufsichtigten Stellen weiterhin als beratender Ansprechpartner geschätzt wird. Dies kommt durch die abermals gestiegene 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.

Beratungen und Kontrollen seit 2021

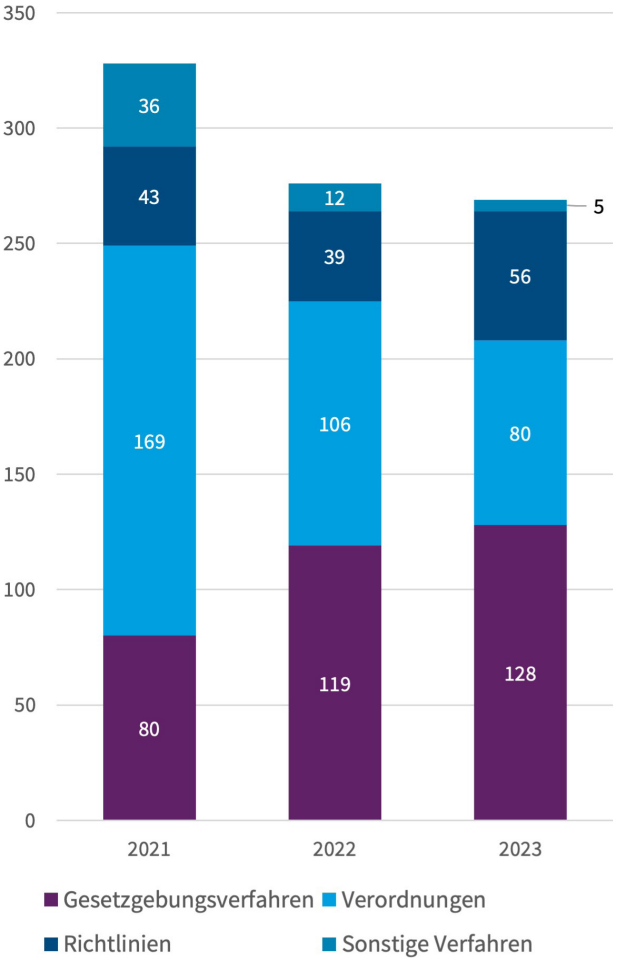


Förmliche Begleitung von Rechtsetzungsvorhaben

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. Diese Zusammenarbeit funktioniert je nach Ressort unterschiedlich gut, von optimal bis völlig unangemessen. Aus der Statistik für das Berichtsjahr lässt sich jedoch ein weiterhin hohes Niveau bei der Beteiligung zu förmlichen Gesetzen erkennen, die entsprechende Aufwände nach sich zieht. In die Gesetzgebung wurde ich auch durch den Deutschen Bundestag eingebunden. In sechs Fällen wurde ich durch Ausschüsse als Sachverständiger gehört. Auf nationaler Ebene wurde ich darüber hinaus in 103 Fällen zur Prüfung von Dateianordnungen bei Sicherheitsbehörden beteiligt.

Auf europäischer Ebene war ich außerdem bei der Erstellung von sieben Verordnungen und drei Richtlinien eingebunden.

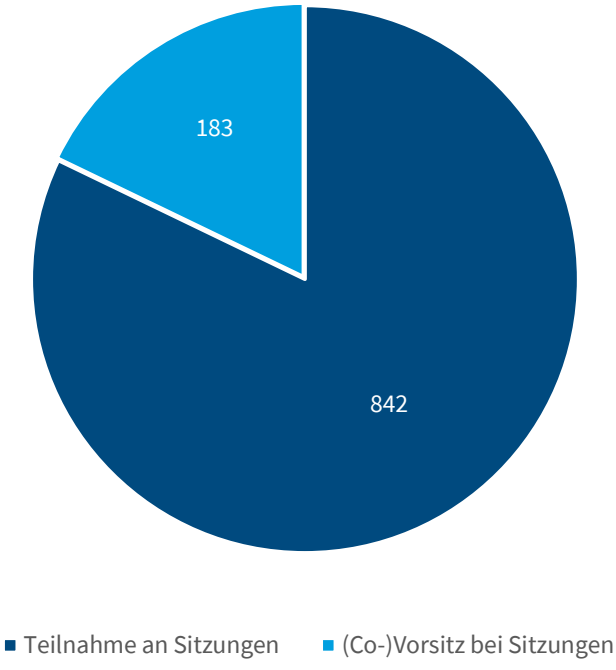
Beteiligungen nach § 21 GGO



Gremiensitzung

Arbeitsreich war das Jahr 2023 auch in der Abstimmung mit anderen nationalen, europäischen und internationalen Datenschutzbehörden. Dabei hat sich der Arbeitsumfang in den letzten Jahren kontinuierlich gesteigert auf nun mehr als eintausend Gremiensitzungen im Jahr. Im Netzwerk der Datenschutzaufsichtsbehörden nimmt meine Behörde oftmals eine koordinierende und führende Rolle ein. So wurden fast 18 Prozent der Sitzungen von meinen Beschäftigten (mit)geleitet. Mit 17 in Gremien eingebrachten Beschlussentwürfen kommt dies auch in der inhaltlichen Arbeit zum Ausdruck.

Teilgenommene Gremiensitzungen im Berichtsjahr



11 Zentrale Anlaufstelle

11.1 Rückblick

Die Aufsichtsbehörden des Bundes und der Länder verfügen in Angelegenheiten der Europäischen Union (EU) über eine Zentrale Anlaufstelle (ZASt), die in meinem Haus angesiedelt ist und die bei der Zusammenarbeit in EU-Angelegenheiten unterstützt. Die ZASt bringt sich mit dem ganz besonderen Blickwinkel des Scharniers zwischen der deutschen und der europäischen Datenschutzaufsicht in die vielfältigen Arbeiten an der Verbesserung zur gesamteuropäischen Zusammenarbeit aktiv ein.

Bericht an die EU-Kommission zum DSGVO-Vollzug

Im Berichtsjahr hat die Europäische Kommission von den Mitgliedern des Europäischen Datenschutzausschusses (EDSA) statistische Kennzahlen erbeten, um sich einen Überblick zum DSGVO-Vollzug in den Mitgliedstaaten zu verschaffen. Dem vorangegangen waren wiederholte Berichte, dass einzelne Aufsichtsbehörden die DSGVO nicht ausreichend durchsetzen. Für die quartalsweise Zulieferung der Daten an die Kommission hat die ZASt in Abstimmung mit den deutschen Aufsichtsbehörden ein entsprechendes Meldeformular und Anschreiben entworfen. In ihrer koordinierenden Rolle hat die ZASt insbesondere die substantiellen Beiträge der deutschen Aufsichtsbehörden zur innereuropäischen Datenschutzzusammenarbeit herausgearbeitet und in quantifizierbarer Form dargestellt. Die ZASt wird die Berichtstätigkeit im Auftrag der deutschen Aufsichtsbehörden weiter fortsetzen.

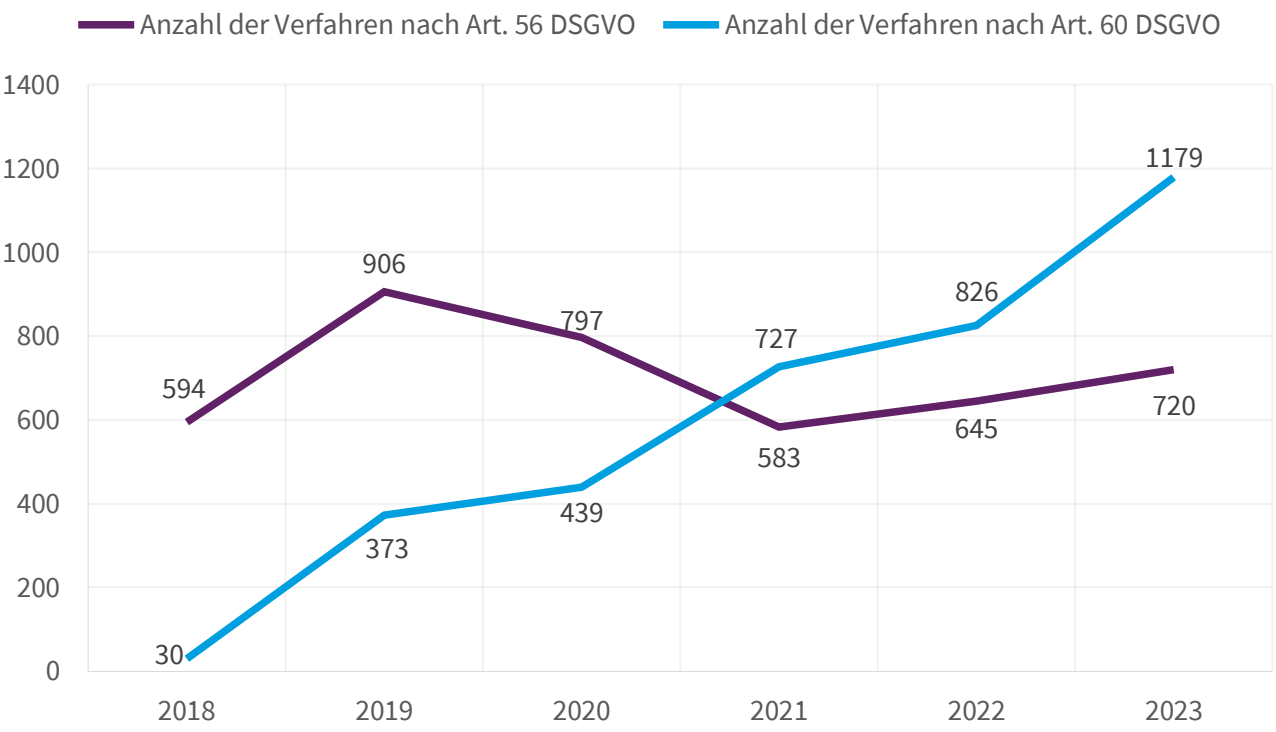
DSGVO-Vollzug im europäischen Aufsichtsverbund – Bessere Ergebnisse durch zusätzliche Verfahrensregelungen?

Immer wieder gibt es Berichte zu defizitärem DSGVO-Vollzug im europäischen Aufsichtsverbund. In diesem Zusammenhang wird öfter auch das Funktionieren der Zusammenarbeit der europäischen Aufsichtsbehörden im Rahmen des One-Stop-Shops in Frage gestellt. Der Kommissionsentwurf einer EU-Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO hält an dem Grundprinzip des One-Stop-Shops mit einer EU-weit federführend zuständigen Aufsichtsbehörde fest. Nach der Begründung der Kommission lägen die Probleme primär in der unzureichenden Zusammenarbeit der betroffenen Aufsichtsbehörden vor Vorlage eines Beschlussentwurfs durch die federführende Aufsichtsbehörde. Daher solle insbesondere der Austausch zweckdienlicher Informationen in diesem Stadium des Kooperationsverfahrens konkreter und differenzierter geregelt werden. Damit solle neben einer Verfahrensbeschleunigung auch eine weiter steigende Anzahl von Streitbeilegungsverfahren im EDSA vermieden werden, zu denen es kommt, wenn sich die beteiligten Aufsichtsbehörden nicht auf einen Beschlussentwurf einigen können.

Unter der bestehenden Rechtslage stellt sich vor dem Hintergrund dieser neuen Regelungsansätze die Frage des Funktionierens der Zusammenarbeit der Aufsichtsbehörden. Die nachstehende Grafik zeigt die quantitative Entwicklung der Verfahrenszahlen zur Klärung nach Art. 56 Abs. 1 DSGVO, welche Behörden in einem Fall europaweit federführend und welche als mitwirkende betroffen sind. Sie zeigt ebenso die Entwicklung der Verfahren nach Art. 60 DSGVO mit Vorlage eines Beschlussentwurfs, eines überarbeiteten Beschlussentwurfs oder eines endgültigen Beschlusses sowie zum Austausch entscheidungsrelevanter Informationen.

Im Berichtsjahr hat sich weiter bestätigt, dass sich der Schwerpunkt der grenzüberschreitenden Zusammenarbeit verlagert (29. TB Nr. 11.2). Deutlich ist, dass in den ersten beiden Anwendungsjahren der DSGVO zunächst die Klärung von Zuständigkeitsfragen im Vordergrund stand. Vermutlich sinkt seit 2020 die Zahl der Art.-56-Verfahren, weil für viele Verantwortliche die Rollenklärung unter den Aufsichtsbehörden nunmehr erfolgt ist. Sofern zu diesen Verantwortlichen neue Beschwerden eingehen, kann direkt in den inhaltlichen Austausch eingetreten werden. Der erneute Anstieg der Art.-56-Verfahren seit 2022 dürfte u. a. eine Spätfolge des Brexits

Entwicklung der Verfahrenszahlen



sein. Seit 2021 nimmt die englische Datenschutzaufsichtsbehörde Information Commissioner's Office (ICO) nicht mehr am Verfahren der Zusammenarbeit und Kohärenz nach der DSGVO teil. Wo bisher die federführende Zuständigkeit nach der DSGVO bei der ICO lag, musste die Zuständigkeit unter den verbliebenen Aufsichtsbehörden neu geklärt werden. Die Zuständigkeitsklärungen dauerten länger als üblich, weil sich viele EU-Niederlassungen erst in Gründung befanden. Zahlreiche Unternehmen mit vormals britischer EU-Niederlassung entschlossen sich dazu, neue Niederlassungen in den verbliebenen Mitgliedstaaten zu errichten. Diese Entwicklung ist auf die DSGVO zurückzuführen, durch die Unternehmen mit EU-Niederlassung privilegiert werden, indem sie eine federführende Aufsichtsbehörde für den gesamten Europäischen Wirtschaftsraum erhalten. Parallele Auseinandersetzungen mit mehreren Aufsichtsbehörden werden dadurch vermieden.

Noch aussagekräftiger als die Entwicklung der Art.-56-Verfahren ist der kontinuierliche Anstieg der Art.-60-Verfahren. Dieser zeigt, dass sich ab 2020 der Fokus der Zusammenarbeit zunehmend hin zur inhaltlichen Beschwerdebearbeitung verlagert hat. Nicht nur basierend auf den vorstehenden Beobachtungen scheint insgesamt das Kooperationsverfahren nach Art. 60 DSGVO von Jahr zu Jahr besser zu funktionieren. Auch der Informationsaustausch unter den europäischen Aufsichtsbehörden, von Dokumenten (199), Bearbeitungsständen (409) und die allgemeine Klärung von Rechtsfragen (37), die losgelöst von konkreten Kooperationsfällen bestehen, funktioniert laut nachstehender Grafik gut. 2023 fanden insgesamt 1078 derartige freiwillige Informationsvorgänge zwischen den europäischen Aufsichtsbehörden statt.

Bei Rechtsfragen unterstützt die ZASt die deutschen Aufsichtsbehörden bei der Herstellung einer innerdeutsch abgestimmten Rechtsauffassung und steht dazu im engen Austausch mit den Vorsitzen der Arbeitskreise der Datenschutzkonferenz (DSK).

Diese fachlich fundierten Beiträge der Expertinnen und Experten der deutschen Datenschutzaufsicht tragen maßgeblich zur Vereinheitlichung des Rechtsverständnisses bei.

Inwieweit vor diesem Hintergrund einige von der Kommission geplanten zusätzlichen Verfahrensschritte im Kooperationsverfahren im aktuell vorliegenden Entwurfsstadium erforderlich sind, erscheint zumindest begründungsbedürftig. Grundsätzlich zu begrüßen sind diejenigen Regelungsziele der Verordnung, die beispielsweise verbindliche Regelfristen auf Seiten der federführenden Aufsichtsbehörde zur Erteilung von Infor-

mationen oder zur Erledigung von Verfahrensschritten vorsehen. Wünschenswert – insbesondere aus Sicht der Beschwerdeführenden – wäre, wenn die Straffung der Fristen tatsächlich zu einer beschleunigten fachlichen Bearbeitung führen und nicht nur rein formal fristwahrende Mitteilungen auslösen. In Deutschland beansprucht zudem die föderale Meinungsbildung einen gewissen Zeitraum für eine qualitativ hochwertige Analyse und Bearbeitung, die die Beschwerdeführenden zu Recht von den Aufsichtsbehörden erwarten. Aus Sicht der ZASt als Schnittstelle der deutschen Datenschutzaufsicht nach Europa bleibt es daher in den Verhandlungen bzw. im Rahmen einer Umsetzung abzuwarten, ob durch die geplanten Rechtsanpassungen der bürokratisch-administrative Aufwand steigt, ohne dass es zu einer tatsächlichen Verfahrensbeschleunigung bei gleichzeitigem Erhalt der Bearbeitungsqualität kommt. Im Rahmen ihrer Mitwirkung an den Stellungnahmen der deutschen und europäischen Aufsichtsbehörden hat sich die ZASt für eine zielorientierte Verschlankung der vorgesehenen Abstimmungsprozesse eingesetzt, die gleichwohl ein hohes Maß an erfolgreicher europaweit gleichmäßiger Rechtsdurchsetzung verspricht.

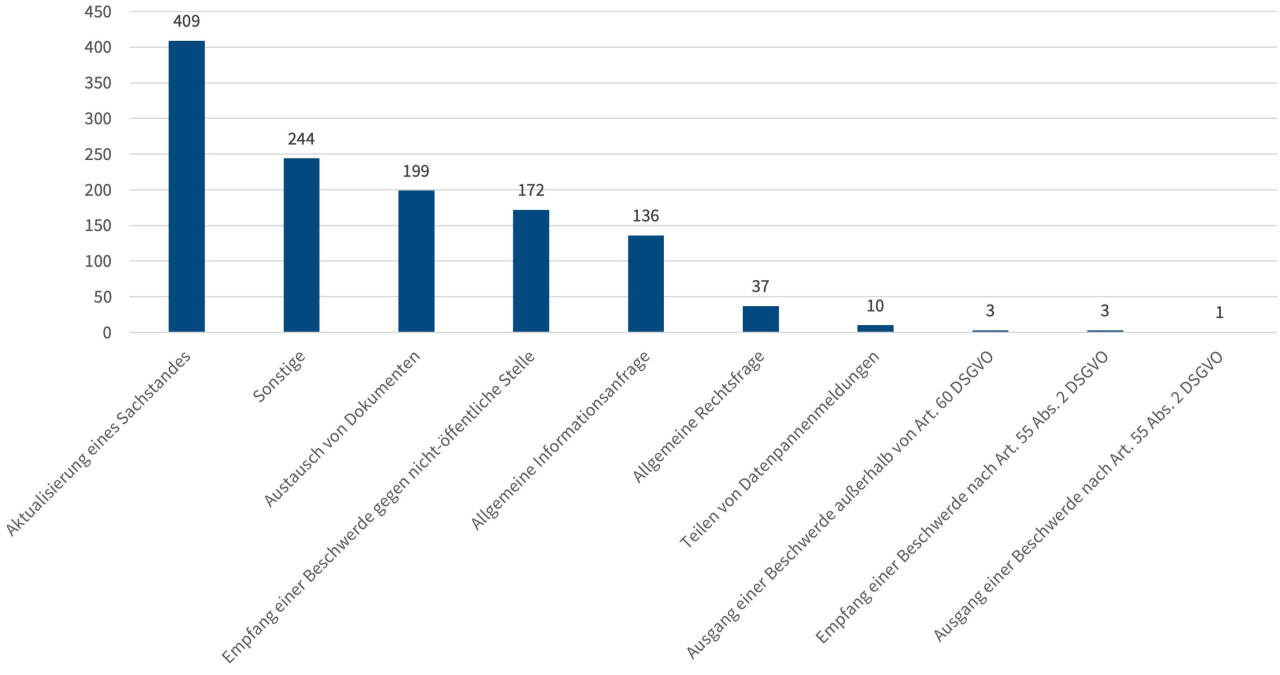
Beiträge der ZASt zum 1. BDSG-Änderungsgesetz

Im Berichtsjahr hat das Bundesministerium des Innern und für Heimat (BMI) den Entwurf für ein 1. Änderungsgesetz des Bundesdatenschutzgesetzes (BDSG) vorgelegt. Hintergrund ist der Koalitionsvertrag 2021–2025. Darin streben die Regierungsparteien eine Verbesserung der Kohärenz des Datenschutzes sowie eine Stärkung der aufsichtsbehördlichen Zusammenarbeit an. Diesen Zielen fühlt sich die ZASt als Scharnier zwischen deutscher und europäischer Datenschutzaufsicht in besonderem Maße verpflichtet. Sowohl im Vorfeld als auch im förmlichen Gesetzgebungsverfahren war die ZASt zur Praxis dieser Zusammenarbeit gefragte Ansprechpartnerin. Besonderes Augenmerk der ZASt lag hierbei auf der Sicherstellung einer durchgehend konsistenten Positionierung der deutschen Aufsichtsbehörden in den Verfahren der Zusammenarbeit und Kohärenz.

Anwenderschulung als Beitrag zur Harmonisierung der Zusammenarbeit und Rechtsanwendung der deutschen und europäischen Aufsichtsbehörden

Auch nach mehr als fünf Jahren nach Anwendungsbeginn der DSGVO besteht weiterhin hoher Schulungsbedarf bei der Anwendung des Binnenmarkt-Informationssystems (IMI). In diesem System wird in einem vollelektronischen Prozess die Abstimmung der europäischen Aufsichtsbehörden bei grenzüberschreitenden Fallbearbeitungen abgewickelt. Die ZASt hat auch im Berichtsjahr Anwenderschulungen durchgeführt und beabsichtigt, diese Angebote bedarfsorientiert aufrechtzuerhalten. Zudem werden zwei Foren angeboten, in denen die deutschen Aufsichtsbehörden in der Praxis

Freiwilliger Austausch unter den europäischen Aufsichtsbehörden 2023



auftretende Probleme lösungsorientiert adressieren und Best-Practices entwickeln.

Vereinfachung des Prozesses zur Herstellung des Einvernehmens bei wiederkehrenden Routineentscheidungen in schriftlichen Verfahren des EDSA

Um die Arbeit im Plenum bei unstreitigen Entscheidungen zu entlasten, nutzt der EDSA ein elektronisch durchgeführtes schriftliches Abstimmungsverfahren mit einwöchiger Frist. Diese kurze Zeit und die föderale Struktur Deutschlands setzt die deutschen Aufsichtsbehörden unter Zeitdruck, mit Unterstützung der ZASt einen gemeinsamen Standpunkt herzustellen, wie in dem Verfahren abgestimmt werden soll. Die deutsche Positionierung gelingt in diesen Verfahren üblicherweise im Einvernehmen.

Gleichwohl ist auch die Herstellung des Einvernehmens mit einem gewissen Aufwand für die Aufsichtsbehörden verbunden. Daher hat die DSK auf Initiative der ZASt in ihrer 1. Zwischenkonferenz am 31. Januar 2023 beschlossen, bei weiteren besonders unkritischen Abstimmungen das Verfahren zu vereinfachen. Bereits seit der 2. Zwischenkonferenz vom 22. Juni 2022 wird für Abstimmungen, in denen es lediglich um die Mandatierung bzw. Bestätigung von Berichterstattenden geht, grundsätzlich ohne gesonderte Abfrage davon ausgegangen, dass Einvernehmen besteht. Zur Wahrung ihrer Verfahrensrechte im Einzelfall hat jede Aufsichtsbehörde allerdings binnen einer von der ZASt gesetzten Frist die Möglichkeit, den Wunsch nach formeller Herstellung eines gemeinsamen Standpunktes unter Einbeziehung aller deutschen Aufsichtsbehörden vorzubringen. Nunmehr wurde das vereinfachte Verfahren auf alle EDSA-Abstimmungen in Sachen Binding Corporate Rules (BCR) und Verwaltungsvereinbarungen nationaler Abschlussprüfungsbehörden mit dem USA-Pendant Public Company Accounting Oversight Board ausgeweitet.

Im Berichtsjahr alleine wurden 40 vereinfachte Verfahren durchgeführt, was zu einer erheblichen administrativen Entlastung der deutschen Aufsichtsbehörden geführt hat.

Querverweise:

4.2.5 Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO, 5.1 Erstes Gesetz zur Änderung des Bundesdatenschutzgesetzes

11.2 Hinter den Kulissen der ZASt

Seit Geltungsbeginn der DSGVO sind die Aufsichtsbehörden des Bundes und der Länder angehalten, in Richtung des Europäischen Datenschutzausschusses (EDSA), dem Gremium aller europäischen Datenschutzaufsichtsbehörden, mit einer Stimme zu sprechen. Hier kommt die Zentrale Anlaufstelle (ZASt) ins Spiel. Als Scharnier zwischen der deutschen und europäischen Ebene unterstützt sie einen geordneten, empfänger- und verfahrensorientierten Informationsfluss in und aus beiden Sphären. Aber was bedeutet das konkret? Wir werfen einen Blick hinter die Kulissen und schauen den Mitarbeitenden der ZASt mal über die Schulter.

Die Zentrale Anlaufstelle

Die ZASt koordiniert die grenzüberschreitende Zusammenarbeit der Datenschutzaufsichtsbehörden des Bundes und der Länder mit den anderen Mitgliedstaaten der Europäischen Union, dem Europäischen Datenschutzausschuss (EDSA) und der Europäischen Kommission. Im in dieser Form europaweit einmaligen föderalen System ermöglicht sie es den Aufsichtsbehörden der EU-Mitgliedstaaten, dem EDSA und der Europäischen Kommission ohne Kenntnis der deutschen Zuständigkeitsverteilung mit den deutschen Datenschutzaufsichtsbehörden zu kommunizieren und zusammenzuarbeiten.

Die Aufgaben der ZASt beschränken sich darauf, die Datenschutzaufsichtsbehörden des Bundes und der Länder bei ihren Aufgaben zu unterstützen, ohne selbst Aufgaben der Datenschutzaufsicht wahrzunehmen. Für das Außenverhältnis gegenüber Bürgerinnen und Bürgern, Behörden und Unternehmen ist die ZASt nicht zuständig und kann insoweit nicht tätig werden.

Wie jeden Tag ist auch heute Morgen ein Mitarbeitender der ZASt dafür zuständig, die Mitteilungen zu freiwilligen Amtshilfeverfahren aus dem Binnenmarktinformationssystem IMI (IMI) an die jeweils zuständigen deutschen Aufsichtsbehörden zu verteilen. Über dieses System kommunizieren die europäischen Aufsichtsbehörden und lassen sich gegenseitig Informationen, Dokumente oder Anfragen zukommen. Alle Informationen des EDSA oder Anfragen anderer europäischer Datenschutzaufsichtsbehörden, die sich an deutsche Datenschutzaufsichtsbehörden richten, gehen mittlerweile zunächst im IMI-Postfach der ZASt ein. Und das kam so:

Im Februar 2020 gab es eine organisatorische Umstellung im IMI-Verfahren. War das IMI-Modul vorher so angelegt, dass nur eine 1:1-Kommunikation möglich war, sollte es nun auf ein Notifizierungsmodell umgestellt werden. Diese Umstellung wurde in der zuständigen Arbeitsgruppe des EDSA, der IT-Users Expert Subgroup, diskutiert. Das neue Modell hatte für die absolute Mehrheit der europäischen Aufsichtsbehörden den Vorteil, dass sie eine Anfrage, die sich an mehrere (oder sogar alle) europäischen Aufsichtsbehörden richten sollte, nicht mehr mehrmals zu stellen brauchten.

Für die deutschen Aufsichtsbehörden entstand dadurch aber zunächst ein vermeintlicher Nachteil. Denn nunmehr konnte nicht mehr eine einzelne deutsche Aufsichtsbehörde individuell kontaktiert werden, sondern nur noch alle deutschen Aufsichtsbehörden zusammen. Hierin wurde in Europa ein Konflikt mit der vertraulichen Fallbearbeitung sowie mit Datenschutzfragen gesehen, denn was nur eine deutsche Aufsichtsbehörde wissen sollte, wäre als Information bei allen deutschen Aufsichtsbehörden eingegangen. Doch auch das mit Vertreterinnen und Vertretern der ZASt, meiner Fachreferate sowie der Aufsichtsbehörden von Rheinland-Pfalz und Berlin gut aufgestellte deutsche Team der IT-Users Subgroup des EDSA konnte nicht erfolgreich auf andere technische Lösungen hinwirken. Aus Sicht der europäischen Aufsichtsbehörden ist es an Deutschland, auf nationaler Ebene eine Lösung zu finden.

Organisatorische Trennung der ZASt

Die ZASt ist zwar in meiner Behörde eingerichtet, aber organisatorisch von ihr getrennt. Das heißt, die ZASt sieht sich als Sachwalter der Interessen aller deutschen Aufsichtsbehörden des Bundes und der Länder. Dieser Anspruch wird durch eine konsequente Trennung von den anderen, insbesondere den aufsichtsbehördlichen Aufgaben sowie den Aufgaben als gemeinsamer Vertreter im EDSA auf Arbeitsebene erfüllt. Diese organisatorische Trennung soll etwaigen Interessenkollisionen entgegenwirken und sicherstellen, dass die Datenschutzaufsichtsbehörden des Bundes und der Länder beim Informationsfluss von und nach Europa gleichbehandelt werden. Die ZASt berichtet aus diesem Grunde auch direkt an die Hausleitung und ist somit unabhängig von der Fachebene.

Diese Aufgabe übernahm daraufhin die ZASt und entwickelte ein entsprechendes Lösungskonzept, nach dem im IMI eingehende Anfragen von europäischen Aufsichtsbehörden an Deutschland als Mitgliedsstaat nur noch zentral bei der ZASt eingehen. Diese sichtet die Informationen und leitet sie sodann umgehend an die richtigen innerdeutschen Stellen weiter. Ein System, das sich seither bewährt hat.

Heute befindet sich im IMI-Postfach zunächst eine Anfrage der slowakischen Datenschutzaufsichtsbehörde nach nationaler Gesetzgebung zu Videoüberwachung in kritischen Infrastruktureinrichtungen und deren Räumlichkeiten (z. B. Raffinerien, Kraftwerke und Gaswerke). Diese Anfrage leitet der ZASt-Mitarbeitende umgehend an den Arbeitskreis Videoüberwachung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weiter. Kurz darauf geht bereits die Rückmeldung ein, dass der Arbeitskreis sich um die Herbeiführung einer koordinierten deutschen Antwort an die slowakischen Kolleginnen und Kollegen kümmern wird. Manchmal geht es eben schnell.

Aber da ist noch eine Anfrage, diesmal von der französischen Datenschutzaufsichtsbehörde (CNIL). Diese untersucht derzeit eine Beschwerde, in der es um ein Auskunftsverlangen vor dem Hintergrund der Richtlinie zur Bekämpfung der Geldwäsche und einer entsprechenden Entscheidung des EuGH zu diesem Thema geht. Im Rahmen der gegenseitigen Amtshilfe interessiert sich die CNIL dafür, wie andere Aufsichtsbehörden mit der Thematik umgehen. Keine ganz alltägliche Anfrage.

Möglich wäre jedoch, dass sich einer der Arbeitskreise der DSK bereits mit der Thematik befasst hat. Der ZASt-Mitarbeitende ruft also zunächst den Vorsitzenden des Arbeitskreises Wirtschaft an, einen Mitarbeiter der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Dieser sieht keinen fachlichen Bezug zu den Aufgaben des AK Wirtschaft, leitet die Anfrage jedoch an seine Kollegin, die Vorsitzende des Arbeitskreises Kreditwirtschaft weiter. Auch diese sieht jedoch keinen fachlichen Bezug zu den Aufgaben ihres Arbeitskreises. Was ist also zu tun? Gemeinsam mit dem Referatsleiter der ZASt wird entschieden, dieses Verfahren an alle deutschen Datenschutzaufsichtsbehörden weiterzuleiten, damit diese die Anfrage der CNIL nun individuell beantworten können.

Die ZASt-Mitarbeiterin im Büro nebenan hat gerade die vom EDSA erhaltenen neuen Dokumente für ein aktuelles Streitbeilegungsverfahren über entsprechende Verteiler an alle deutschen Datenschutzaufsichtsbehörden weitergeleitet. Das muss immer schnell gehen, denn bei solchen Verfahren laufen Fristen und die Aufsichtsbehörden sind bei ihrer Arbeit auf die unverzügliche Information angewiesen.

Nun schaut sie in den vom EDSA-Sekretariat zirkulierten Zeitplan des Streitbeilegungsverfahrens, das in der Enforcement Expert Subgroup (ENF ESG) zurzeit behandelt wird. Diskutiert wird dort derzeit die Entscheidung der zuständigen federführenden Aufsichtsbehörde, der irischen Data Protection Commission (DPC), mit Blick auf die Verarbeitung personenbezogener Daten von Kindern in einem sozialen Netzwerk. Mit der in diesem Verfahren entworfenen Entscheidung der DPC waren u. a. die italienische Datenschutzaufsichtsbehörde und die Berliner Beauftragte für Datenschutz und Informationsfreiheit nicht einverstanden gewesen und hatten Einsprüche eingelegt. Sie fordern im laufenden Streitbeilegungsverfahren die Feststellung weiterer Verstöße und die Ausübung weiterer Abhilfebefugnisse durch die DPC.

Da das Streitbeilegungsverfahren sich nunmehr auf der Zielgeraden befindet, erkundigt sich die ZASt-Mitarbeiterin bereits jetzt bei den deutschen Vertretern der ENF ESG, ob es möglicherweise uneinheitliche Sichtweisen der deutschen Datenschutzaufsichtsbehörden gibt. Sollte dies der Fall sein, müsste rechtzeitig vor der Entscheidung im EDSA ein gemeinsamer Standpunkt eingeholt werden, den die ZASt koordinieren würde. Denn Deutschland hat wie jedes EDSA-Mitglied nur eine Stimme, trotz seiner insgesamt 18 Datenschutzaufsichtsbehörden. Bei Uneinigkeit unter diesen stünde erst nach Einholung eines gemeinsamen Standpunktes fest, ob Deutschland im Plenum des EDSA dem Beschuss zustimmen kann oder nicht.

Glücklicherweise ist das Telefonat heute kurz. Der Vertreter der Länder in der ENF ESG, ein Mitarbeiter des Landesdatenschutzbeauftragten für den Datenschutz Niedersachsen, hat bereits informell die Meinungen abgefragt und keine Einwände erhalten. Wie so häufig in der vertrauensvollen Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder, besteht also auch hier Einigkeit unter den deutschen Datenschutzaufsichtsbehörden und ein formelles Verfahren zur Feststellung eines gemeinsamen Standpunkts ist nicht erforderlich.

Der ZASt-Mitarbeiter im Nebenzimmer brütet gerade über dem neuen Entwurf der Europäischen Kommission für eine Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO. Was würde sich durch das vorgeschlagene Verfahren ändern? Was bedeutet das für das föderale System und die bereits eingerichteten Prozesse? Zu jeder einzelnen Fallgestaltung gibt es bereits Kommunikationsstränge, die von den deutschen Aufsichtsbehörden gemeinsam mit der ZASt beleuchtet wurden und bei denen um möglichst passende Lösungen in den Arbeitskreisen der DSK gerungen wurde. Die ZASt muss hier die Bedürfnisse aller deutschen Aufsichtsbehörden im Blick behalten und vor diesem Hintergrund ihre Stellungnahme gegenüber der bei der DSK eingerichteten „Taskforce Verfahrensverordnung“ abgeben. Diese Arbeit wird jedoch noch eine Weile in Anspruch nehmen und dabei wollen wir nicht weiter stören.

Interview

Julian A. Terrero Gelhaus arbeitet bereits seit mehr als vier Jahren bei der ZASt. Bei ihm haben wir uns erkundigt, was seine Arbeit dort ausmacht.

Hallo Julian, Arbeitskreise, DSK, Europa … wie behält man da den Überblick?

Ja, wir sind da in der Tat eine Art Schnittstelle. Wir haben den ersten Zugriff auf zahlreiche unterschiedliche Dokumente oder Anfragen, die im Binneninformationssystem IMI aus Europa eingehen und sind daher häufig die ersten in Deutschland, die sich damit befassen. Dabei müssen wir verstehen, worum es im Kern geht. In die tiefere datenschutzrechtliche Bewertung steigen wir dabei aber in der Regel nicht ein. Dies obliegt natürlich den Fachbereichen der Aufsichtsbehörden in Deutschland, die diese Informationen so schnell wie möglich erhalten sollen. Unser Fokus liegt auf dem reibungslosen Ablauf. Wir organisieren, sortieren, ordnen zu oder leiten weiter.

Englisch ist dabei ein „Muss“, oder?

Ohne Englisch geht es nicht, das muss man ganz klar sagen. Selbst wenn man nicht wie ich in einer Arbeitsgruppe des EDSA sitzt, sind einfach viele Dokumente, mit denen man zu tun hat, zunächst nur auf Englisch vorhanden. Aber das ist auch ein wesentlicher Teil, der mir persönlich besonderen Spaß macht. Und wer sich noch nicht hundertprozentig sattelfest in der englischen Sprache fühlt, der kann parallel auch einen Sprachkurs belegen, der während der Arbeitszeit wahrgenommen werden kann. Es ist aber auch nicht nur die Sprache, die sich bei der Arbeit im EDSA ändert. Man muss sich auch auf eine andere Kultur der Kommunikation einlassen können.

Ach ja? Welche denn zum Beispiel?

Auf europäischem Parkett gibt es eben bestimmte Gepflogenheiten, mit denen man sich vertraut machen muss. Das betrifft zum Beispiel die Art und Weise in der man seine Meinung und eben manchmal auch Kritik äußert. Die Interessen sind schließlich nicht immer gleichgelagert, das ist bei einer so großen Zahl von europäischen Aufsichtsbehörden mit unterschiedlichen nationalen Rechtssystemen ja auch nachvollziehbar.

Man möchte respektvoll und auch vertrauensvoll zusammenarbeiten. Vielleicht könnte man es auch einfach „diplomatisches Feingefühl“ nennen, das hier erforderlich ist. Da kommt man aber schnell rein, wenn man ein gutes Gefühl für diese „Zwischentöne“ hat. Und die Kolleginnen und Kollegen der ZASt unterstützen auch immer gerne, gerade in der Anfangszeit.

Oft ist die Rede von eingerichteten Prozessen für die Zusammenarbeit zwischen den Aufsichtsbehörden. Aber was passiert, wenn es noch keinen Prozess für eine bestimmte Situation gibt?

Das kann hin und wieder mal vorkommen.

Ohnehin schauen wir ja auch immer, ob es weiteren Optimierungsbedarf bei den eingerichteten Prozessen zur Zusammenarbeit zwischen den deutschen Aufsichtsbehörden gibt. Sobald wir für neue Prozesse Abstimmungs- oder für bestehende Abläufe Optimierungsbedarf erkennen, tragen wir das Thema in der Regel mit eigenen Vorschlägen zunächst in die relevanten Arbeitskreise der DSK, wo sie besprochen und analysiert werden. In der DSK werden die im jeweiligen Arbeitskreis erarbeiteten Vorschläge dann zwischen den Leitungen der Aufsichtsbehörden erörtert und in entsprechende Vorgaben zur Zusammenarbeit gegossen, an die sich dann alle halten.

Aber auch darüber hinaus stehen wir im engen und vertrauensvollen Austausch mit den deutschen Aufsichtsbehörden, wann immer es um Sachverhalte mit europäischem Bezug handelt. Zudem behalten wir als zentrale Schnittstelle den Überblick, indem wir uns gezielt informieren und bestimmte Vorgänge statistisch auswertbar erheben und dokumentieren.

Zudem bieten wir den Aufsichtsbehörden des Bundes und der Länder Fortbildungen und Praktikerworkshops rund um das Binnenmarktinformationssystem IMI an (31. TB Nr. 11.1).

Ich nehme an, dass bei dieser vielfältigen Tätigkeit auch die Absprachen innerhalb des Teams einen wichtigen Stellenwert einnehmen?

Das kann ich voll und ganz bestätigen. Wir arbeiten alle wirklich eng zusammen, tauschen uns aus und es gibt immer jemanden, den man fragen kann. Wir versuchen auch, vorhandenes Wissen zu dokumentieren, sodass jeder Zugriff darauf hat, auch wenn die verantwortliche Person mal nicht im Dienst sein sollte. Auch bezüglich der Arbeitszeiten ergänzen wir uns gut. Einige fangen gerne früher an, um früher in den Feierabend gehen zu können. Andere starten lieber etwas später, z. B. weil erst die Kinder versorgt werden müssen, und bleiben dann etwas länger. So können wir einen breiten Zeitraum anbieten, in dem die ZASt gut ansprechbar ist. Manchmal ist das auch wirklich erforderlich, z. B. wenn Dienstagabend Dokumente für die Sitzung am Mittwochvormittag eingehen. Da dürfen wir dann nicht das Nadelöhr sein! Und für einen gemeinsamen Kaffee zwischendurch findet sich auch immer eine Gelegenheit.

Zum Abschluss noch eine letzte Frage: Was macht Dir persönlich am meisten Spaß bei der Arbeit?

Das Kommunikative und das Vertrauen, das sich entwickelt, sowie gestalten zu können! Wir müssen uns oft austauschen, mit Kolleginnen und Kollegen bei den Aufsichtsbehörden der Länder, beim BfDI oder beim EDSA oder mit den Vorsitzenden der Arbeitskreise u.s.w. Da es meistens schnell gehen muss, nehmen wir hierbei in der Regel als Erstes den Hörer in die Hand. So haben wir immer den persönlichen Kontakt. Wir sind oft auch erster Ansprechpartner, wenn es Fragen gibt oder etwas nicht läuft. Da kann es auch schon mal passieren, dass man die Sorgen und Nöte der Aufsichtsbehörden aus erster Hand erfährt. Ein wenig Einfühlungsvermögen benötigt man dabei auch, schließlich läuft nicht alles überall gleich und die unterschiedlichen Aufsichtsbehörden haben eben auch ihre eigenen Anforderungen und Bedürfnisse. Da geht es nicht immer nach „Schema-F“, schließlich wollen wir alle Akteure bestmöglich unterstützen. Das macht das Ganze so schön abwechslungsreich.

Lieber Julian, vielen Dank für das Gespräch!

Querverweise:

4.2.5 Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO

12 Positives

12.1 Ein Beispiel guter Zusammenarbeit

Von einer rechtzeitigen Einbindung meiner Behörde in die Entwicklung neuer Projekte profitieren alle Seiten.

Die Wahrnehmung meiner Aufgaben besteht auch in der Kritik an bestehenden Verfahren und Vorgehensweisen der Verantwortlichen in Bezug auf die Verarbeitung personenbezogener Daten. Nach der Aufdeckung von Missständen erfolgen gegebenenfalls konkrete Abhilfemaßnahmen oder Sanktionen. Zum Selbstverständnis meiner Aufgabenstellung gehört es, die Entscheidungsträger in Politik und Verwaltung sowie die interessierte Öffentlichkeit über meine Aktivitäten und Erfahrungen zu informieren.

Darüber hinaus ist es mir aber auch ein Anliegen, Berichtenswertes aus dem großen Bereich der Beratung zu Fragestellungen des Datenschutzes sowohl der meiner Aufsicht unterstehenden Stellen als auch der mich anrufenden Bürgerinnen und Bürger zur Sprache zu bringen. Beides macht einen wesentlichen Teil der täglichen Arbeit meiner Mitarbeiterinnen und Mitarbeiter aus. Hier stelle ich fest, dass zunehmend mein Angebot angenommen wird, möglichst frühzeitig bei Gesetzesvorhaben oder vor der Einführung neuer Verfahren, die eine nicht unerhebliche Verarbeitung personenbezogener Daten zum Gegenstand haben werden, meine Beratung zu suchen. Solche erfreulichen Entwicklungen sollen daher nicht unerwähnt bleiben.

So hat mich etwa das Statistische Bundesamt (StBA) schon früh in die Vorbereitung diverser neu aufgelegter Projekte eingebunden, bei denen datenschutzrechtliche Auswirkungen zu bedenken waren und gesetzeskonforme Lösungen gefunden werden mussten. Beispielhaft seien hier erste vorbereitende Maßnahmen im Hinblick auf die künftige Durchführung eines registergestützten Zensus, der Aufbau eines Verfahrens für einen Datenfernzugriff (Remote Access) durch wissenschaftliche Einrichtungen auf faktisch anonymisierte Datensätze des eigenen Forschungsdatenzentrums oder die konkrete Einrichtung eines Unternehmens-Basisregisters beim StBA genannt. In diesen Projekten hat mir das StBA seine Überlegungen in schriftlicher Form zukommen lassen und mir in Besprechungen die Vorhaben erläutert. Zu den aktuellen Vorhaben des Bundesamts im Bereich der Erschließung neuer digitaler Daten und deren Nutzung zu statistischen Zwecken hat sich bereits über mehrere Jahre ein regelmäßiger Informationsaustausch etabliert.

Von diesem weitsichtigen Vorgehen profitieren alle Beteiligten. Mir wird die Möglichkeit eröffnet, schon in einem frühen Entwicklungsstadium auf etwaige datenschutzproblematische Folgen hinzuweisen und so aktiv zu einem datenschutzfreundlichen Produkt beizutragen. Das Bundesamt gewinnt Zeit und Anstöße zur Entwicklung möglicher alternativer Vorgehensweisen und vermeidet spätere Restriktionen zur (Wieder-) Herstellung von Datenschutzkonformität. Hauptprofiteure sind jedoch die Nutzerinnen und Nutzer des neuen Verfahrens als mögliche Betroffene der vorgesehenen Datenverarbeitungen, deren Recht auf informationelle Selbstbestimmung auf diese Weise von vornherein gewahrt werden kann.

12.2 Verbesserungen am Vorgangsbearbeitungssystem des Bundeskriminalamtes

Das Bundeskriminalamt (BKA) setzt datenschutzrechtliche Anpassungen an seinem Vorgangsbearbeitungssystem (VBS) um. Das umfangreiche Projekt verspricht eine gelungene Symbiose zwischen Datenschutz und effektiver Polizeiarbeit.

Nach einer datenschutzrechtlichen Kontrolle habe ich im Jahr 2019 mehrere, zum Teil erhebliche, datenschutzrechtliche Defizite des VBS angemahnt (28. TB Nr. 6.7.3, 29. TB Nr. 9.5.3, 30. TB Nr. 8.2.2). Zunächst folgte das für die Fachaufsicht über das BKA zuständige Bundesministerium des Innern und für Heimat meinem rechtlichen Standpunkt in wesentlichen Aspekten nicht (29. TB

Nr. 9.5.3). Nachdem das BKA meine Beratungsleistungen in Form von gemeinsamen Workshops in Anspruch genommen hatte, legte es im Herbst 2022 ein Konzept zur Umsetzung meiner Forderungen aus dem Kontrollbericht 2019 vor (vgl. 31. TB Nr. 12.6). Inzwischen hat das BKA ein Fachkonzept erstellt und mit technischen Anpassungen begonnen. In einem Workshop im Sommer 2023 habe ich mich über den aktuellen Stand informiert und das BKA bei der weiteren Umsetzung beraten.

Die technischen Anpassungen im VBS betreffen insbesondere die Datenspeicherung, Such- und Recherchefunktionen. Mit den Anpassungen des VBS wird die Datenqualität und die Datenverarbeitung im Sinne des Datenschutzes erheblich verbessert. Ganz besonders freut es mich, dass die datenschutzrechtlichen Anpassungen das BKA auch polizeifachlich weiterbringen. Dies verdeutlicht, dass guter Datenschutz und gute Polizeiarbeit keine Gegensätze sein müssen.

12.3 E-Rezept

Das E-Rezept findet 2023 größere Verbreitung. Auch durch meine Beratung konnte die Sicherheit eines alternativen, barrierearmen Einlösewegs von E-Rezepten erheblich verbessert werden.

Bereits im Jahr 2020 wurde mit dem Patientendaten-Schutz-Gesetz in den §§ 360 und 361 Sozialgesetzbuch V (SGB) festgelegt, dass ärztliche Verordnungen ab dem 1. Januar 2022 elektronisch über die Telematikinfrastruktur (TI) übermittelt werden müssen. Das sogenannte E-Rezept ist damit die erste medizinische Pflichtanwendung überhaupt. Nach mehreren Verzögerungen und gestoppten Tests in einzelnen Regionen hat sich das E-Rezept seit Sommer 2023 weiterverbreitet.

Rezepte im Rahmen der vertragsärztlichen Versorgung werden in der Anwendung E-Rezept immer in einem zentralen Speicher in der TI abgelegt. Patientinnen und Patienten können dann nur wählen, ob sie die Zugangsinformationen dazu in elektronischer Form oder als Papierausdruck mit einem Code-Block zur Einlösung in einer Apotheke ausgehändigt bekommen wollen. Die Vorteile der Digitalisierung ergeben sich, wenn Patientinnen und Patienten auf den Papierausdruck verzichten können, weil sie ihre Rezepte mit der E-Rezept-App über die TI abrufen und dann auch sicher an die Apotheken zuweisen können.

In meinem 31. Tätigkeitsbericht habe ich darüber berichtet, dass ich die gematik im damaligen Berichtszeitraum zu weiteren Einlösewegen des E-Rezepts beraten hatte.

Die gematik hatte ein Verfahren vorgeschlagen, bei dem Versicherte in den Apotheken ihre elektronische Gesundheitskarte (eGK) in das Kartenlesegerät (ohne PIN-Eingabe) stecken und die Apotheke so alle E-Rezepte vom zentralen E-Rezepte-Server abrufen kann. Diese Funktionalität hatte ich als eine barrierearme Möglichkeit begrüßt, E-Rezepte in den Apotheken einzulösen. Die erste von der gematik konkrete vorgeschlagene technische Umsetzung hatte allerdings erhebliche Mängel aufgezeigt. Dass Unbefugte beispielsweise auf fremde Rezeptdaten zugreifen könnten, hätte ein hohes Risiko für alle Versicherten bedeutet. Ich hatte dieser Lösung deshalb nicht zugestimmt. Gleichzeitig hatte ich Vorschläge unterbreitet, wie die Funktion sicher umgesetzt werden könnte, ohne dabei Komfort für Versicherte einzubüßen.

Hierzu haben im Berichtszeitraum Beratungen mit der gematik stattgefunden. Die gefundene Lösung entspricht einem meiner Vorschläge: Nachdem Versicherte ihre eGK in der Apotheke gesteckt haben, erhält das Apothekenverwaltungssystem darüber von der TI digital im Hintergrund einen fälschungssicheren Nachweis. Nur mit diesem Nachweis gibt der E-Rezept-Server die E-Rezepte frei. Dieser Umsetzung habe ich zugestimmt. Die Sicherheit wird dabei signifikant erhöht, ohne dass sich das Verfahren für Versicherte oder Apotheken ändert.

Die eGK nimmt auch ohne PIN durch diesen neuen Einlöseweg des E-Rezeptes und Änderungen im Zuge des Digital-Gesetzes in ihrer Bedeutung zu. Der Ausgabeprozess muss entsprechend überarbeitet werden, sodass unbefugte Dritte sie nicht nutzen können, um Zugang zu Gesundheitsdaten zu erlangen.

Querverweise:

3.1.3 Beschleunigung der Digitalisierung im Gesundheitsbereich durch ein Digital-Gesetz

12.4 Einsatz von Bodycams nach § 27a Bundespolizeigesetz

Meine Kontrolle führt zu Klarstellungen zum Einsatzort der Bodycams.

Im Jahr 2017 wurde im Bundespolizeigesetz (BPolG) mit § 27a eine Rechtsgrundlage für den Einsatz von mobilen Bild- und Tonaufzeichnungsgeräten geschaffen, allgemein bekannt als Bodycams. Danach kann die Bundespolizei unter bestimmten Voraussetzungen Bild und Tonaufzeichnungen mittels Bodycams an öffentlich zugänglichen Orten anfertigen. Dies habe ich im September 2021 kontrolliert.

Bei dieser Kontrolle sind mir einige Mängel und Verstöße aufgefallen. Bodycamaufnahmen an nicht öffentlich zugänglichen Orten musste ich beanstanden. Zum Einsatz und zur Handhabung der Technik habe ich mehrere Empfehlungen ausgesprochen. Erfreulicherweise hat das Bundesministerium des Innern und für Heimat (BMI) – als Fachaufsicht – die Beanstandung aufgegriffen und den Begriff des „nicht öffentlich zugänglichen Ortes“, der im aktuellen BPolG nicht näher erläutert wird, in einem internen Erlass genauer konkretisiert. So wird beispielsweise geklärt, dass Gewahrsamsbereiche keine öffentlich zugänglichen Orte sind und dort daher nach aktueller Rechtslage keine Bodycamaufnahmen zulässig sind. Gleiches gilt unter anderem für Dienstfahrzeuge der Bundespolizei. Somit gibt es nun für die Vollzugsbeamten klarere Anweisungen, wo die Bodycams eingesetzt werden dürfen und wo nicht.

Der Entwurf des neuen BPolG enthält eine klarer formulierte Norm zum Einsatz der Bodycams sowie eine zusätzliche Norm zum Einsatz von Videoaufzeichnungen in Gewahrsamsräumen. Daher halte ich auch unter diesem Aspekt die Einführung des überarbeiteten BPolG für dringend notwendig.

Querverweise:

3.3.2 Modernisierung des Bundspolizeigesetzes

12.5 Kindeswohlstudie

Das laufende Gerichtsverfahren zu meinem Bescheid vom 17. Februar 2021 gegenüber dem Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) konnte durch einen Vergleichsschluss beendet werden.

Das BMFSFJ hatte gegen meinen Bescheid vom 17. Februar 2021 Klage erhoben. Ich hatte angeordnet, alle Rohdaten, Auswertungen inklusive Tabellen und Forschungsergebnisse, d. h. Zwischenberichte, Berichte, Endergebnisse der Studie „Kindeswohl und Umgangsrecht“ nach Art. 18 DSGVO unverzüglich in der Verarbeitung einzuschränken. Zur Beendigung dieser gerichtlichen Auseinandersetzung habe ich mich mit dem BMFSFJ nunmehr auf einen Vergleich geeinigt, der im Wesentlichen Folgendes beinhaltet: Das BMFSFJ räumte datenschutzrechtliche Verstöße bei der Erstellung der Studie ein und sicherte zu, dass die Studie Kindeswohl keinen Personenbezug und keine Personenbeziehbarkeit mehr aufweist. Die Klage gegen den Bescheid meiner Behörde wurde zurückgenommen. Im Gegenzug habe ich eine datenschutzrechtliche Verwarnung ausgespro-

chen und angeordnet, die personenbezogene Datenbasis nicht weiterzuverwenden. Einer Veröffentlichung der bereits vorliegenden Entwurfsfassung und der finalen Fassung der Studie ohne personenbezogene Daten habe ich jedoch zugestimmt.

12.6 Deutsche Akkreditierungsstelle stellt Videokonferenzsystem um

Aufgrund meiner frühzeitigen und engmaschigen Beratung konnte die Deutsche Akkreditierungsstelle (DAkkS) ihr Videokonferenzsystem auf sichere datenschutzfreundliche Füße stellen.

Vor dem Hintergrund der zurückliegenden Corona-Pandemie sah sich die DAkkS mit der Herausforderung konfrontiert, sogenannte Fernbegutachtungen bzw. Remote-Witnessaudits immer weiter in ihre Akkreditierungspraxis zu integrieren. Die DAkkS stellte daher das bislang für Videokonferenzen eingesetzte System auf den Prüfstand und bat mich im Kontext möglicher Übermittlungen personenbezogener Daten in Drittstaaten um Beratung.

Meine Hinweise führten bei der DAkkS im Ergebnis zur zwischenzeitlichen Umstellung ihres Videokonferenzsystems auf ein datenschutzfreundliches System, das seit dem 1. September 2023 im ausschließlichen Wirkbetrieb ist. Hierbei handelt es sich um eine in Deutschland entwickelte Software für Videokonferenzen, die eine datenschutzgemäße Nutzung unter anderem durch das Unterbinden von Aufzeichnungen ermöglicht. Des Weiteren wird die Übertragung der Videokonferenzdaten nach dem Stand der Technik, entsprechend den einschlägigen Technischen Richtlinien des BSI, transportverschlüsselt. Auch werden dem Anbieter zufolge ausschließlich zertifizierte Rechenzentren in Deutschland und dem Europäischen Wirtschaftsraum genutzt. Bei einem Beratungs- und Kontrollbesuch konnten sich meine Mitarbeiterinnen und Mitarbeiter von der Datenschutzfreundlichkeit der neuen Software überzeugen.

Durch die frühzeitige Beratungsanfrage der DAkkS konnte ich meine Erfahrungen und Einschätzungen bereits bei der Beauftragung des neuen Videokonferenzsystems umfassend einbringen, so dass Datenschutzverstöße bzw. teurere und zeitintensivere Maßnahmen zur Herstellung eines datenschutzkonformen Zustands vermieden werden konnten. Ein Gewinn für das Unternehmen, die von der Datenverarbeitung betroffenen Personen und meine Aufsichtstätigkeit.

12.7 Besondere Beteiligung des BfDI bei Anhörungen im Bundestag

Zum 1. Januar 2023 änderte der Deutsche Bundestag seine Geschäftsordnung. Ziel war, die Beratungen in den Ausschüssen durch regelmäßige öffentliche Sitzungen, die Veröffentlichung von Ausschussunterlagen im Internet und „klare Regeln zur Benennung von Sachverständigen für öffentliche Anhörungen“ transparenter und für die Öffentlichkeit nachvollziehbarer zu machen.

Teil der auch unter dem Aspekt der Informationsfreiheit begrüßenswerten Anpassungen war auch die Einführung eines besonderen Beteiligungsrechtes des BfDI bei öffentlichen Anhörungen der Ausschüsse (§ 69a Abs. 3 GOBT).

§ 69a Abs. 3 GOBT

Betrifft eine Anhörung gemäß § 70 Absatz 1 durch den federführenden Ausschuss Gesetzentwürfe, die in erheblicher Weise die Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten betreffen, ist auf Beschluss des Ausschusses oder auf Verlangen eines Viertels seiner Mitglieder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Gelegenheit zur Teilnahme an der Anhörung zu geben. Abs. 2 Satz 3 und 4 gilt entsprechend.

Wenn es um Gesetzentwürfe geht, die in erheblicher Weise den Schutz personenbezogener Daten betreffen, soll ich bei allen Sachverständigenanhörungen im federführenden Ausschuss Gelegenheit zur Teilnahme gegeben werden. Voraussetzung ist, dass mindestens ein Viertel der Ausschussmitglieder meine Beteiligung unabhängig von der Anrufung durch eine Fraktion verlangt.

Mit Blick auf die Vorgaben der DSGVO zur beratenden Einbindung der Datenschutzaufsicht in legislative Prozesse (Art. 57 Abs. 1 lit. c) und 58 Abs. 3 lit. b) DSGVO) ist dies sachgerecht und entspricht meinen Vorschlägen. Mit der Änderung wird meine Rolle als unabhängiges und überparteiliches Beratungsorgan des Bundestages gestärkt, da es formal nicht länger erforderlich ist, zwingend von einer einzelnen Fraktion als Sachverständiger benannt zu werden.

Mit der getroffenen Änderung gibt es aber keinen Automatismus meiner Einbeziehung bei Sachverständigenanhörungen, da diese auch bei offenkundiger datenschutzrechtlicher Relevanz noch einen Beschluss im Ausschuss voraussetzt. Daher habe ich weiterhin immer wieder proaktiv auf die Sinnhaftigkeit meiner Beteiligung hingewiesen und hoffe, dass diese neue Möglichkeit des „Vor-die-Klammer-Ziehens" in der Zukunft von den Ausschüssen regelmäßig als Mehrwert für den legislativen Prozess erkannt und genutzt wird.

Einen weiteren Optimierungsbedarf im Zusammenhang mit meiner Beteiligung nach der neuen Geschäftsordnung bestand noch mitunter in der fehlenden Möglichkeit, wie die „klassischen" Sachverständigen nicht nur für Fragen zur Verfügung zu stehen, sondern meine Positionen im Rahmen eines Eingangsstatements darstellen zu können. Ich bin aber optimistisch, dass sich auch dies mit der Zeit zur Zufriedenheit Aller noch einspielen wird.

Für eine weitere Anpassung der Geschäftsordnung des Deutschen Bundestages oder des BDSG rege ich weiterhin an, meiner Behörde formal den Zugang zu den Beratungen und Unterlagen der Ausschüsse von Bundestag und Bundesrat einzuräumen. Auch hier gab es in der Vergangenheit vereinzelt Probleme. Dies verwundert umso mehr, als dass meine immerhin oberste Bundesbehörde vor ihrer Unabhängigkeit dieses Recht als damaliger Teil der Bundesregierung unproblematisch bereits innehatte.

Die Effektivität der mir gesetzlich obliegenden Beratung gegenüber Regierung und Parlament korrespondiert mit dem Zeitpunkt und dem Umfang meiner Einbeziehung. Nicht zuletzt deshalb setze ich mich weiterhin auch dafür ein, dass mein Tätigkeitsbericht – vergleichbar der Wehrbeauftragten – im Plenum des Deutschen Bundestages vorgestellt und dort gemeinsam erörtert wird. Dies trüge auch der infolge der Digitalisierung erheblich gestiegenen öffentlichen Bedeutung des Datenschutzes Rechnung.

12.8 Unterstützung der Bundesregierung bei Streithilfe zu Gunsten des EDSA

Die Bundesregierung unterstützt den Europäischen Datenschutzausschuss (EDSA) als Streithelferin vor dem Europäischen Gerichtshof (EuGH) und verteidigt das von der Datenschutz-Grundverordnung (DSGVO) vorgesehene System der Streitbeilegung.

Die einheitliche Anwendung der DSGVO sicherzustellen, ist eine der wichtigsten Aufgaben des EDSA. Dazu dient auch das Kohärenzverfahren, in dem der EDSA Meinungsverschiedenheiten zwischen den Aufsichtsbehörden schlichtet. Im Anschluss an viele Kohärenzverfahren findet sich der EDSA jedoch mittlerweile selbst als beklagte Partei vor den Gerichten der Europäischen Union (EU) wieder. Dies ist systemwidrig. So hat das Gericht der Europäischen Union auch bestätigt, dass Klagen von datenschutzrechtlich Verantwortlichen gegen verbindliche Beschlüsse des EDSA vor den Unionsgerichten unzulässig sind.[111]

Gegen dieses Urteil wurde ein Rechtsmittelverfahren vor dem EuGH eingelegt. Ich habe erfolgreich angeregt, dass die Bundesregierung diesem Verfahren als Streithelferin zu Gunsten des EDSA beitritt und sie bei der Erstellung eines Streithilfeschriftsatzes unterstützt. Selbstverständlich gebietet das Rechtsstaatsprinzip, dass Unternehmen gegen jede an sie adressierte behördliche Entscheidung der Rechtsweg offensteht. Am Ende des Kohärenzverfahrens steht aber immer die finale Entscheidung einer nationalen Aufsichtsbehörde, gegen die vor den nationalen Gerichten geklagt werden kann. Solange das Prinzip der dezentralen Durchsetzung durch die nationale Exekutive fortbesteht („One-Stop-Shop") und dem EDSA selbst keine Ermittlungs- und Durchsetzungsbefugnisse zustehen, sollte sich diese Aufgabenverteilung auch auf der Ebene der Judikative entsprechend widerspiegeln.

12.9 Digitale Beantragung von Visa und Reisepässen

In Umsetzung des Online-Zugangsgesetzes stellt das Auswärtige Amt (AA) Schritt für Schritt Dienstleistungen der deutschen Auslandsvertretungen online zur Verfügung. Das Auslandsportal ist die Plattform, auf der alle online verfügbaren Informationen zusammengeführt und Verwaltungsleistungen in Anspruch genommen werden können.

In meiner bisherigen Kontroll- und Beratungspraxis im Hinblick auf das Verfahren zur Beantragung von Visa musste ich die Fehleranfälligkeit des papiergebundenen Verfahrens zur Beantragung von Visa oft feststellen. Sowohl der Transport der umfangreichen Dokumente

111 EuG (Urteil vom 07. Dezember 2022, Az. T-709/21), abrufbar unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=268419&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=520470

von den Auslandsvertretungen nach Deutschland, als auch die weitere Beteiligung der Inlandsbehörden (z. B. Ausländerbehörden, Bundesagentur für Arbeit) bergen ein hohes Risiko für Verlust, unbefugte Offenbarung von (sensiblen) personenbezogenen Daten, aber auch Verzögerungen bei der Bearbeitung. Mit der Möglichkeit, die Dienstleistungen online zu beantragen, besteht die Aussicht auf eine medienbruchfreie Weiterleitung an die Inlandsbehörden auf elektronischem Weg. Im Vergleich zur Beantragung „am Schalter", sehe ich eine höhere Wahrscheinlichkeit, dass sich die Antragstellenden bei der Online-Beantragung der Dienstleistungen in Ruhe mit den ihnen zustehenden Datenschutzrechten auseinandersetzen können. Ich begrüße daher die nunmehrige Pilotierung des Auslandsportals im Bereich der Visa- und Reisepassbeantragung.

Das AA bat mich im Laufe des Verfahrens um Beratung. Nach meiner bisherigen Einschätzung denkt das AA hier die datenschutzrechtlichen Implikationen von Beginn an mit. Unabhängig davon stehe ich weiterhin als Ansprechpartner für die weitere datenschutzkonforme Ausgestaltung des Auslandsportals als auch bei der Digitalisierung der Verwaltungsverfahren zur Verfügung.

Dies gilt insbesondere auch für die Frage, in welcher Form der Einsatz von Künstlicher Intelligenz im Rahmen der digitalisierten Verfahrensbearbeitung datenschutzkonform möglich ist.

Im Zuge der technischen Fortentwicklung und der Aufnahme weiterer Antragsarten und Auslandsvertretungen in das Auslandsportal sollte aber auch die Notwendigkeit des Einsatzes externen Dienstleister im Rahmen der Beantragung von Visa einer kritischen Überprüfung durch das AA unterzogen werden. Es liegt auf der Hand, dass die Einschaltung von Unternehmen in Ländern außerhalb des Geltungsbereichs der DSGVO und nicht selten ohne entsprechend angemessenes Datenschutzniveau, datenschutzrechtlichen Risiken unterliegt, die es zu vermeiden gilt.

Querverweise:

9.2.4 Datenschutzrechtlicher Beratungs- und Kontrollbesuch bei den Auslandsvertretungen in Kasachstan

Anlagen

Anlage 1

Kontrollierte Stellen

Acht Unternehmen zum SÜG

1&1 Mail & Media Applications SE

Auswärtiges Amt, Botschaft Dakar

Autobahn GmbH

Bike Syndikat Kurierdienst GbR

BITMARCK

BKK ZF & Partner

Bundeamt für Justiz

Bundesagentur für Arbeit

Bundesamt für den Militärischen Abschirmdienst

Bundesamt für die Sicherheit in der Informationstechnik

Bundesamt für Migration und Flüchtlinge

Bundesamt für Verfassungsschutz

Bundesanstalt für Ernährung und Landwirtschaft

Bundesanstalt für Landwirtschaft und Ernährung

Bundesanstalt für Materialforschung und -prüfung

Bundeseisenbahnvermögen

Bundeskartellamt

Bundeskriminalamt

Bundesministerium für Digitales und Verkehr

Bundesministerium für Familie, Senioren, Frauen und Jugend

Bundesministerium für Gesundheit

Bundesministerium für Wirtschaft und Klimaschutz

Bundesnachrichtendienst

Bundesnetzagentur

Bundespolizei

Bundespolizeiakademie

Bundespolizeidirektion Berlin

BWI GmbH

BWPOST GmbH & Co. KG

Deutsche Akkreditierungsstelle GmbH

Deutsche Rentenversicherung Bund

Deutscher Bundestag

Deutsches Zentrum für Luft- und Raumfahrt

DHL Express Germany GmbH

DHL Paket GmbH

Dienstältester Deutscher Offizier/ Deutscher Anteil 1st NATO Signal Battalion

DPD Deutschland GmbH

Eisenbahn-Bundesamt

FedEx Express Deutschland GmbH

Financial Intelligence Unit

Finanzamt Flensburg

General Logistics Systems Germany GmbH & Co. OHG

Generalzolldirektion

Hauptzollamt Köln

Hermes Germany GmbH

Informationstechnikzentrum Bund

Jobcenter Freiburg

Jobcenter Landkreis Celle

Jobcenter Mainz

Jobcenter Rhein-Sieg-Kreis

Jobcenter Stadt Bamberg

Knappschaft Bahn-See

MZZ-Briefdienst GmbH

Postfiliale Getränke Hoffmann GmbH

Scheval (Finnland)

Stashcat GmbH

SVLFG Berufsgenossenschaft

Telefónica Germany GmbH & Co. OHG

Telekom Deutschland GmbH

Thüringer Netkom GmbH

T-Systems International GmbH

United Parcel Service Deutschland S.à r.l. & Co. OHG

Vodafone GmbH

Wasserstraßen- und Schifffahrtsamt Spree-Havel

Wasserstraßen- und Schifffahrtsamt Weser-Jade-Nordsee

Wasserstraßen-Neubauamt Datteln

Zollkriminalamt

Diese Liste enthält auch schriftliche Kontrollen. Manche der aufgeführten Stellen wurden mehrfach kontrolliert.

Bei den in dieser Liste genannten Stellen wurde während des Berichtszeitraums ein Kontroll- oder Beratungsgespräch vor Ort, virtuell oder in schriftlicher Form begonnen. Dies bedeutet jedoch nicht, dass alle Gesamtverfahren ebenfalls im Berichtszeitraum abgeschlossen werden konnten. Insbesondere liegt noch nicht für sämtliche Verfahren ein Abschlussbericht vor. Diese veröffentlicht der BfDI im Rahmen der rechtlichen Möglichkeiten zeitnah nach der Fertigstellung auf seiner Website unter: www.bfdi.bund.de/kontrollberichte

Anlage 2

Erlassene Maßnahmen/Beanstandungen gegenüber öffentlichen Stellen

Stelle	Maßnahme/Beanstandung	Grund
Agentur für Arbeit Hanau	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Übermittlung Kontaktdaten an falschen Arbeitgeber
Agentur für Arbeit Kempten-Memmingen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Datenübermittlung ohne Rechtsgrundlage
Agentur für Arbeit München	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Datenübermittlung ohne Rechtsgrundlage
BARMER	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 5 Abs. 1 lit. a) DSGVO, Art. 9 Abs. 1 DSGVO i. V. m. § 35 Abs. 1 Erstes Buch Sozialgesetzbuch (SGB I)
BARMER	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 9 Abs. 1 DSGVO
BARMER	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 5 Abs. 1 lit. a), 6 Abs. 1 DSGVO
BARMER	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß, indem die zur Geltendmachung von Regressansprüchen verarbeiteten Daten nicht eher als im Nachgang an die datenschutzaufsichtsbehördliche Maßnahmenanhörung und somit entgegen der gebotenen Sorgfalt gelöscht worden sind, obgleich der erforderliche Verarbeitungszweck bereits seit dem 26. April 2022 entfallen ist.
BARMER	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 15 Abs. 1 DSGVO, Art. 12 Abs. 3 DSGVO i. V. m. Art. 15 Abs. 1 DSGVO
Berufsgenossenschaft Handel und Warenlogistik (BGHW)	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 5 Abs. 1 lit. a), 6 Abs. 1 lit. e) DSGVO i. V. m. § 76 Abs. 2 Nr. 1 Zehntes Buch Sozialgesetzbuch (SGB X)
BG BAU	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 5 Abs. 1 lit. a) i. V. m. Art. 6 Abs. 1 lit. e) DSGVO i. V. m. § 76 Abs. 2 Nr. 1 und § 67a Abs. 2 S. 2 Nr. 1 Zehntes Buch Sozialgesetzbuch (SGB X)
BIG direkt gesund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 6 Abs. 1 lit. e) DSGVO i. V. m. § 35 Abs. 1 Erstes Buch Sozialgesetzbuch (SGB I) und § 67b Abs. 1 Zehntes Buch Sozialgesetzbuch (SGB X)
BKK 24	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 5 Abs. 1 lit. a) bis c) DSGVO, Art. 44 ff. DSGVO, § 77 Abs. 3 Zehntes Buch Sozialgesetzbuch (SGB X), § 35 Erstes Buch Sozialgesetzbuch (SGB I), Art. 25 DSGVO, Art. 33 DSGVO
BKK Linde	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 6 Abs. 1 lit. e) DSGVO i. V. m. § 35 Abs. 1 Erstes Buch Sozialgesetzbuch (SGB I) und § 67a Abs. 1 Zehntes Buch Sozialgesetzbuch (SGB X), Art. 33 DSGVO
BKK ProVita	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 6 Abs. 1 DSGVO

Stelle	Maßnahme/Beanstandung	Grund
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Datenschutzpanne eServices, Jobbörse
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Datenschutzpanne eServices, Jobbörse
Bundesamt für den Militärischen Abschirmdienst	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 13 Nr. 2 MADG i. V. m. § 64 Abs. 1 Satz 1, Abs. 2 Satz 2 Nr. 1 BDSG wegen Nichtgewährleistung der Datenintegrität
Bundesamt für den Militärischen Abschirmdienst	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 6 Abs. 2 MADG i. V. m. § 12 Abs. 2 BVerfSchG wegen fehlender Verarbeitungssperre
Bundesamt für den Militärischen Abschirmdienst	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 73 Abs. 3 Satz 2 AufenthG wegen zu langer Speicherfristen
Bundesamt für Sicherheit in der Informationstechnik	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 Abs. 1 lit. b) DSGVO wegen fehlender technischer und organisatorischer Maßnahmen bei der Veröffentlichung von hausintern erstellen Dokumenten auf der Webseite
Bundesamt für Sicherheit in der Informationstechnik	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 DSGVO i. V. m. Art. 12 Abs. 1 Satz 1 DSGVO wegen Übermittlung eines Auskunftsersuchens nach Art. 15 DSGVO ohne Nachvollziehbarkeit
Bundesamt für Verfassungsschutz	Beanstandung gemäß § 16 Abs. 2 BDSG	Datensparsamkeit – Struktur einer Datei sorgt für eine Speicherung über das nach § 10 BVerfSchG zulässige Maß hinaus.
Bundesamt für Verfassungsschutz	Beanstandung gemäß § 16 Abs. 2 BDSG	Fehlende Dokumentation verhindert Datenschutzkontrolle
Bundesamt für Verfassungsschutz	Beanstandung gemäß § 16 Abs. 2 BDSG	Fehlende Löschfristen nach § 12 BVerfSchG
Bundesanstalt für Ernährung und Landwirtschaft	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 19 Abs. 2 Satz 1 SÜG und § 22 Abs. 2 Nr. 1 SÜG sowie § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 64 BDSG
Bundesanstalt für Materialforschung und -prüfung	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 30 Abs. 1 S. 1 DSGVO wegen fehlender Führung eines Verzeichnisses von Verarbeitungstätigkeiten und Verstoß gegen Art. 28 Abs. 1 i. V. m. Art. 5 Abs. 2 DSGVO wegen fehlender geeigneter Prozesse zur Auswahl, zum Einsatz (Management) und zur Überprüfung von Auftragsverarbeitern
Bundeskriminalamt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO u. Anweisung gemäß Art. 58 Abs. 2 lit. c) DSGVO	unvollständige Auskunft

Stelle	Maßnahme/Beanstandung	Grund
Bundeskriminalamt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO u. Anweisung gemäß Art. 58 Abs. 2 lit. c) DSGVO	unvollständige Auskunft
Bundeskriminalamt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verarbeitung nicht erforderlicher personenbezogener Daten in Auswahlvermerken zu Stellenbesetzungsverfahren
Bundesministerium der Verteidigung	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Beschwerde über die mit der Bezügeabrechnung übersandte Werbung für das Musikfest der Bundeswehr
Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)	Anordnung gemäß Art. 58 Abs. 2 lit. g) i. V. m. 18 DSGVO	Änderungsbescheid
Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 6 Abs. 1 DSGVO, Art. 12 Abs. 1, 13 und 14 DSGVO, Art. 12 Abs. 2, 15 Abs. 1 DSGVO
Bundesministerium für Gesundheit	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 §§ 19 Abs. 2 und 22 Abs. 2 SÜG
Bundesnachrichtendienst	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 36 Abs. 1 Nr. 2 i. V. m. § 64 Abs. 1 Satz 1 BDSG; Verstoß gegen § 20 Abs. 1 SÜG i. V. m. § 36 Abs. 1 Nr. 2 SÜG und § 64 Abs. 1 Satz 1 BDSG; Verstoß gegen §§ 19 Abs. 3 Satz 2, 22 Abs. 2 Nr. 2 lit. a) SÜG i. V. m. § 3 Abs. 3 SÜG
Bundespolizei	Beanstandung gemäß § 16 Abs. 2 BDSG	Keine Benennung aufgrund einer Einstufung

Stelle	Maßnahme/Beanstandung	Grund
Bundespolizei	Beanstandung gemäß § 16 Abs. 2 BDSG	1. Die Bundespolizei verstößt gegen § 27b Abs. 4 Bundespolizeigesetz (BPolG), indem sie seit dem 21. Juni 2022 ein System zur Kennzeichenerfassung für Zwecke der Gefahrenabwehr betreibt, welches im Falle eines Nichttreffers sämtliche Daten inklusive des Urbildes für 30 Minuten vorhält, um eine manuelle Nachkontrolle zu ermöglichen. 2. Die Bundespolizei verstößt gegen § 27b Abs. 5 BPolG, indem sie im Rahmen der automatisierten Kennzeichenerfassung eine weitere Sachaufklärung bei Fahndungstreffern durchführt, die nicht im Zusammenhang mit der Verfolgung der Zwecke des § 27b Abs. 1 Nr. 1 bis 3 BPolG stehen und auch nicht benötigt werden, um die Begehung einer Straftat von erheblicher Bedeutung zu verfolgen. 3. Die Bundespolizei hat gegen § 71 Abs. 1 BDSG verstoßen, indem Sie die Amazon Web Services (AWS) in ihre Systemarchitektur eingebunden hat. 4. Die Bundespolizei hat gegen § 62 Abs. 5 BDSG verstoßen, indem sie AWS mit der Verarbeitung personenbezogener Daten beauftragt hat, ohne einen Vertrag über die Auftragsverarbeitung abzuschließen. 5. Die Bundespolizei hat gegen § 62 Abs. 2 i. V. m. Abs. 1 BDSG verstoßen, indem sie unmittelbar AWS mit der Verarbeitung personenbezogener Daten beauftragt hat, ohne zu prüfen, dass mit geeigneten technischen und organisatorischen Maßnahmen sichergestellt ist, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird. 6. Die Bundespolizei verstößt gegen § 76 Abs. 1 Nr. 1 und 6 BDSG, indem sie „Kennzeichen Erfassung Anlassbezogen“ seit dem 21. Juni 2022 ohne die Protokollierung von Erhebungs- und korrespondierenden Löschvorgängen betreibt.
Bundespolizeiakademie	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen §§ 19 Abs. 2 Satz 1 und 2 sowie 22 Abs. 2 Nr. 1 lit. a) und b) SÜG und gegen § 20 Abs. 1 SÜG
Bundespolizeidirektion Pirna	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Offenbarung von Gesundheitsdaten
DAK-Gesundheit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 9 Abs. 1 DSGVO
DAK-Gesundheit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO, Art. 58 Abs. 2 lit. e) DSGVO	Art. 9 DSGVO

Stelle	Maßnahme/Beanstandung	Grund
Deutsche Rentenversicherung Knappschaft-Bahn-See	Anweisung gemäß Art. 58 Abs. 2 lit. c) DSGVO mit Verwarnung gemäß Art. 58 Abs. 2 lit. b), d) DSGVO	Art. 15 i. V. m. Art. 12 Abs. 3 S. 1 DSGVO
Deutscher Bundestag	Beanstandung gemäß § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 BDSG	Verstoß gegen § 18 Abs. 3 Satz 3 SÜG
DRV Knappschaft Bahn-See	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 5 Abs. 1 lit. a), 6 Abs. 1 DSGVO
energie BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 32 i. V. m. Art. 9 DSGVO
Financial Intelligence Unit	Beanstandung gemäß § 16 Abs. 2 BDSG	Keine Benennung aufgrund einer Einstufung
Financial Intelligence Unit	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen die Informationspflicht nach § 16 Abs. 4 Nr. 2 BDSG, indem der Abschlussbericht des Beratungsunternehmens PwC Strategy & (Deutschland) GmbH zur Untersuchung der Bearbeitungsrückstände bei der FIU nur in teilweiser geschwärzter Form übersandt wurde.
Finanzamt Hamburg-Oberalster	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 5 und 6 DSGVO
Generalzolldirektion	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Gutachten aus DU-Verfahren wurde für Disziplinarverfahren verwendet
Generalzolldirektion	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	möglicherweise Datenschutzverstoß im Rahmen eines disziplinarrechtlichen Ermittlungsverfahren
Generalzolldirektion	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
Handelskrankenkasse hkk	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 15 i. V. m. Art. 12 Abs. 3 S. 1 DSGVO
Hauptzollamt Osnabrück	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Beziehung eines ärztlichen Gutachtens zum Ermittlungsverfahren (Disziplinarverfahren) gegen den Beschäftigten
HZA Braunschweig	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	unverschlüsselte E-Mails, offene Briefumschläge u. a.
IKK – Die Innovationskrankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 5 Abs. 1 lit. a), 6 Abs. 1 DSGVO
IKK classic	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 5 Abs. 1 lit. f) DSGVO
Informationstechnik-zentrum Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verpflichtung des US-Anbieters Cloudflare als CDN-Dienstleister für die Zensus-Webseite

Stelle	Maßnahme/Beanstandung	Grund
Informationstechnikzentrum Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 Abs. 3 i. V. m. Art. 12 Abs. 5 DSGVO wegen Verlangen eines Entgelts für Datenkopie; Art. 12 Abs. 3 DSGVO wegen nicht fristgerechter Bearbeitung eines Auskunftsersuchens; Art. 15 Abs. 1 lit. d) DSGVO wegen Unterlassen der Mitteilung einer Speicherdauer an Auskunftsersuchenden
Informationstechnikzentrum Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 Abs. 1 lit. b) DSGVO wegen fehlender technischer und organisatorischer Maßnahmen beim Betreiben eines E-Mail-Verteilers
Informationstechnikzentrum Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO wegen Verarbeitung personenbezogener Daten von Beschäftigten ohne Rechtsgrundlage; Art. 44 DSGVO wegen Datenübermittlung in Drittländer ohne Rechtsgrundlage; Art. 33 Abs. 1 DSGVO wegen verspäteter Meldung an den BfDI
Informationstechnikzentrum Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO wegen Verarbeitung personenbezogener Daten zweier externer Beschäftigter ohne Rechtsgrundlage; Art. 9 Abs. 1 DSGVO wegen Verarbeitung von Gesundheitsdaten ohne Rechtsgrundlage; Art. 34 Abs. 1 DSGVO wegen Nichtbenachrichtigung der Betroffenen
Jobcenter Berlin Charlottenburg-Wilmersdorf	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Anforderung von ungeschwärztem Mietvertrag nach Wohnungsbrand (Antrag auf Gewährung einer Erstausstattung als unabweisbarem Bedarf), Art. 15-Antrag
Jobcenter Dahme-Spreewald	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Kein Hinweis auf Schwärzung des Arbeitsvertrages
Jobcenter Nürnberg, Stadt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Anforderung von Daten Dritter bei Antrag auf Arbeitslosengeld II; Antrag nach Art. 15 DSGVO
Jobcenter Tirschenreuth	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Anforderung Arbeitsvertrag
Presse- und Informationsamt der Bundesregierung	Untersagung gemäß Art. 58 Abs. 2 lit. f) und Verwarnung nach Art. 58 Abs. 2 lit. b)	Verstoß gegen Art. 5 Abs. 2 DSGVO wegen Betrieb einer Facebook-Fanpage; Verstoß gegen § 25 Abs. 1 Satz 1 TTDSG wg. Speicherung von Informationen ohne Erfüllung der Rechtsgrundlage; Verstoß gegen Art. 5 Abs. 1 lit. a) i. V. m. Art. 6 Abs. 1 DSGVO wg. Übermittlung von personenbezogenen Daten an Meta
SBK Siemens-Betriebskrankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 6 Abs. 1 lit. e) DSGVO i. V. m. § 35 Abs. 1 SGB I und § 67a Abs. 1 SGB X, Art. 33 DSGVO
Techniker Krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 6 Abs. 1 DSGVO
Techniker Krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 15 Abs. 3 S. 1 DSGVO
Techniker Krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Art. 6 Abs. 1 lit. e) DSGVO i. V. m. § 67a Abs. 1 Zehntes Buch Sozialgesetzbuch (SGB X)

Stelle	Maßnahme/Beanstandung	Grund
Technisches Hilfswerk	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Offenlegung von Daten aller ehrenamtlicher Helfer
Universität der Bundeswehr München	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Offenlegung von personenbezogenen Daten (einschließlich eines Fotos) im Rahmen einer Veranstaltung
Zollkriminalamt	Beanstandung gemäß § 16 Abs. 2 BDSG	Keine Benennung aufgrund einer Einstufung
Bundesbehörden des Gemeinsamen Terrorismusabwehr-zentrum	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen die Übermittlungsvorschriften
Bundesnachrichtendienst	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen die Mitwirkungspflichten
Bundesnachrichtendienst	Beanstandung gemäß § 16 Abs. 2 BDSG	Verarbeitung personenbezogener Daten ohne Rechtsgrundlage, Verstoß gegen das Prinzip der Erforderlichkeit

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 gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 17 Abs. 1 lit. d) DSGVO wegen unterbliebener Löschung
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO wegen rechtswidriger Verknüpfung von Empfängeradresse mit GPS Ortungsdaten von Zustellfahrrädern zur Zustellbestätigung
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 Abs. 1 lit. b) DSGVO wegen unzureichender technisch-organisatorischer Maßnahmen, die zu unberechtigten Offengelegungen personenbezogener Daten gegenüber Dritten führten
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 DSGVO wegen unzureichender technisch-organisatorischer Maßnahmen, die zur unberechtigten Offenlegungen personenbezogener Daten gegenüber Dritten führten und Postsendungen nicht ausreichend vor unberechtigter Einsichtnahme Dritter schützten
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Verstoß gegen Art. 27 DSGVO weil kein Vertreter in der EU benannt ist; Verstoß gegen Art. 37 Abs. 1 und Abs. 1 Satz 1 i. V. m. § 38 Abs. 1 BDSG wegen Nicht-Ernennung eines Datenschutzbeauftragten; Verstoß gegen Art. 13 wegen Nichtzurverfügungstellung der in Art. 13 DSGVO genannten Informationen in deutscher Sprache
Ein Telekommunikations-dienstleistungs-unternehmen	Festsetzung Zwangsgeld nach Nichterfüllung einer Anweisung nach Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen §38 Abs. 1 Satz 1 BDSG und Art. 37 Abs. 1 lit. b) DSGVO, Unternehmen benennt keinen Datenschutzbeauftragten
Ein Telekommunikations-dienstleistungs-unternehmen	Mehrere Anweisungen nach Art. 58 Abs. 2 lit. c) DSGVO	Verstöße gegen Art. 15 DSGVO, Unternehmen erteilt keine Auskunft, gegen Art. 21 DSGVO, Unternehmen führt Werbewidersprüche nicht durch und gegen Art. 17 DSGVO Unternehmen führt keine Löschung durch
Ein Telekommunikations-dienstleistungs-unternehmen	Festzsetzung Zwangsgeld nach Nichterfüllung mehrerer Anweisungen nach Art. 58 Abs. 1 lit. a) DSGVO	Keine Vorlage einer Datenschutzerklärung gemäß Art. 13 DSGVO, keine Mitteilung über den Versand der Datenschutzerklärung an Personen und über Speicherung von personenbezogenden Daten im Rahmen der Verfügbarkeitsprüfung, keine Mitteilung über Versand der Datenschutzerklärung im Rahmen von Vertragsabschlüssen
Ein Telekommunikations-dienstleistungs-unternehmen	Festsetzung Zwangsgeld nach Nichterfüllung einer Anweisung gemäß Art. 58 Abs. 2 lit. c) DSGVO	Verstoß gegen Art. 15 DSGVO, Unternehmen erteilt keine Auskunft

Stelle	Maßnahme/Beanstandung	Grund
Ein Telekommunikations-dienstleistungs-unternehmen	Anweisung nach Art. 58 Abs. 1 lit. a) DSGVO	Vorlage mehrerer Informationen bzw. Beantwortung von Fragen im Rahmen einer Sicherheitsverletzung nach § 169 TKG (große Anzahl an Rechnungen von Kunden waren z. T. mit Einzelverbindungsnachweis über das Internet ohne Passwort zugänglich)

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)
- Task Force Facebook Fanpages (Vorsitz Hamburg)
- 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 (Düsseldorfer Kreis) (Vorsitz Nordrhein-Westfalen)
- AK Wissenschaft und Forschung (Vorsitz Hessen)
- AK Zertifizierung (Vorsitz Schleswig-Holstein)

Unterarbeitskreise (UAK) der DSK

- UAK BCR-Neuverteilung
- UAK Regeln für die Kommunikation von und nach Europa (DSK Auftrag)
- UAK Internationaler Datenverkehr (ad hoc)

Konferenz der Informationsfreiheitsbeauftragten in Deutschland (Vorsitz 2023: BfDI)

AK Informationsfreiheit der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

Gremien der Europäischen Union:

Europäischer Datenschutzausschuss (EDSA)

Unterarbeitsgruppen (Expert Subgroups) des EDSA:

- Borders, Travel and Law Enforcement Expert Subgroup (Koordination BfDI)
- Compliance, e-Government and Health Expert Subgroup
- Cooperation Expert Subgroup
- Coordinators Expert Subgroup
- Enforcement Expert Subgroup
- Financial Matters Expert Subgroup
- International Transfer Expert Subgroup
- IT Users Expert Subgroup
- Key Provisions Expert Subgroup
- Social Media Expert Subgroup
- Strategic Advisory Expert Subgroup
- Technology Expert Subgroup

Task Forces des EDSA:

- Taskforce 101 Complaints
- Taskforce Chat GPT
- Taskforce Competition and Consumer Law

- Taskforce Cookie Banner
- Taskforce Fining (Ko-Koordination BfDI)
- Taskforce International Engagement (Ko-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, 2023: Japan)

Arbeitsgruppen des G7 DPA Roundtable:

- Emerging Technologies Working Group (Koordinatoren Vereinigtes Königreich und Frankreich; BfDI ist Mitglied)
- Enforcement Cooperation Working Group (Koordinator Kanada; BfDI ist Mitglied)
- Data Free Flow with Trust Working Group (Koordinatoren U.S. FTC und Japan; BfDI ist Mitglied)

International Working Group on Data Protection in Technology (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)
- Digital Citizen and Consumer Working Group (Koordinatoren Kanada und Australien, BfDI ist Mitglied)
- Ethics and Data Protection in Artificial Intelligence Working Group (Koordinatoren Frankreich und EDPS; BfDI ist Mitglied)
- Data Protection and other Rights and Freedoms Working Group (Koordinator Kanada; BfDI ist Mitglied)
- Digital Economy Working Group (Koordinator: Marokko; BfDI ist Mitglied)
- Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management Working Group (Koordinator Schweiz; BfDI ist Mitglied)

Europarat
Beratender Datenschutz-Ausschuss (T-PD; Vorsitz Deutschland, vertreten durch BMI; BfDI ist beratendes Mitglieder der deutschen Delegation)

Working Party Data Governance and Privacy der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) (Vorsitz Kanada; BfDI ist beratendes Mitglied der deutschen Delegation)

Global Privacy Enforcement Network (Komitee mit den USA, dem Vereinigten Königreich, Kanada, Israel und Hongkong; BfDI ist Mitglied)

Europäische Datenschutzkonferenz (Spring Conference) (Vorsitz beim jeweiligen Gastgeber, 2023 Ungarn; BfDI ist Mitglied)

European Case Handling Workshop (Vorsitz beim jeweiligen Gastgeber, 2023 Schweiz; BfDI ist Mitglied)

International Conference of Information Commissioners (BfDI ist Mitglied des Executive Committee)

Leitungsstab Presse/Öffentlichkeitsarbeit
MR Hensel
R 5010

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Prof. Ulrich Kelber
R 5000

Gleichstellungs-beauftragte
RD'n Dr. Branskat
R 1900

Behördlicher Datenschutzbeauftragter
ORR Kapsa
R 1950

Interessensvertretungen

Personalrat
Vorsitzende
OAR'n Lübke
R 1910

Vertrauensperson der schwerbehinderten Menschen
OAR'n Thelen
R 1920

Zentrale Anlaufstelle
MR Meister
R 7100

Leitender Beamter
MinDir Müller, J. H
R 6000

Referat Informationsfreiheit
MR'n Dr. Schlögel
R 6100

Geheim- und Sabotageschutzbeauftragter
OAR Finzelberg
R 1940

IT-Sicherheitsbeauftragter
OAR Höllen
R 1930

Ansprechperson für Korruptionsprävention, Sponsoringbeauftragter
RD Roski
R 1960

Abteilung Z
Zentrale Aufgaben
MinDirig'n Dr. Grundmann
R 9000

Referat Z 1
Personal
MR'n Dr. Kreiling
R 9100

Referat Z 2
Organisation/Haushalt
MR'n Bönner
R 9200

Referat Z 3
Innerer Dienst/Beschaffung
MR'n Westkamp
R 9300

Referat IKT
Informations- und Kommunikationstechnik
MR Dr. Garbotz
R 9400

Justitiariat
MR Peschel
R 9600

Abteilung 1
Grundsatz, Verwaltung des Bundes, Internationales
MinDirig Heyn
R 1000

Referat 11
Grundsatz, nichtöffentlicher Bereich
MR Hermerschmidt
R 1100

Referat 12
Finanz-/Steuerverwaltung, Rechtswesen, Parlamentarischer Bereich
MR Lenzen
R 1200

Referat 13
Kranken- und Pflegeversicherung, Grundsatzfragen SGB
MR Müller, T R 1300

Referat 14
Europäische und Internationale Angelegenheiten
MR Dr. Haupt
R 1400

Referat 15
Arbeitsverwaltung
MR Dr. Kisker
R 1500

Referat 16
Innere Verwaltung, Auswärtiger Dienst
MR Faßbender
R 1600

Referat 17
Gesundheit und Soziales
RD'n Dr. Schräder R 1700/-01
RD'n Virks R 1700/-02

Referat 18
Beschäftigtendatenschutz, BMVg
RD Deitermann
R 1800

Abteilung 2
Technologischer Datenschutz, Telekommunikation und Telemedien
MinDirig'n Jost
R 2000

Referat 21
Projekte der angewandten Informatik, Telematik
TB Leopold
R 2100

Referat 22
Postdienste, Wirtschaftsverwaltung
MR'n Schäfer
R 2200

Referat 23
Telemedien und Messenger Dienste
MR'n Hartmann
R 2300

Referat 24
Telekommunikation
MR Dr. Stadler
R 2400

Referat 25
Technologischer Datenschutz, Datensicherheit
MR Dr. Bender
R 2500

Referat 26
Technikentwicklung, Labor
TRD'n Voigtländer
R 2600

Referat 27
IT-Sicherheitsbehörden
N.N.
R 2700

Abteilung 3
Polizei und Nachrichtendienste
MinDirig'n Polfers
R 3000

Referat 31
Grundsatz, Internationales im Bereich Polizei und Justiz
MR Behn
R 3100

Referat 32
Bundeskriminalamt, Generalbundesanwalt
MR Bergemann
R 3200

Referat 33
Bundesamt für Verfassungsschutz, Bundesamt für den Militärischen Abschirmdienst, Zentrale Stelle für Informationstechnik im Sicherheitsbereich
MR'n Dr. Sosna R 3300

Referat 34
Bundesnachrichtendienst, Militärisches Nachrichtenwesen, Unabhängiger Kontrollrat
MR'n Mittnacht R 3400

Referat 35
Bundespolizei, Zollkriminalamt, Financial Intelligence Unit
MR'n Löwnau R 3500

Referat 36
Sicherheitsüberprüfungsgesetz
MR'n Dr. Gnedler
R 3600

Anschrift:
Dienstsitz Bonn: Graurheindorfer Str. 153, 53117 Bonn
Postfach 14 68, 53004 Bonn

Verbindungsbüro
Berlin: Friedrichstr. 50, 10117 Berlin

Erreichbarkeit:
Telefon: 0228/997799-0
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Stand: 12. Januar 2024

Abkürzungsverzeichnis

1. BDSG ÄndG	Erstes Bundesdatenschutzänderungsgesetz
a. F.	alte Fassung
AA	Auswärtiges Amt
Abs.	Absatz
AI LLM	Artificial Intelligence – Large Language Models
AK	Arbeitskreis
AKIF	Arbeitskreis Informationsfreiheit
AO	Abgabenordnung
APD	Autorité de protection des données, belgische Datenschutzaufsichtsbehörde
APEC	Asia Pacific Expert Subgroup
AufenthG	Aufenthaltsgesetz
AWS	Amazon Web Services
AZR	Ausländerzentralregister
BA	Bundesagentur für Arbeit
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BAMF	Bundesamt für Migration und Flüchtlinge
BBF	Bundesamt zur Bekämpfung von Finanzkriminalität
BCR	Binding Corporate Rules
BCR-P	Binding Corporate Rules for Processors
BDA	Bundesvereinigung der Deutschen Arbeitgeberverbände
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BKM	Bundesbeauftragte für Kultur und Medien
BMAS	Bundesministerium für Arbeit uns Soziales
BMDV	Bundesministerium für Digitales und Verkehr
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern und für Heimat
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BND	Bundesnachrichtendienst
BNDG	BND-Gesetz
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BPA	Bundespresseamt
BPolG	Bundespolizeigesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestag-Drucksache
BTLE ESG	Borders, Travel & Law Enforcement Expert Subgroup
BTMK	Betäubungsmittelkonsument
BT-Polizei	Polizei des deutschen Bundestages
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfSchG	Bundesverfassungsschutzgesetz
BZR	Bundeszentralregister
BZSt	Bundeszentralamt für Steuern
bzw.	beziehungsweise

CEA	Coordinated Enforcement Action
CEF	Coordinated Enforcement Framework
CNIL	Commission Nationale de l'Informatique et des Libertés (französische Datenschutzbehörde)
CSAM	Child sexual abuse material
CSAM-VO	Verordnung zum Auffinden von Material des sexuellen Online-Kindesmissbrauchs
CSC	Coordinated Supervision Committee
CWA	Corona Warn App
DA	Data Act
DAkkS	Deutsche Akkreditierungsstelle
DEMIS	Deutsches elektronisches Melde- und Informationssystem für Infektionskrankheiten
DFFT	Data Free Flow with Trust
DFS	Deutschen Flugsicherung GmbH
DGA	Data Governance Act
DGUV	Spitzenverband der gewerblichen Berufsgenossenschaften und der Unfallkassen
DigiG	Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens
DPC	Data Protection Commission (irische Datenschutzbehörde)
DPO	Data Protection Officer
Dr.	Doktor
DRV	Deutsche Rentenversicherung
DSC	Datenschutzcockpit
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DSRV	Datenstelle der Rentenversicherung
ECRIS-TCN	Europäische Strafregisterinformationssystem für Drittstaatsangehörige und Staatenlose
EDHS	European Health Data Space
EDIB	European Data Innovation Board
EDSA	Europäischer Datenschutzausschuss
EES	Einreise-/Ausreisesystem
eFBS	einheitliches Fallbearbeitungssystem
EG	Europäische Gemeinschaft
eGK	elektronische Gesundheitskarte
EGovG	E-Government-Gesetz
EHDS	Europäischer Raum für Gesundheitsdaten
EHW	ermittlungsunterstützenden Hinweisen
eID	electronic Identification
eIDAS	Electronic Identification, Authentication and Trust Services
EinwVO	Einwilligungsverwaltungsverordnung
ELStAM	elektronischen Lohnsteuerabzugsmerkmale
ENF ESG	Enforcement Expert Subgroup
ENISA	Agentur der Europäischen Union für Cybersicherheit
ePA	elektronische Patientenakte
EPRIS	European Police Record Index System
ETIAS	Europäische Reiseinformations- und -genehmigungssystem
EU	Europäische Union
EUDI-Wallet	European Digital Identity Wallet
EuGH	Europäischer Gerichtshof
Eurodac	European Dactyloscopy
EU-U.S. DPF	EU-U.S. Data Privacy Framework
EWR	Europäischer Wirtschaftsraum
ExCo	Executive Commitee
EZG	Ermittlungszentrum Geldwäsche

FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FKBG	Finanzkriminalitätsbekämpfungsgesetz
FlugDaG	Fluggastdatengesetz
G7 DPA Roundtable	G7 Data Protection and Privacy Authorities Roundtable
GDNG	Gesundheitsdatennutzungsgesetz
GG	Grundgesetz
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GKV	Gesetzliche Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GOBT	Geschäftsordnung des Deutschen Bundestages
GPA	Global Privacy Assembly
GPDP	Garante per la protezione dei Dati Personali (italienische Aufsichtsbehörde)
GS RegMo	Gesamtsteuerung Registermodernisierung
GTAZ	Gemeinsame Terrorismusabwehrzentrum
HinSchG	Hinweisgeberschutzgesetz
HLG	High Level Group on access to data for effective law enforcement
HSOG	Gesetz über die öffentliche Sicherheit und Ordnung (Hessen)
i. d. R.	in der Regel
i. S. d.	im Sinne des/der
i. V. m.	in Verbindung mit
ICIC	Internationalen Konferenz der Informationsfreiheitsbeauftragten
ICO	Informations Commissioner‘s Office (britische Datenschutzbehörde)
IDNr	Identifikationsnummer
IDNrG	Identifikationsnummerngesetz
IFG	Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten aus Bund und Ländern
IMI	EU Binnenmarktinformationssystem
INPOL	Fahndungssystem des bundesweiten zentralen polizeilichen Informationssystems
IoT	Internet of Things
IP	Intermediäre Plattform
IRD	Implantateregister
IRegBV	Implantateregister-Betriebsverordnung
IRegG	Implantateregistergesetz
ITS ESG	International Transfer Expert Subgroup
IT-PLR	IT-Planungsrat
IWGDPT	International Working Group on Data Protection and Technology
JI-Richtlinie	Richtlinie zum Datenschutz bei Polizei und Justiz
KBS	Knappschaft Bahn See
KEYP ESG	Key Provisions Expert Subgroup
KI	Künstliche Intelligenz
MADG	Gesetze über den Militärischen Abschirmdienst
Meta Irland	Meta Platforms Ireland Limited
Mio.	Million
N.SIS II	nationales System des Schengener Informationssystems der zweiten Generation
NADIS	Nachrichtendienstliche Informationssystem
NAT-Verfahren	Netzwerkadressübersetzung
NfL	Nachrichten für Luftfahrer
NIS2-Richtlinie	Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union

NIS2UmsuCG	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
NOOTS	Nationale Once-Only-Technical-System
Nr.	Nummer
NWR	Nationale Waffenregister
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OPC Canada	Office of the Privacy Commissioner of Canada (kanadische Datenschutzbehörde)
OVG	Oberverwaltungsgericht
OZG	Onlinezugangsgesetz
OZG 2.0	Onlinezugangsgesetz-Änderungsgesetz
PETs	Privacy Enhancing Technologies
PHW	personengebundenen Hinweisen
PIAV	Polizeilicher Informations- und Analyseverbund
PIAV-S	strategische Komponente des Polizeilichen Informations- und Analyseverbunds
PIAV-S-PMK	Polizeilicher Informations- und Analyseverbund Politisch motivierte Kriminalität
PKGr	Parlamentarisches Kontrollgermium
PNR	Passenger Name Record
PNR-RL	Passenger Name Record Richtlinie
PoC	Proof of Concept Datenkonsolidierung
PolDVG	Gesetz über die Datenverarbeitung der Polizei (Hamburg)
Prof.	Professor
PSYV	Psychische- und Verhaltensstörung
PUEG	Pflegeunterstützungs- und -entlastungsgesetz
RegMoG	Registermodernisierungsgesetz
RKI	Robert Koch-Institut
S.	Seite
s.	siehe
SDG-VO	Single-Digital-Gateway-Verordnung
SGB	Sozialgesetzbuch
SIGINT	Signal Intelligence
SIS	Schengener Informationssystem
SIS III	Schengener Informationssystem der dritten Generation
StBA	Statistisches Bundesamt
Steuer-ID	Steuerliche Identifikationsnummer
StIdV	Verordnung zur Vergabe steuerlicher Identifikationsnummern
SÜG	Sicherheitsüberprüfungsgesetz
TB	Tätigkeitsbericht
TB-IFG	Tätigkeitsbericht zur Informationsfreiheit
TF C&C	Taskforce zum Zusammenspiel zwischen Datenschutz, Wettbewerb und Verbraucherschutz
TF INT	Taskforce „International Engagement“
TI	Telematikinfrastruktur
TIA	Transfer Impact Assessments
TKG	Telekommunikationsgesetz
T-PD	Datenschutz Ausschuss des Europarats
TTDSG	Telekommunikations-Telemedien-Datenschutz-Gesetz
UAK	Unterarbeitskreis
UIG	Umweltinformationsgesetz
UK-Rat	Unabhängige Kontrollrat
USA	Vereinigte Staaten von Amerika
V	römisch Fünf
VBS	Vorgangsbearbeitungssystem

VdA	Verband der Automobilindustrie
VDuG	Verbraucherrechtedurchsetzungsgesetz
Verbund DMS	Dokumentenmanagementsystem im Verfassungsschutzverbund
vgl.	vergleiche
VII	römisch Sieben
ViKon	Visa-Konsultationsverfahren
VIS	Visa-Informationssystem
VKR	Verbandsklagenrichtlinie
VM	virtuelle Maschine
VPN	virtuelles privates Netzwerk
VRUG	Verbandsklagenrichtlinienumsetzungsgesetz
VS-nfD	Verschlussache – Nur für den Dienstgebrauch
VS-Verbund	Verbundes aus Bundesamt für Verfassungsschutz und Landesbehörden für Verfassungsschutz
VVO	Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO
VwVfG	Verwaltungsverfahrensgesetz
WBRL	Whistleblowing-Richtlinie
WP	Working Paper
X	römisch Zehn
z. B.	zum Beispiel
ZASt	Zentrale Anlaufstelle
ZfA	Zentrale Zulagenstelle für Altersvermögen
ZFdG	Zollfahndungsdienstgesetz
ZfS	Zentralstelle für Sanktionsdurchsetzung
ZIS	Zentrale Informationsstelle für Sporteinsätze
ZKA	Zollkriminalamt

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Graurheindorfer Straße 153
53117 Bonn

Tel. +49 (0) 228 997799-0
E-Mail: poststelle@bfdi.bund.de
Web: www.bfdi.bund.de

Bonn 2024
Dieser Bericht ist als Bundestagsdrucksache erschienen.

Bildnachweis: BfDI, PPC Japan, Ralph Ruthe, Mark Parisi, Chris Slane, Alamy – Man with a camera

Realisation
Appel & Klinger Druck und Medien GmbH

www.bfdi.bund.de