Tätigkeitsbericht 2021

30. Tätigkeitsbericht
für den Datenschutz und
die Informationsfreiheit

BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

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

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Tätigkeitsbericht für das Jahr 2021
– 30. Tätigkeitsbericht –

Inhaltsverzeichnis

1 Einleitung

2021 – ein weiteres Jahr, das immer wieder und umfassend durch die Corona-Pandemie und deren Bekämpfung geprägt war. Wie schon 2020 legte die Bundesregierung dabei Gesetzentwürfe und Verordnungen zur Pandemie-Bekämpfung im Akkord vor, und wie im Vorjahr gab es selten Zeit, diese Entwürfe sachgerecht zu prüfen und die Bundesregierung zu beraten. Bei allem Verständnis für die zum Teil gebotene Eile hätten ein wenig mehr Sorgfalt und eine Einbindung von Beginn an – wie eigentlich vorgeschrieben – der Sache sicher gut getan.

Denn nicht alle zu ergreifenden Maßnahmen kamen überraschend: Beispielsweise habe ich die Bundesregierung bereits im Sommer darauf hingewiesen, dass eine gesetzliche Grundlage zur Regelung der Überwachung von 3G oder 2G am Arbeitsplatz erforderlich sein wird. Ein entsprechendes Gesetzgebungsverfahren wurde dann aber erst Ende November und auch hier wieder mit einer extrem kurzen Prüf- und Stellungnahmefrist auf den Weg gebracht.

Meine stetigen Hinweise, dass es für solche Maßnahmen gesetzliche Grundlagen braucht, würde ich mir gerne ersparen, wenn denn entsprechend gehandelt würde. Stattdessen werden Lösungsvorschläge – auch solche, die bei richtiger Ausgestaltung datenschutzrechtlich möglich wären – oft gar nicht erst vorgelegt oder besprochen. Vielmehr wird öffentlich lamentiert, „der Datenschutz“ würde im Weg stehen. Entgegen dieser immer wieder vorgebrachten Kritik hat der Datenschutz und damit auch meine Behörde aber keine einzige geeignete Pandemiebekämpfungsmaßnahme der Bundesregierung beschränkt oder gar gestoppt. So müßig es mittlerweile geworden ist, werde ich auch in Zukunft nicht müde werden, dies richtigzustellen und mich Schwarzer-Peter-Spielen entgegenstellen, die nur den Blick auf die notwendigen Maßnahmen behindern.

Die Diskussion um die Kontrolle zur Einhaltung der 3G- oder gar 2G-Regelungen am Arbeitsplatz haben darüber hinaus exemplarisch aufgezeigt, wie notwendig, sinnvoll und überfällig Regelungen zum Beschäftigtendatenschutz sind. Der vom Bundesarbeitsministerium eingesetzte Beirat, dem auch ich angehört habe, hat dazu Vorschläge erarbeitet.

Die Digitalisierung unserer Lebens- und Arbeitswelt wird pandemiebedingt schneller vorangetrieben. Der Einsatz von Künstlicher Intelligenz (KI) und maschinellem Lernen nimmt deutlich zu, aber nicht immer ist klar, ob Programmierung, Auftrag, Training und Ergebnis wirklich den gesteckten Zielen entsprechen. Die Ergebnisse sind bei komplexen Aufgaben kaum zu kontrollieren. Nachdem die Datenethikkommission in ihrem Bericht aus dem Jahr 2020 weitreichende Vorschläge zum Umgang mit „algorithmischen Systemen“ gemacht hat, liegt jetzt ein Regulierungsentwurf der EU-Kommission vor, den es zu konkretisieren gilt.

Für den Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr habe ich ein umfangreiches Konsultationsverfahren gestartet, mit dem eine öffentliche Debatte in Gang gesetzt werden soll.

Über zehn Jahre mussten wir auf die Umsetzung der Privacy-Richtlinie durch den Gesetzgeber warten, ehe im Jahr 2021 das Telekommunikationsgesetz durch das Telekommunikationsmodernisierungsgesetz überarbeitet wurde. Zeitgleich wurde das Telekommunikation-Telemedien-Datenschutz-Gesetz geschaffen, mit dem unter anderem die, für viele so lästigen, Cookie-Banner reguliert oder gar ganz vermieden werden sollen.

Zunehmend wichtiger wird die Arbeit in den EU- und internationalen Gremien. Der Europäische Datenschutz-Ausschuss (EDSA) trifft nach langen Vorarbeiten durch die jeweils zuständigen Datenschutzaufsichtbehörden der EU-Länder und seine Arbeitsgruppen Beschlüsse und Leitlinien, die für alle EU-Staaten verbindlich sind. Es fehlen zwar immer noch wichtige Entscheidungen über bestimmte Datenerhebungen und -verarbeitungen gerade der großen Internetkonzerne, es gibt aber erste Anzeichen für ein härteres Vorgehen ge

gen offensichtliche Datenschutzverstöße. Erstmalig hat der EDSA dabei auch Entscheidungen federführender nationaler Aufsichtsbehörden deutlich nachgeschärft und z. B. Bußgelder empfindlich erhöht.

So wie die DSGVO inzwischen weltweit die Standards für den Datenschutz legt, hat die internationale Zusammenarbeit immer größere Bedeutung. Ich arbeite im Exekutiv-Komitee der Global Privacy Assembly (weltweiter Zusammenschluss der nationalen Datenschutzbehörden) mit und habe am G7-Treffen der Datenschutzbehörden teilgenommen. Parallel zur G7-Präsidentschaft der Bundesrepublik Deutschland habe ich im Jahr 2022 den Vorsitz dieses neuen Zusammenschlusses.

Coronabedingt konnten auch in diesem Jahr nicht so viele Vor-Ort-Kontrollen stattfinden wie gewünscht und geplant. Stattdessen werden Möglichkeiten für ergänzende schriftliche Kontrollen gesucht und diese – wo immer sie möglich sind – umfangreich genutzt.

Neben der Kontrolle der von mir beaufsichtigten Behörden und Unternehmen ist die Beratung und Information von Bundesregierung und Bundestag, aber auch der Bürgerinnen und Bürger, meine wichtigste Aufgabe. Dem komme ich gerne nach und gehe dabei auch neue Wege. So wurden im letzten Jahr in Zusammenarbeit mit dem Carlsen-Verlag zwei Pixi-Bücher für Kinder zum Thema Datenschutz herausgebracht. Bei der Vorstellung der Bücher in Schulen war ich selbst überrascht, wie interessiert selbst Grundschulkinder schon an diesem Thema sind. Unser Dienstleister kommt kaum mit dem Ausliefern der bestellten Pixi-Bücher an die interessierten Bürgerinnen und Bürger nach. Das stärkt mich in meiner Überzeugung, dass man mit Datenschutz gar nicht früh genug anfangen kann.

All diese Themen und Aufgaben kann ich natürlich nicht alleine bewältigen, dabei unterstützen mich ca. 275 hochmotivierte und fachlich exzellente Mitarbeiterinnen und Mitarbeiter, bei denen ich mich an dieser Stelle ausdrücklich für ihre tägliche Unterstützung bedanken möchte.

Mein weiterer Dank gilt „Erzaehlmirnix“, die ich – als Alternative zu den Karikaturen unterschiedlicher Zeichnerinnen und Zeichner in den vorherigen Tätigkeitsberichten – gebeten haben, diesmal exklusiv meinen Bericht mit ihrer erfrischenden Sicht auf verschiedene Datenschutzthemen zu bereichern.

Prof. Ulrich Kelber

2 Empfehlungen

2.1 Zusammenfassung der Empfehlungen des 30. Tätigkeitsberichts

Ich empfehle der Bundesregierung, die im Koalitionsvertrag angekündigte Institutionalisierung der DSK und die verbesserte verbindliche Kooperation der deutschen Datenschutzaufsichtsbehörden durch die entsprechenden gesetzgeberischen Maßnahmen alsbald in Angriff zu nehmen. (Nr. 3.1.1; 5.7)

Ich empfehle, die Wege und den Datenkranz bei der Meldung von Impfungen – Impfquotenmonitoring – zu überprüfen. (Nr. 4.1.9)

Ich empfehle dem BMG für den Betrieb des Implantateregisters eine geeignete Behörde vorzusehen – und gegebenenfalls zu schaffen –, die den Registerbetrieb dauerhaft rechtssicher und datenschutzkonform ohne Interessenkonflikte übernehmen kann. (Nr. 5.10)

Ich empfehle, beim Modellvorhaben Genomsequenzierung den Aufbau der „gemeinsamen Dateninfrastruktur“ dezentral zu strukturieren und statt einer doppelten Datenhaltung jeweils anlassbezogene Datenzugänge vorzusehen. (Nr. 6.6)

Ich empfehle, das Einsichtsrecht der betrieblichen Datenschutzbeauftragten in die im Unternehmen geführten Sicherheitsakten, den Adressaten einer Beanstandung im nichtöffentlichen Bereich, den Umfang der Maßnahmen bei Sicherheitsüberprüfungen gem. § 33 SÜG sowie die Datenübermittlung im sogenannten Besuchskontrollverfahren im SÜG zu regeln. (Nr. 6.20)

Ich empfehle dem Gesetzgeber weiterhin angesichts des festgestellten geringen Nutzwerts von Antiterrordatei und Rechtsextremismusdatei, diese abzuschaffen. (Nr. 8.1.1)

2.2 Empfehlungen des 29. Tätigkeitsberichts

	Empfehlungen des 29. Tätigkeitsberichts	Stand der Umsetzung
🟡	Ich empfehle den meiner Aufsicht unterliegenden Stellen, mich auch bei zeitkritischen Projekten frühzeitig einzubinden. Dadurch kann dem Datenschutz und damit auch dem Schutz der Betroffenenrechte von Anfang an ausreichend Rechnung getragen werden. (vgl. 29. TB Nr. 4.1.4, 4.1.8, 4.1.9)	Nach Besprechungen bei einzelnen Projekten hat sich eine gewisse Besserung bei der frühzeitigten Bereitstellung von Dokumenten eingestellt. Leider gilt diese Feststellung nicht für aller Projekte.
🟢	Ich empfehle dem Bundesrat, eine Stellvertreterin bzw. einen Stellvertreter des gemeinsamen Vertreters nach § 17 Abs. 1 BDSG zu wählen. (vgl. 29. TB Nr. 10.1)	Die Wahl erfolgte am 25. Juni 2021.
🔴	Ich empfehle, bei der Registermodernisierung statt auf eine einheitliche Personenkennziffer auf mehrere bereichsspezifische Identifikatoren zurückzugreifen. Zumindest sollte das 4-Corner-Modell für jede Datenübermittlung eingesetzt und eine strenge Zweckbindung für die Verwendung der ID-Nr. festgelegt werden. Das Datencockpit sollte zeitnah zu einer echten Bestandsdatenauskunft weiterentwickelt werden. (vgl. 29. TB Nr. 5.1)	Bis auf die Weiterentwicklung des Datencockpits wurde keiner meiner Empfehlungen gefolgt.
🟡	Ich empfehle, dass die meiner Aufsicht unterliegenden Stellen ihre Datenübermittlungen an Drittländer im Hinblick auf die Anforderungen des Schrems II-Urteils des EuGH sorgfältig überprüfen und erforderliche Anpassungen vornehmen. (vgl. 29. TB Nr. 4.3)	Auch wenn überwiegend ein Bewusstsein für die Anforderungen der Schrems II-Entscheidung des EuGH bei den von mir beaufsichtigten Stellen attestiert werden kann, sind Anpassungen oft mit komplexen Fragestellungen behaftet. Bei meinen Kontrollen werde ich die bereits erkennbaren Anpassungsbemühungen begleiten und weiter überwachen.
🔴	Ich empfehle, die Gesetze, Projekte und Maßnahmen, die im Rahmen der Corona-Pandemie unter hohem Druck und innerhalb kürzester Fristen entwickelt und umgesetzt wurden, nach Ende der Pandemielage bewusst und sorgfältig zu evaluieren. (vgl. 29. TB Nr. 4.1.3, 4.1.4)	Eine Evaluierung ist bislang nicht erfolgt. Dies sollte unverzüglich nachgeholt werden, sobald eine endemische Lage erreicht wird.
🔴	Ich empfehle, „digitale Gesundheitsanwendungen“ in der sicheren Telematikinfrastruktur oder auf maschinell lesbaren Datenträgern an die Nutzer zu übermitteln. Zudem sollte für die Bereitstellung der „digitalen Gesundheitsanwendungen“ in der Telematikinfrastruktur ein App-Store neu geschaffen und von schweigepflichtigen Akteuren des Gesundheitssystems betrieben werden. (vgl. 29. TB Nr. 5.6)	„Digitale Gesundheitsanwendungen“ werden (noch) nicht in der sicheren Telematikinfrastruktur oder auf maschinell lesbaren Datenträgern an die Nutzer übermittelt. Ebenso wenig wurde bislang für die Bereitstellung der „digitalen Gesundheitsanwendungen“ ein von schweigepflichtigen Akteuren des Gesundheitssystems betriebener App-Store geschaffen.
🔴	Ich empfehle klarzustellen, dass die Ausübung von Datenschutzrechten nicht zu Strafschärfungen in Disziplinarverfahren führen darf. (vgl. 29. TB Nr. 6.10)	Eine Klarstellung in diese Richtung ist bislang nicht erfolgt.

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

3 Gremien

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

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

Der Vorsitz der DSK wechselt jährlich. 2021 nahm die Saarländische Landesbeauftragte Monika Grethel diese Aufgabe wahr. Pandemiebedingt fanden alle Konferenzen im Videoformat statt. Es wurden zwei Entschließungen zum Themenbereich Corona-Pandemie und vier Beschlüsse zu verschiedenen Einzelfragen der Verarbeitung von Positivdaten durch Auskunfteien, zur Verarbeitung des Datums „Impfstatus“ sowie zur Nichtanwendung technischer und organisatorischer Maßnahmen auf Wunsch der betroffenen Person verabschiedet.

Darüber hinaus erarbeitete die DSK Orientierungshilfen zum Schutz von personenbezogenen Daten bei Übermittlung per E-Mail und für Anbieterinnen und Anbieter von Telemedien ab dem 1. Dezember 2021 sowie Anwendungshinweise für Anforderungen an datenschutzrechtliche Zertifizierungen.

3.1.1 Arbeitskreis DSK 2.0

Die Zusammenarbeit der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder sollte weiter verbessert werden. Dazu hat der Arbeitskreis DSK 2.0 in einem Zwischenbericht erste Ergebnisse vorgestellt und Vorschläge unterbreitet, wie dieses Ziel erreicht werden kann.

Innerhalb der DSK besteht Einvernehmen, dass sie sich weiterentwickeln, schneller und flexibler werden sowie sich kurzfristig in aktuelle datenschutzpolitische öffentliche Diskussionen einbringen muss. Deshalb hatte sie im Juni 2020 einen Arbeitskreis DSK 2.0 auf Leitungsebene eingerichtet, der die Zusammenarbeit einschließlich der Arbeitsweise der DSK evaluieren und Vorschläge für eine Neugestaltung erarbeiten sollte (vgl. 29. TB Nr. 3.1.6).

Im Jahr 2021 hat der Arbeitskreis erste Ergebnisse in einem Zwischenbericht zusammengefasst und der DSK vorgelegt. Der Zwischenbericht enthält neben einer Bestandsaufnahme auch konkrete Vorschläge zu den drei Themenfeldern „DSK als europäischer Player“, „Mutigere/schnellere Positionierung“ sowie „verbindliche Mehrheitsentscheidungen“. Konkret wird u. a. vorgeschlagen,

- ein Präsidium der DSK zu bilden
- spezifische Sprecherfunktionen zu etablieren und
- eine gemeinsame Geschäftsstelle einzurichten.

Auf dieser Grundlage wird der AK DSK 2.0 seine Arbeit fortsetzen und dabei insbesondere die rechtlichen Rahmenbedingungen für eine engere Kooperation unter Wahrung der Unabhängigkeit der Aufsichtsbehörden prüfen.

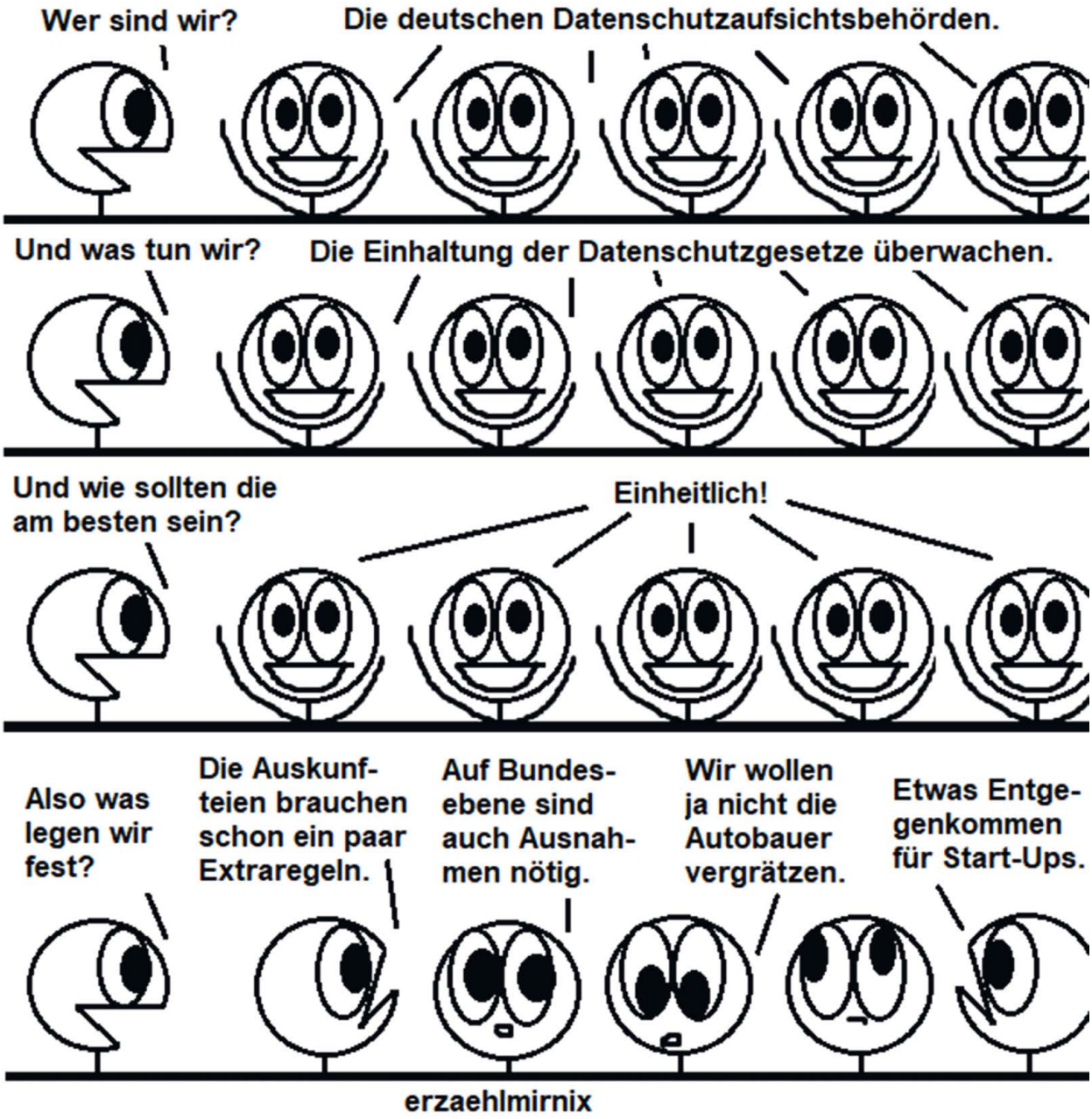
Ich werde mich weiter dafür einsetzen, die DSK fortzuentwickeln und die Aufsichtspraxis innerhalb der deutschen Datenschutzaufsichtsbehörden noch stärker zu harmonisieren.

Ich empfehle der Bundesregierung, die im Koalitionsvertrag angekündigte Institutionalisierung der DSK und die verbesserte verbindliche Kooperation der deutschen Datenschutzaufsichtsbehörden durch die entsprechenden gesetzgeberischen Maßnahmen alsbald in Angriff zu nehmen.

3.1.2 Positivdaten Auskunfteien

Eine Verarbeitung von sogenannten Positivdaten aus Verträgen über Mobilfunkdienste und Dauerhandelskonten ist nur aufgrund wirksamer Einwilligung möglich. Auch ein so genannter „Engergieversorgerpool“ darf nicht zu gläsernen Verbrauchern führen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte bereits im Jahr 2018 festgestellt, dass Auskunfteien Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage der Interessenabwägung des Art. 6 Abs. 1 Abs. 1 lit. f DSGVO erheben dürfen.



In der öffentlichen Wahrnehmung wird die Tätigkeit von Auskunfteien überwiegend mit der Speicherung und Weitergabe von so genannten Negativdaten in Verbindung gebracht. Dabei geht es um Informationen über negative Zahlungserfahrungen oder Zinsen und Tilgung von Krediten, Zahlungsausfälle bei einer Ratenzahlung oder eine Privatinsolvenz. Die Meldung solcher Daten an die Auskunfteien, die Speicherung und die Beauskunftung dieser Daten werden in der Regel auf die Interessenabwägung gemäß Art. 6 Abs. 1 Satz 1 lit. f) DSGVO gestützt. Diese Datenverarbeitungen sind demnach dann erlaubt, wenn es ein berechtigtes Interesse entweder der Auskunftei oder ihrer Vertragspartner gibt und schutzwürdige Interessen der betroffenen Verbraucherinnen und Verbraucher nicht überwiegen.

Weniger bekannt ist, dass es auf Seiten der Auskunfteien und ihrer Vertragspartner auch ein Interesse gibt, so genannte Positivdaten zu verarbeiten. Positivdaten sind Informationen über bestehende Verträge, die von den Verbraucherinnen und Verbrauchern vertragsgemäß bedient werden. Auch diese Positivdaten gehen unter Umständen in die Berechnung der Wahrscheinlichkeit eines Zahlungsausfalls (Score) ein. Diese Informationen können nach Ansicht der Datenschutzaufsichtsbehörden – abgesehen von bestimmten Ausnahmen im Bankenbereich – nur auf der Basis einer wirksamen Einwilligung der betroffenen Person verarbeitet werden. Es überwiegt bei solchen Positivdaten regelmäßig das schutzwürdige Interesse der betroffenen Person, selbst über die Verwendung ihrer Daten zu bestimmen. Bereits die

Übermittlung solcher Daten durch deren Vertragspartner an eine Auskunftei kann nicht auf Art. 6 Abs. 1 Abs. 1 lit. f DSGVO gestützt werden: Solange eine Person ihre vertraglichen Verpflichtungen einhält, gibt es keinen Grund, ohne ihre Zustimmung Daten über ihre Verträge oder ihr Zahlungsverhalten vorzuhalten.

Die DSK hatte bereits bei ihrem Beschluss im Jahr 2018 angedacht, sich mit der Verarbeitung von Positivdaten bei Dauerschuldverhältnissen zu einem späteren Zeitpunkt zu befassen, was im Berichtszeitraum nun der Fall war. Besonders ging es um die Frage, ob für die verbreitete Praxis der Übermittlung und Verarbeitung von Positivdaten zu Verträgen über Mobilfunkdienste und Dauerhandelskonten von Privatpersonen eine andere Bewertung erforderlich ist. Dies betrifft beispielsweise die verbreitete Praxis, Mobiltelefone über die Laufzeit eines Mobilfunkvertrages in monatlichen Raten abzuzahlen. Mit Dauerhandelskonten sind wiederum Verträge gemeint, bei denen die betroffene Person Waren auf Kredit erhält, indem sie beispielsweise eine von einem Händler bereitgestellte Kundenkarte nutzt und die gekauften Waren durch monatliche Abbuchungen oder auf andere Weise nachträglich bezahlt.

Die DSK kam zu dem Ergebnis, dass für die Übermittlung der Positivdaten durch die Mobilfunkdiensteanbieter und die Handelsunternehmen zwar berechtigte Interessen bestehen, die Qualität der Bonitätsbewertungen zu verbessern und die beteiligten Wirtschaftsakteure vor kreditorischen Risiken zu schützen. Allerdings ist die DSK auch der Auffassung, dass die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen regelmäßig dieses berechtigte Interesse der Verantwortlichen oder Dritter an der Verarbeitung der Positivdaten überwiegen. Besondere Umstände, die in diesen Fällen eine Verarbeitung von Positivdaten auf der Basis der Interessenabwägung rechtfertigen, konnte die DSK nicht feststellen. Die Auskunfteien haben damit argumentiert, die Verarbeitung von Positivdaten sei besonders dann von Vorteil für die Verbraucherinnen und Verbraucher, wenn sonst wenige Informationen zu einer Person vorlägen. Dieses Argument überzeugt aber nicht. Zum einen lässt sich auch damit nicht begründen, warum eine Verarbeitung gegen den Willen der Person zulässig sein soll. Zum anderen ist dieses Argument überhaupt nur aus der Logik heraus verständlich, dass aus dem fehlenden Vorhandensein von Daten zu einer Person häufig eine negative Bewertung folgt, obwohl aus dem Nichtvorhandensein von Daten keine Schlüsse gezogen werden können.

Eine Übermittlung und Verarbeitung von Positivdaten über Mobilfunkdienstverträge und Dauerhandelskonten durch Vertragspartner und Auskunfteien sind nur auf der Grundlage einer Einwilligung der betroffenen Person zulässig. Dafür müssen die allgemeinen Anforderungen gewahrt werden. Insbesondere darf die Erteilung der Einwilligung nicht zur Bedingung des Vertragsabschlusses gemacht werden.

Zeitgleich mit den Erörterungen zur Verarbeitung von Positivdaten gab es bei Auskunfteien und Energieversorgern im Berichtszeitraum Überlegungen, einen sogenannten Energieversorgerpool zu schaffen. In diesem zentralen Datenpool sollten auch Positivdaten der Vertragspartner gespeichert und an andere Energieversorger übermittelt werden. Informationen über die Anzahl abgeschlossener Verträge und die jeweilige Vertragsdauer können Hinweise darauf geben, ob eine längere Vertragsbeziehung zu einem Stromversorger beabsichtigt oder regelmäßig Angebote für Neukunden genutzt werden. Verbraucher, die regelmäßig das kostengünstigste Angebot am Markt wählen und dazu den Anbieter wechseln möchten, könnten dann von Versorgungsunternehmen bei preislich attraktiven Angeboten ausgeschlossen werden, obwohl sie ausschließlich von ihren Rechten als Kunden Gebrauch gemacht haben.

Ich begrüße es, dass die DSK auch zum sogenannten Energieversorgerpool klar Stellung bezogen hat. Der Wunsch, „Schnäppchenjäger“ in einem Datenpool zu erfassen, um sie bei Vertragsanbahnung als solche identifizieren und von Angeboten ausschließen zu können, stellt kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 Abs. 1 lit. f DSGVO dar. Zudem überwiegen insoweit auch die schutzwürdigen Interessen und Grundrechte der Kundinnen und Kunden. Die DSK hat es nicht akzeptiert, dass ein ausdrücklich erwünschtes Verhalten – hier die Suche nach dem preisgünstigsten Energieanbieter – zu negativen Konsequenzen für die Verbraucherinnen und Verbraucher führt.

3.1.3 Arbeitskreis Microsoft

Für Verantwortliche ist es eine Bredouille: Da gibt es eine Software wie Microsoft 365, die vielerorten eingesetzt wird, sich gleichzeitig aber einer gewichtigen Datenschutzkritik ausgesetzt sieht. Wie lässt sich so ein Konflikt mit dem Datenschutz vermeiden? Die DSK hat einen intensiven Dialog mit Microsoft begonnen, um für mehr Klarheit zu sorgen und Verantwortlichen eine Empfehlung an die Hand zu geben.

Bereits Ende 2020 wurde von der DSK eine Dialogrunde mit Microsoft initiiert, um gemeinsam datenschutzrechtliche Nachbesserungen der vertraglichen Grundlagen für die Online-Dienste des Unternehmens zu erreichen. Unter der Leitung der Aufsichtsbehörden aus Brandenburg und Bayern (LDA) engagieren sich aktuell auch die Aufsichtsbehörden aus Berlin, Schleswig-Holstein, Sachsen, Mecklenburg-Vorpommern, Baden-Württemberg,

Hessen und mein Haus in diesem Arbeitskreis. Im Fokus stehen Fragen zur Auftragsverarbeitung gem. Art. 28 DSGVO und die praktischen Auswirkungen der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems II“).

Die DSK hatte bereits im Vorfeld einige Kritikpunkte geäußert, z. B. wenn Microsoft bei der Diensteerbringung personenbezogene Daten auch für eigene Zwecke nutzt. Dies erfordert eine tragfähige Rechtsgrundlage für die Bereitstellung dieser Daten aus dem Auftragsverhältnis der Verantwortlichen/Kunden an Microsoft. Die Prüfung einer tragfähigen Rechtsgrundlage setzt wiederum die Kenntnis der konkreten Zwecke und genutzten personenbezogenen Daten voraus.

In der Dialogrunde geht es u. a. darum, diese Transparenz herzustellen, um auf dieser Grundlage eine rechtliche Bewertung abzuleiten. Aus meiner Sicht sollte sich diese Transparenz selbstverständlich in den vertraglichen Grundlagen wiederfinden. Nur so können Verantwortliche/Kunden ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO gerecht werden. Generell diskutiert die DSK aber auch andere vertragliche Verbesserungsvorschläge, so auch beim Einsatz von Unterauftragnehmern.

Ich möchte diesen Dialogprozess mit Blick auf die Fragen zur Auftragsverarbeitung gem. Art. 28 DSGVO möglichst zeitnah abschließen und als DSK-Handlungsempfehlungen für Verantwortliche/Kunden veröffentlichen, die einschlägige Microsoft-Produkte einsetzen wollen.

In einem weiteren Schritt wird sich die Dialogrunde mit den konkreten Auswirkungen des Schrems-II-Urteils befassen. Hier ebnen die neuen rechtlichen Anforderungen, aber auch veränderte Kundenwünsche, den Weg für eine verstärkt europazentrierte Datenverarbeitung. Mit der Initiative des sog. „EU Data Boundary“ kündigt auch Microsoft die Möglichkeit einer EU-Datengrenze an und bietet perspektivisch europäischen Kunden so die Möglichkeit, ihre Daten ausschließlich innerhalb der Europäischen Union zu verarbeiten und zu speichern. Ich werde diese Entwicklungen weiter intensiv begleiten.

3.1.4 Wichtige Beschlüsse und Entschließungen

3.1.4.1 Coronavirus: Es ist notwendig, Nachweise über Impfungen, Testergebnisse und Genesungen gesetzlich zu regeln

Eine Verarbeitung von Gesundheitsdaten wie Impfnachweis oder Körpertemperaturmessung gehören gesetzlich geregelt. Hierbei müssen zwingend die strengen Vorgaben des Art. 9 Abs. 2 DSGVO eingehalten werden.

Die DSK hat in ihrer Entschließung den Gesetzgeber aufgefordert, entsprechende Gesetzgebungsverfahren in die Wege zu leiten. Die Verarbeitung von Gesundheitsdaten zu privatwirtschaftlichen Zwecken muss den Anforderungen der europäischen Datenschutz-Grundverordnung genügen. Unter den Begriff der Gesundheitsdaten fallen auch Informationen zum Impfstatus oder das Ergebnis eines Coronatests. Der besonders strenge Schutz der Datenschutz-Grundverordnung lässt eine Verarbeitung nur unter Ausnahmen zu. Ohne eine gesetzliche Grundlage wäre eine Verarbeitung lediglich mit Einwilligung möglich. Dies ist insbesondere problematisch, was die Freiwilligkeit einer solchen Einwilligung im Beschäftigungsbereich angeht. Um Rechtsklarheit, Rechtssicherheit und einheitliche Lösungen zu erreichen, bedarf es gesetzlicher Regelungen.

Um die von der DSK geforderte Rechtsklarheit zu schaffen, habe und werde ich die beteiligten Bundesministerien weiterhin intensiv beraten und auf eine gesetzliche Regelung drängen.

3.1.4.2 Verarbeitung des Datums „Impfstatus“ von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber

Die Verarbeitung des Datums „Impfstatus“ von Beschäftigten darf nur mit einer ausdrücklichen gesetzlichen Ermächtigung erfolgen. Auch in Zeiten der COVID-19-Pandemie.

Arbeitgeberinnen und Arbeitgeber dürfen das Datum „Impfstatus“ grundsätzlich nur mit einer ausdrücklichen gesetzlichen Ermächtigung verarbeiten. In dem Beschluss der DSK wird auch klargestellt, dass § 26 Abs. 3 Satz 1 BDSG nicht als eine solche in Betracht kommt. Die Verarbeitung von Gesundheitsdaten, wie z. B. der Impfstatus, ist nur ausnahmsweise erlaubt (vgl. Art. 9 Abs. 1 DSGVO).

Auf die Einwilligung Beschäftigter kann die Verarbeitung solcher Daten nur dann gestützt werden, wenn sie freiwillig und damit rechtswirksam erteilt wurde, vgl. Art. 26 Abs. 3 S 2 und Abs. 2 BDSG. In einem Über- und Unterordnungsverhältnis, wie es im Regelfall im Beschäftigungsverhältnis gegeben ist, bestehen Zweifel an der Freiwilligkeit und somit auch an der Rechtswirksamkeit der Einwilligung.

Auf diesen Missstand habe ich den Gesetzgeber lange hinweisen müssen, bis es eine gesetzliche Regelung gab.

3.1.4.3 Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail

Bei der Übermittlung von E-Mails bestehen Risiken, die mit einer Verletzung von Vertraulichkeit und Integrität

personenbezogener Daten verbunden sind. Verantwortliche und Auftragsverarbeitende müssen einschätzen können, welche Schäden ein Bruch von Vertraulichkeit und Integrität anrichten können. Können Anforderungen an eine sichere Übermittlung nicht erfüllt werden, muss ein anderer – sicherer – Kommunikationskanal gewählt werden.

Die DSK hat in ihrer Orientierungshilfe zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail Überlegungen zu Anforderungen an die Verfahren zum E-Mail-Versand und -Empfang angestellt. Sie behandelt die Risiken, die mit einer Verletzung der Vertraulichkeit und Integrität personenbezogener Daten verbunden sind. Sie geht dabei von typischen Verarbeitungssituationen aus, um praxisrelevante Anwendungsfälle aufzuzeigen. Insbesondere wird auf die Ende-zu-Ende-Verschlüsselung als auch die Transportverschlüsselung als geeignete Verfahren für eine Risikominimierung abgestellt. Die DSK stellt durch den risikobasierten Ansatz der Orientierungshilfe den Verantwortlichen und Auftragsverarbeitenden ein geeignetes Hilfsmittel im Umgang mit der Übermittlung von E-Mails zur Verfügung.

Die Orientierungshilfe finden Sie unter folgendem Link: www.bfdi.bund.de/orientierungshilfen

3.2 Europäischer Datenschutzausschuss

3.2.1 Allgemeiner Bericht

Der Europäische Datenschutzausschuss (EDSA) hat im Berichtszeitraum seine Arbeit an einer europaweit einheitlichen Anwendung der Datenschutz-Grundverordnung weiter intensiviert. Hierzu wurden weitere Leitlinien angenommen, Empfehlungen ausgesprochen und Stellungnahmen abgegeben. Auch die grenzüberschreitende Zusammenarbeit wurde weiter verstärkt. Erste Verfahren der Streitbeilegung, darunter ein Verfahren der Dringlichkeit, wurden verhandelt.

Der Europäische Datenschutzausschuss (EDSA) ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beiträgt und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördert. Diese Aufgaben habe ich bereits in meinen vorangegangenen Tätigkeitsberichten näher erläutert. Als gemeinsamer Vertreter aller deutschen Aufsichtsbehörden ist der BfDI ein Mitglied des Ausschusses. Nähere Ausführungen können über meinen Internetauftritt abgerufen werden.[1]

Die Arbeitsweise des EDSA wurde auch im Jahr 2021 durch die Auswirkungen der COVID-19-Pandemie bestimmt. Mit einer Ausnahme fanden alle Plenarsitzungen in Form von Videokonferenzen statt. Dabei hat der EDSA die hohe Dichte an Plenarsitzungen verfestigt und insgesamt 15 Mal konferiert. Hinzu kommen zahlreiche Sitzungen der Arbeitsgruppen (expert subgroups) des EDSA.

Ein Schwerpunkt der Arbeiten lag auch in diesem Berichtszeitraum auf der Erarbeitung von Leitlinien nach Art. 70 DSGVO zur einheitlichen Umsetzung der DSGVO in Europa. Daneben hat der Ausschuss auch Stellungnahmen im Kohärenzverfahren nach Art. 64 DSGVO angenommen. In meinem letzten Tätigkeitsbericht habe ich auf erste Entscheidungen gegenüber weltweit führende Tech-Unternehmen hingewiesen. Hier hat es weitere Entwicklungen gegeben, darunter eine erste Entscheidung im sog. Dringlichkeitsverfahren.

Der EDSA hat zudem begonnen, seine Strategie für die Jahre 2021 bis 2023 umzusetzen.

Leitlinien, Empfehlungen und Orientierungshilfen

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

- Die **Leitlinien 01/2021 zu Beispielen zu Benachrichtigungen über Datenschutzverletzungen** (Guidelines 01/2021 on Examples regarding Data Breach Notification) betrachten Beispiele aus der Aufsichtspraxis der beteiligten Aufsichtsbehörden. Diese beinhalten die Aspekte der Risikobewertung bei Datenpannen, die Rolle der technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO sowie Vorschläge für Maßnahmen, die Verantwortliche nach Datenpannen ergreifen sollten.
- Die **Empfehlungen 01/2021 zu der Referenzgrundlage für den Begriff „Angemessenheit" in der Richtlinie zum Datenschutz bei der Strafverfolgung (JI-Richtlinie)** setzen den Rahmen und die Mindestanforderungen für die Annahme eines Angemessenheitsbeschlusses auf der Basis des EU-Rechts.
- Die **Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen** erläutern das Verhältnis zur geplanten E-Privacy-Verordnung und Fragen der Verarbeitung von personenbezogenen Daten zu neuen Zwecken.

1 www.bfdi.bund.de/edsa

- Die **Leitlinien 02/2021 zu Sprachassistenten** (Guidelines 02/2021 on Virtual Voice Assistants) zeigen die wichtigsten Bezüge zur Rechtskonformität („Compliance"). Darüber hinaus geben sie den Beteiligten praktische Empfehlungen, wie sie diese einhalten können.
- Die **Leitlinien 9/2020 zu maßgeblichen und begründeten Einwänden gemäß Verordnung 2016/679** geben eine Anleitung, was unter einem „maßgeblichen und begründeten Einspruch" betroffener Aufsichtsbehörden gegen Entscheidungsvorschläge der federführenden Aufsichtsbehörden in grenzüberschreitenden Aufsichtsfällen zu verstehen ist. Erläutert werden die Verfahren und die Kriterien, die bei der Beurteilung eines Einspruchs zu berücksichtigen sind.
- Die **Orientierungshilfe zur Bewertung von Zertifizierungskriterien** (Guidance on certification criteria assessment [Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation]) verfolgt das Ziel, Elemente aus den EDSA-Leitlinien 1/2018 zu verfeinern. Ziel ist eine einheitliche Bewertungen im Zusammenhang mit der Genehmigung von Zertifizierungskriterien zu etablieren.
- Die **Leitlinien 03/2021 zur Anwendung von Art. 65 (1)(a) DSGVO** (Guidelines 03/2021 on the application of Article 65(1)(a) GDPR) beschreiben den Ablauf einer Streitbeilegung durch den EDSA. Sie beziehen sich ausschließlich auf Fälle eines gescheiterten Kooperationsverfahrens nach Art. 60 Abs. 4 DSGVO und sollen diese Verfahren einer Entscheidung zuführen.
- Die **Leitlinien 8/2020 bezüglich der Zielgruppenansprache von Social-Media-Nutzern** sollen – vor dem Hintergrund mehrerer EuGH-Urteile – die Verteilung der Rollen und Verantwortlichkeiten zwischen Social-Media-Plattformen und Unternehmen oder anderen Nutzern der Targeting-Funktionen dieser Social-Media-Plattformen, klarstellen. Außerdem sollen sie die Wirkung der Datenverarbeitungsvorgänge auf (Grund-)Rechte und Freiheiten betroffener Personen mit praktischen Beispielen verdeutlichen.
- Die **Empfehlungen 02/2021 zur Rechtsgrundlage für die Speicherung von Kreditkartendaten ausschließlich zum Zweck der Erleichterung weiterer Online-Transaktionen** zielen auf europaweit einheitliche Anforderungen an die Rechtmäßigkeit einer Datenspeicherung von Kreditkartendaten im Onlinehandel ab. Sie sorgen für ein klare Rechtslage und verhindern Wettbewerbsnachteile.
- Die **Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten** (Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data) zielen darauf ab, Datenexporteure beim Ermitteln und durchführen geeigneter zusätzlicher Maßnahmen zu unterstützen. Dies um ein gleichwertiges Schutzniveau zu erreichen. Sie enthalten mehrere Änderungen aus der öffentlichen Konsultation. Außerdem legen sie einen besonderen Schwerpunkt auf die Gepflogenheiten der Behörden eines Drittlandes.
- Die **Leitlinien 04/2021 über Verhaltensregeln als Instrument für Übermittlungen** (Guidelines 04/2021 on codes of conduct as tools for transfers) haben den Zweck, die Voraussetzungen der Genehmigung von Verhaltensregeln durch eine zuständige Aufsichtsbehörde und Erklärung ihrer allgemeinen Gültigkeit innerhalb des EWR durch die Kommission als Übermittlungsinstrument zu präzisieren.
- Die **Leitlinien 7/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO** haben das Hauptziel, die Bedeutung der Begriffe zu klären. Darüber hinaus werden die verschiedenen Rollen und die Verteilung der (rechtlichen) Verantwortlichkeiten zwischen diesen Akteuren verdeutlicht.
- Die **Leitlinien 10/2020 zu Beschränkungen gemäß Art. 23 der DSGVO** (Guidelines 10/2020 on restrictions under Article 23 GDPR) zielen darauf ab, die Bedingungen für die Anwendung solcher Einschränkungen durch die Mitgliedstaaten oder den EU-Gesetzgeber im Lichte der Charta der Grundrechte und der Datenschutz-Grundverordnung zu betonen. Sie analysieren die Kriterien wie Beschränkungen angewendet werden, der zu beachtenden Bewertungen, die Art und Weise, wie betroffene Personen ihre Rechte nach Aufhebung der Beschränkungen ausüben können und die Folgen von Verstößen gegen Art. 23 DSGVO.
- Die **Leitlinien 05/2021 zum Zusammenspiel zwischen der Anwendung von Art. 3 und den Bestimmungen über internationale Übermittlungen** (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) erläutern drei grundlegende Kriterien. Sie geben Beispiele zur Klärung, ob eine Verarbeitung eine Übermittlung in ein Drittland oder an eine internationale Orga

nisation ist und ob folglich die Bestimmungen von Kapitel V der DSGVO eingehalten werden müssen.

Stellungnahmen zu Angemessenheitsentscheidungen

Der EDSA gibt in Verfahren eine Stellungnahme über die Entscheidung ab, ob ein Drittland oder eine internationale Organisation über ein angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten verfügen. Bei seiner Beurteilung verwendet der EDSA

- die **DSGVO-Referenzgrundlage für Angemessenheit**,
- die **Empfehlungen des EDSA 2/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen** sowie
- die Entscheidungen des EuGH und des EGMR zum Zugriff durch Behörden.

Im Jahr 2021 hat der EDSA sich zur Angemessenheit in zwei Drittstaaten geäußert (s.a. 3.2.2.):

- In der **Stellungnahmen zur Angemessenheit im Vereinigten Königreich**
  (Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom und Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom) stellt der EDSA fest, dass sich die datenschutzrechtlichen Rahmen der EU und des Vereinigten Königreichs in Kernbereichen stark ähneln. Das gilt z. B.:
  - für Grundlagen rechtmäßiger und fairer Verarbeitung für legitime Zwecke
  - die Zweckbindung, Datenqualität und Verhältnismäßigkeit
  - Datenspeicherung, Sicherheit und Vertraulichkeit,
  - Transparenz
  - besondere Datenkategorien sowie
  - automatisierte Entscheidungen und Profiling.

Dennoch empfiehlt der EDSA, einzelne Punkte genau zu untersuchen bzw. zu überwachen, z. B. bei der Ausnahmeregelung für den Einwanderungsbereich und ihre Wirkungen auf die Rechte der betroffenen Personen geltenden Beschränkungen.

- In der **Stellungnahme zum Entwurf eines Angemessenheitsbeschlusses der Europäischen Kommission für die Republik Korea**
  (Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea) konzentriert sich der EDSA auf allgemeine Aspekte der DSGVO. Außerdem hat der EDSA den Fokus auf den Zugang von Behörden zu personenbezogenen Daten, die aus dem Europäischen Wirtschaftsraum (EWR) in die Republik Korea für Zwecke der Strafverfolgung und der nationalen Sicherheit übermittelt werden. Dieses beinhaltet auch die Rechtsbehelfe, die Personen im EWR zur Verfügung stehen. Der EDSA prüft, ob die im koreanischen Rechtsrahmen vorgesehenen Garantien wirksam sind.

Stellungnahmen im Kohärenzverfahren / Entscheidungen im Kooperationsverfahren

Im Kohärenzverfahren hat der EDSA fast 40 Stellungnahmen verfasst.

Diese betreffen zum großen Teil:

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

Auf Antrag der Hamburger Aufsichtsbehörde hat der EDSA einen ersten verbindlichen Beschluss im Dringlichkeitsverfahren gemäß Art. 66 Abs. 2 DSGVO erlassen, nachdem diese einstweilige Maßnahmen gegen Facebook Ireland Ltd verfügt hatte.

Die Hamburger Aufsichtsbehörde hatte ein Verbot der Verarbeitung von WhatsApp-Nutzerdaten durch Facebook Ireland Ltd für eigene Zwecke angeordnet. Dies geschah nachdem eine Änderung der Nutzungsbedingungen und Datenschutzbestimmungen für europäische Nutzer von WhatsApp Ireland Ltd durchgeführt worden war. Der EDSA entschied mehrheitlich, dass die Voraussetzungen für den Nachweis eines Verstoßes und einer Dringlichkeit nicht erfüllt seien. Daher erfolgte keine endgültige Maßnahme.

In einem zweiten Verfahren erließ der EDSA einen Streitbeilegungsbeschluss auf der Grundlage von Art. 65 DSGVO. Hierdurch sollte der mangelnde Konsens über bestimmte Aspekte eines Beschlussentwurfs der irischen Aufsichtsbehörde als federführender Aufsichtsbehörde in Bezug auf WhatsApp Ireland Ltd und den anschließenden Einsprüchen einiger betroffener Aufsichtsbehörden ausgeräumt werden. Der EDSA kam zu dem Schluss, die irische Aufsichtsbehörde solle ihren

Beschlussentwurf zu Verstößen gegen die Transparenz, zur Berechnung der Geldbuße und zur Frist für die Umsetzung der Anweisung ändern.

Umsetzung der EDSA-Strategie 2021-2023

Die **EDSA-Strategie 2021-2023** habe ich bereits in meinem letzten Tätigkeitsbericht erläutert. Mit der Umsetzung wurde – beispielhaft – bereits begonnen:

- Um die Harmonisierung zu fördern und die Rechtskonformität (Compliance) zu erleichtern, werden die Leitlinien, Empfehlungen und Orientierungshilfen umgesetzt.
- Der EDSA richtet einen **Expertenpool** (Support Pool of Experts) ein, um eine effektive Durchsetzung und die effiziente Zusammenarbeit zwischen nationalen Aufsichtsbehörden zu unterstützen. Dieser wird auf Ebene des EDSA eingesetzt, um Untersuchungen und Durchsetzungsmaßnahmen zu fördern, die für die Mitglieder des EDSA von gemeinsamem Interesse sind. Zudem hat der EDSA beschlossen, seine erste koordinierte Maßnahme **(Coordinated Enforcement Framework)** zur Nutzung von Cloud-basierten Diensten durch den öffentlichen Sektor zu starten. Die Ergebnisse dieser nationalen Maßnahmen werden dann gebündelt und analysiert.
- Den grundrechtlichen Ansatz für neue Technologien stützt der EDSA mit seinem **Statement on Digital and Data Strategy**. Dabei äußert er im Kern übergreifend alle Bedenken, die die Rechtsakte (Data Governance Act, Digital Services Act, Digital Markets Act und Artificial Intelligence Act) betreffen. Neben einem mangelnden Schutz der Grundrechte und Grundfreiheiten des Einzelnen besteht eine nur fragmentierte Aufsicht (s.a. 4.2 und 5.9).

Querverweise:

3.2.2 Schwerpunkt Drittlandübermittlung, 3.2.4 Leitlinien Verantwortlichkeit, 3.2.6 Leitlinien Streitbeilegungsverfahren, 4.2 Künstliche Intelligenz, 5.9 EU Digitalisierungsgesetzgebung

3.2.2 Drittlandübermittlungen / Schrems II-Entscheidung

3.2.2.1 Taskforce Supplementary Measures / Umsetzung Schrems II

Auch im Jahr 2021 hat das „Schrems II"-Urteil des EuGH (Rechtssache C-311/18) die Aufsichtsbehörden in der EU und auf nationaler Ebene weiter beschäftigt. Ein wichtiger Schritt im Hinblick auf die Umsetzung der Ergebnisse des Schrems II-Urteils war die Arbeit der vom EDSA eingesetzten Taskforce Supplementary Measures. Daneben wurden die Aufsichtsbehörden im Rahmen ihrer Beratungs- und Kontrolltätigkeit mit Fragen zur Umsetzung der Schrems II-Entscheidung konfrontiert, die es zu lösen gilt.

I. Das Schrems II-Urteil

In meinen letzten beiden Tätigkeitsberichten hatte ich bereits über das Schrems II-Verfahren berichtet. Der EuGH hatte am 16. Juli 2020 mit seinem Schrems II-Urteil verkündet, dass die Regelungen des EU-US „Privacy Shield" unwirksam sind. Auf Basis der Regelungen des Privacy Shields dürfen keine Datenübermittlungen mehr in den Gültigkeitsbereich US-amerikanischen Rechts vorgenommen werden. Die Nichtigkeitserklärung des EuGH betraf hingegen nicht das Übermittlungsinstrument der Standardvertragsklauseln. Das Gericht stellte fest, dass diese gegebenenfalls um „zusätzlichen Maßnahmen" (supplementary measures) ergänzt werden müssten, damit die Daten im Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU. Aus dem Urteil ergibt sich, dass die Standardvertragsklauseln keinen hinreichenden Schutz vor Zugriffen auf personenbezogene Daten aus der EU durch Nachrichtendienste oder andere Sicherheitsbehörden der USA bieten. Hier ist im Einzelfall die genaue Prüfung zusätzlicher Maßnahmen erforderlich.

Die Auswirkungen des Urteils auf andere Drittländer und auf weitere Übermittlungsinstrumente gemäß Art. 46 DSGVO werden durch den Europäischen Datenschutzausschuss (EDSA) im Rahmen der Arbeiten der Expertenuntergruppe „International Transfers" behandelt (vgl. Nr. 3.2.2.2).

II. Taskforce Supplementary Measures – Empfehlungen des EDSA zu den zusätzlichen Maßnahmen

Wie bereits in meinem letzten Tätigkeitsbericht erwähnt, wurden am 10. November 2020 im EDSA die Empfehlungen zu den „zusätzlichen Maßnahmen" angenommen („Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" – Version 2.0). Diese Empfehlungen konnte der EDSA am 18. Juni 2021 in seiner endgültigen Fassung verabschieden[2]. Der abschließenden Annahme durch den EDSA war eine öffentliche Konsultation vorausgegangen. Die Ergebnisse der Konsultation wurden durch ein Drafting Team ausgewertet, dem ich selbst und weitere Aufsichtsbehörden der Länder angehörten.

Die Empfehlungen sollen Datenexporteure bei der Bewertung unterstützen, ob bei einer Übermittlung von Daten an Drittländer zusätzliche Maßnahmen erforderlich sind. Die Empfehlungen enthalten dazu praktische Beispiele für verschiedene Übermittlungsszenarien. Außerdem findet sich in einem Annex eine nicht abschließende Liste möglicher zusätzlicher Maßnahmen, wie z. B. einer Datenverschlüsselung.

III. Umsetzung / Kontrollen

Im Schrems II-Urteil hat der EuGH eine klare Aufgabenzuweisung vorgenommen. Unternehmen und öffentliche Stellen sind verpflichtet, selbständig die Rechtmäßigkeit ihrer Datentransfers an Drittländer zu prüfen und gegebenenfalls anzupassen. Hierbei werden sie durch die Aufsichtsbehörden beraten und kontrolliert. Wie bereits in meinem letzten Tätigkeitsbericht und in Kapitel 3.2.2.2 ausgeführt, haben die Aufsichtsbehörden auf nationaler und europäischer Ebene Hilfestellungen für Verantwortliche und Auftragsverarbeiter (Datenexporteure) erarbeitet. Im Oktober 2020 habe ich mit einem Informationsschreiben an die öffentlichen Stellen des Bundes sowie die meiner Aufsicht unterliegenden Unternehmen Hinweise zu den Auswirkungen der Rechtsprechung des EuGH auf den internationalen Datentransfer gegeben[3]. In dem Schreiben habe ich die Kernaussagen des Urteils zusammengefasst. Darüber hinaus habe ich auf die Verpflichtung der datenexportierenden Stelle zur Prüfung der Schrems II-Grundsätze bei Datenübermittlung an Drittländer hingewiesen. In meinem Zuständigkeitsbereich habe ich im Berichtszeitraum mit Kontrollmaßnahmen zur Umsetzung der Schrems II-Anforderungen begonnen.

Auf meiner Webseite unterstütze ich Verantwortliche und Auftragsverarbeiter mit aktuellen Informationen zur Thematik.[4]

Die aus dem Schrems II-Urteil resultierenden, komplexen Rechtsfolgen werden die deutschen und europäischen Aufsichtsbehörden in ihrer Arbeit weiterhin erheblich fordern. Abhilfe können langfristig einheitliche, rechtsbasierte internationale Standards für globale Datentransfers sein, die auch den besonders kritischen Aspekt des staatlichen Zugriffs auf personenbezogene Daten (sog. Government Access) erfassen.

3.2.2.2 Schwerpunkt Drittlandübermittlung

Wenn Daten in ein Drittland oder an eine internationale Organisation übermittelt werden, müssen Verantwortliche oder Auftragsverarbeiter zunächst prüfen, ob die allgemeinen Voraussetzungen der DSGVO für eine Datenübermittlung erfüllt sind. Außerdem muss den zusätzlichen Anforderungen nach Kapitel V der DSGVO Rechnung getragen werden. Mit dem sogenannten Schrems II-Urteil des EuGH (Rechtssache C-311/185) wurden neue Maßstäbe gesetzt. Die erheblichen Auswirkungen des Urteils auf Datenübermittlungen in Drittländer stellen an Verantwortliche, Auftragsverarbeiter und Aufsichtsbehörden hohe Anforderungen. Sie haben die Arbeit der Expert Subgroups International Transfers (ITS ESG) und Borders, Travel and Law Enforcement (BTLE ESG) im Berichtsjahr geprägt.

In Zusammenarbeit mit den Aufsichtsbehörden der Länder in den Expert Subgroups ITS ESG und BTLE des Europäischen Datenschutzausschusses (EDSA) war der Schwerpunkt meiner Aktivitäten:

- → die Erarbeitung von Leitlinien und Empfehlungen für Datenübermittlungen an Drittländer oder internationale Organisationen sowie
- → Stellungnahmen zu Angemessenheitsbeschlüssen und sonstigen datenschutzrelevanten Entscheidungen der Europäischen Kommission.

---

2 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal dataVersion 2.0 Adopted on 18 June2021, abrufbar unter: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

3 Informationsschreiben des BfDI, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2020/Rundschreiben-Informationen-Schrems-II.html

4 Informationen auf der BfDI Webseite, abrufbar unter: www.bfdi.bund.de/schrems-II

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

I. Angemessenheitsbeschlüsse

Nach Art. 45 DSGVO bzw. Art. 36 JI-RL kann die Europäische Kommission feststellen, dass ein Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau gewährleistet. Findet eine Datenübermittlung im Anwendungsbereich eines Angemessenheitsbeschlusses statt, bedarf es keiner besonderen Genehmigung durch die Datenschutz-Aufsichtsbehörden. Die Datenübermittlung muss von keinen weiteren Schutzmaßnahmen aus Kapitel V der DSGVO bzw. Kapitel V der JI-RL begleitet werden. Dessen ungeachtet bleibt es erforderlich zu prüfen, ob die allgemeinen datenschutzrechtlichen Voraussetzungen für die entsprechende Datenverarbeitung erfüllt sind. Der Ausschuss hat im Berichtszeitraum Stellungnahmen zu den Angemessenheitsbeschlüssen zum Vereinigten Königreich und zu Südkorea abgegeben.

Vereinigtes Königreich

Die Europäische Kommission startete am 19. Februar 2021 das Annahmeverfahren zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (vgl. 6.11). Zu beiden Entwürfen der Angemessenheitsbeschlüsse hat der EDSA im Annahmeverfahren zwei Stellungnahmen abgegeben[6]. Darin stellt er fest, dass der Datenschutzrahmen des Vereinigten Königreichs weitgehend auf dem Datenschutzrahmen der Europäischen Union basiert. Er betont aber auch, dass einige Punkte genauer überwacht werden müssen. U. a. die Ausnahmeregelung für den Einwanderungsbereich und deren Auswirkungen auf die Rechte der betroffenen Personen.

Überwacht werden müssen auch mögliche Beschränkungen bei der Übermittlung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in das Vereinigte Königreich (z. B. auf Grundlage künftiger Angemessenheitsbeschlüsse des Vereinigten Königreichs oder internationaler Abkommen zwischen dem Vereinigten Königreich und Drittländern).

Darüber hinaus kritisiert der EDSA verschiedene Regelungen und Praktiken im Sicherheitsbereich, die weiter beobachtet und geprüft werden müssten. Beispielsweise das Abfangen von Massendaten oder die unabhängige Bewertung und Überwachung des Einsatzes von Instrumenten für die automatisierte Datenverarbeitung.

Der EDSA erwartet, dass sich die Gesetze im Vereinigten Königreich weiterentwickeln und verlangt, die Angemessenheit kontinuierlich zu beobachten und zeitlich zu begrenzen. Der EDSA begrüßt die Verfallsklausel der beiden von der Europäischen Kommission am 28. Juni 2021 angenommenen Angemessenheitsbeschlüsse gemäß der Datenschutz-Grundverordnung (DSGVO) und der Strafverfolgungsrichtlinie (JI-RL), die bis zum 27. Juni 2025 befristet sind.

Republik Korea

Am 16. Juni 2021 leitete die Europäische Kommission das Verfahren zur Annahme des Angemessenheitsbeschlusses für die Datenübermittlung an die Republik Korea ein. Grundlage für die Verarbeitung von personenbezogenen Daten an die Republik Korea ist das nationale Gesetz zum Schutz personenbezogener Daten (Personal Information Protection Act – PIPA), das in den Kernelementen mit dem Datenschutzniveau der EU übereinstimmt.

Der EDSA hat in seiner Stellungnahme vom 24. September 2021 keine grundsätzlichen Bedenken gegen den Angemessenheitsbeschluss geäußert. Er bittet die Kommission jedoch, bestimmte Begriffe und Regeln des koreanischen Rechts klarzustellen[7]. Der Angemessenheitsbeschluss wurde am 17. Dezember 2021 von der Europäischen Kommission angenommen[8].

II. Neue Standarddatenschutzklauseln der Europäischen Kommission

Wie bereits in meinem letzten Tätigkeitsbericht dargelegt, hatte der EuGH im Schrems II-Urteil (EuGH-Urteil vom 16. Juli 2020: Rechtssache C-311/18) die Unwirksamkeit des EU-US-Privacy Shields festgestellt. Das hat zur Folge, dass auf dieser Grundlage keine Datenübermittlungen mehr aus der EU an die USA stattfinden können. In seinem Urteil hat der EuGH zwar das Instrument der Standardvertragsklauseln (SDK) nicht grundsätzlich in Frage gestellt, aber festgelegt, dass diese gegebenenfalls um sogenannte „zusätzlichen Maßnahmen“ (vgl. o. 3.2.2.1) ergänzt werden müssten. Dies, damit die Daten im Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU. Denn die Standardvertragsklauseln reichen nach Feststellungen des Gerichts gegebenenfalls als Schutz vor möglichen Zugriffen durch Nachrichtendienste oder sonstige Sicherheitsbehörden auf personenbezogene Daten aus der EU nicht aus.

---

6 EDPB Opinions on draft UK adequacy decisions, abrufbar unter: https://edpb.europa.eu/news/news/2021/edpb-opinions-draft-uk-adequacy-decisions_en

7 Opinion 32/2021regardingthe European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea Version 1.0 Adopted on 24 September 2021; abrufbar unter: https://edpb.europa.eu/system/files/2021-09/edpb_opinion322021_republicofkoreaadequacy_en.pdf

8 COMMISSION IMPLEMENTING DECISION of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act: https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf

Am 4. Juni 2021 hat die Europäische Kommission überarbeitete Standarddatenschutzklauseln (SDK) erlassen, welche die Vorgaben des Schrems II-Urteils berücksichtigen, aber eine Prüfung der Rechtslage und Behördenpraxis im Drittland im Einzelfall nicht entbehrlich machen[9]. Dabei hat die Kommission einen modularen Ansatz verfolgt, der mehr Flexibilität bei der Gestaltung von Drittstaatenübermittlungen bieten soll. Für die Nutzer der alten Standardvertragsklauseln der Kommission ist ein 18-monatiger Übergangszeitraum vorgesehen, um die bisherigen Standardvertragsklauseln auf die neuen umzustellen.

Die deutschen Aufsichtsbehörden hatten zu dem Entwurf dieser neuen SDK eine eigene Position entwickelt, die in den EDSA eingebracht wurde. Sie findet sich an vielen Stellen in der gemeinsamen Stellungnahme des EDSA und des Europäischen Datenschutzbeauftragten (EDSB) vom 14. Januar 2021 wieder[10]. Zu den neuen Standardvertragsklauseln der Europäischen Kommission zur Auftragsverarbeitung (vgl. 3.2.4).

III. Genehmigte Verhaltensregeln – Codes of Conduct

Der EDSA hat in der ITS ESG unter aktiver Mitwirkung meiner Behörde als Co-Rapporteur Leitlinien erarbeitet, die zu genehmigende branchenspezifische Verhaltensregeln als angemessene Garantie nach Art. 46 DSGVO für die Übermittlung von personenbezogenen Daten an ein Drittland zu behandeln. Im Unterschied zu den Codes of Conduct, die die Anforderungen des Art. 28 DSGVO präzisieren (vgl. 3.2.3), handelt es sich um spezielle Verhaltensregeln, die Datenübermittlungen in Drittstaaten einfacher machen sollen. Insbesondere können Datenimporteure im Drittland – die nicht der DSGVO unterliegen – diesen Verhaltensregeln beitreten, um geeignete Garantien für die Datenübermittlung zu bieten. Die Leitlinien geben praktische Hinweise zu den Anforderungen, zum Verfahren bis hin zur Annahme dieser Kodizes für die beteiligten Akteure. Außerdem sollen sie als Referenz für alle internationalen Kontrollinstanzen, den EDSA und die Kommission im Hinblick auf eine einheitliche Bewertung der Kodizes dienen.

Aktuell werden die Eingaben aus der öffentlichen Konsultation ausgewertet, die zum 1. Oktober 2021 endete. Die Guidelines sollen Anfang nächsten Jahres durch den EDSA angenommen werden.

IV. Zertifizierung als Datenübermittlungsinstrument an Drittstaaten

Als ein weiteres Instrument für Datenübermittlungen in Drittländer bestimmt die DSGVO in Art. 46 Abs. 2 das Instrument der Zertifizierung. Die ITS ESG beschäftigte sich im Berichtsjahr mit der Erstellung von Leitlinien für dieses Übermittlungsinstrument. Hier habe ich in der ITS ESG die Rolle des Hauptberichterstatters übernommen. Da der EDSA bereits im Jahre 2018 allgemeine Leitlinien zur Zertifizierung und Akkreditierung im Rahmen der Datenschutz-Grundverordnung (DSGVO) veröffentlicht hat, konzentrieren sich diese Leitlinien auf die spezifischen Aspekte der Zertifizierung als Instrument für Datentransfers. Sie sollen Hinweise für die Anwendung in der Praxis geben.

Die Leitlinien sollen dem EDSA zeitnah zur Verabschiedung vorgelegt und in die öffentliche Konsultation gegeben werden.

V. Verbindliche interne Datenschutzvorschriften – Binding corporate rules (BCR)

Die verbindlichen internen Datenschutzvorschriften (BCR) sind eine weitere geeignete Garantie des Kapitels V der DSGVO für eine Übermittlung an Drittländer. Auf Ebene der ITS ESG werden eine Vielzahl von BCR geprüft und Einzelfragen geklärt. Darüber hinaus befasst sich die ITS ESG mit der Weiterentwicklung des BCR-Annahmeverfahrens des EDSA im Hinblick auf deren Effizienz (Qualitätssicherung, Beschleunigung, Vereinfachung).

Querverweise:

3.2.2.1 Taskforce Supplementary Measures, 3.2.3 Abschluss Kohärenzverfahren CoC, 3.2.4 Leitlinien Verantwortlichkeit und neue Standardvertragsklauseln, 6.11 Brexit

9 s. hierzu ausführlich die Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 21. Juni2021, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pm/2021_pm_neue_scc.pdf

10 Gemeinsame Stellungnahme1/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern für die in Art. 28 Abs. 7 der Verordnung (EU) 2016/679 und Art. 29 Abs. 7 der Verordnung (EU) 2018/1725 genannten Aspekte, abrufbar unter: https://edpb.europa.eu/system/files/2021-04/edpb-edpsjointopinion01_2021_sccs_c_p_de_1.pdf

3.2.3 Abschluss Kohärenzverfahren CoC EU Cloud und CISPE

Der Europäische Datenschutzausschuss hat am 19. Mai 2021 die positiven Stellungnahmen zu den beiden thematisch eng verwandten Codes of Conduct „EU Cloud CoC“ und „CISPE CoC“ angenommen. Es handelt sich um die ersten EU-weiten Verhaltensregeln, zu denen der EDSA eine Stellungnahme im Kohärenzverfahren angenommen hat.

Erstmalig hat der Europäische Datenschutzausschuss im Rahmen eines Kohärenzverfahrens zwei positive Stellungnahmen zu Verhaltensregeln, sogenannten Codes of Conduct (CoC), angenommen und damit bestätigt, dass diese den Anforderungen der Datenschutz-Grundverordnung entsprechen.

Codes of Conduct sind Verhaltensregeln, die die Anwendung der DSGVO präzisieren. Das Bedürfnis für eine solche Präzisierung ergibt sich daraus, dass die Verordnung an vielen Stellen unbestimmt ist und Generalklauseln enthält. Verhaltensregeln können als Auslegungshilfen herangezogen werden und dienen daher der Rechtssicherheit. Die DSGVO knüpft bestimmte, für die dem Code of Conduct beigetretenen Unternehmen „positive“ Folgen an die Einhaltung der von der zuständigen Behörde genehmigten Verhaltensregeln. So kann die Einhaltung der genehmigten Verhaltensregeln z. B. als Gesichtspunkt herangezogen werden, um nachzuweisen, dass die Verantwortlichen ihre Pflichten erfüllen (Art. 24 Abs. 3 DSGVO).

Auch kann sie als Faktor herangezogen werden, um hinreichende Garantien bei der Einhaltung der Anforderungen an den Auftragsverarbeiter (Art. 28 Abs. 5) oder die Erfüllung der in Art. 32 Abs. 1 genannten Anforderungen an die Sicherheit der Verarbeitung nachzuweisen (Art. 32 Abs. 3). Zudem ist sie bei der Datenschutzfolgenabschätzung zu berücksichtigen (Art. 35 Abs. 8). Zu erwähnen ist insbesondere auch, dass die Einhaltung bei der Verhängung von Geldbußen zu berücksichtigen ist (Art. 83 Abs. 2 Satz 2 lit. j) DSGVO).

Der EU Cloud CoC adressiert alle Services des Cloud-Marktes und konkretisiert insoweit die Anforderungen des Art. 28 DSGVO zur Auftragsverarbeitung und der damit verbundenen Vorschriften der DSGVO. Cloud Service Provider sind Auftragsverarbeiter. Der EU Cloud CoC gibt praktische Hilfe und definiert spezifische Anforderungen für Cloud-Service-Provider. Der CISPE CoC ist wie der EU Cloud CoC ein europäischer Verhaltenskodex für Cloud Service Provider. Er adressiert aber anders als der EU Cloud CoC lediglich spezifische Features von Providern, die Infrastructure as a Service anbieten.

Codes of Conduct sind nicht nur ein Instrument der Selbstregulierung, sondern dienen zugleich auch der Transparenz gegenüber den Betroffenen. Ich begrüße daher sehr, dass auf diese Weise auch die Wirtschaft ihren Beitrag zur Konkretisierung und Handhabbarkeit der DSGVO leistet.

3.2.4 Leitlinien Verantwortlichkeit und neue Standardvertragsklauseln

Der Europäische Datenschutzausschuss (EDSA) hat im Juli 2021 die endgültige Fassung der Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO angenommen. Zudem hat die Europäische Kommission im Juni 2021 neue Standardvertragsklauseln zur Auftragsverarbeitung herausgegeben, zu denen der EDSA zuvor Stellung genommen hatte.

Der EDSA hatte 2020 die Konsultationsfassung der Leitlinien 07/2020 verabschiedet (vgl. 29. TB Nr. 3.2.1). Nach Abschluss der öffentlichen Konsultation wurden die Leitlinien noch leicht überarbeitet und präzisiert. Die Begriffe „Verantwortlicher“, „Gemeinsam Verantwortliche“ und „Auftragsverarbeiter“ sind für die an der Datenverarbeitung beteiligten Akteure von zentraler rechtlicher Bedeutung. Die Leitlinien geben Hilfestellung, wie diese Begriffe voneinander abzugrenzen sind. Der Anhang der Leitlinien enthält ein Flow-Chart, das es den beteiligten Akteuren ermöglicht, ihre Rolle bzgl. einer Datenverarbeitung zu prüfen. Die Leitlinien stehen auf der Seite des EDSA zum Abruf zur Verfügung[11]. Die deutsche Fassung wird Anfang 2022 eingestellt werden.

Ein weiteres wichtiges Dokument im Bereich der Auftragsverarbeitung sind die neuen Standardvertragsklauseln, die die Kommission als Durchführungsbeschluss nach Art. 28 Abs. 7 DSGVO herausgegeben hat (Durchführungsbeschluss [EU] 2021/915, ABl. EU L 199, S. 18). Die Kommission stellt mit den Standardvertragsklauseln ein Muster für eine Auftragsverarbeitungsvereinbarung (Art. 28 Abs. 3 DSGVO) zur Verfügung. Wichtig ist, dass diese Standardvertragsklauseln nur für die innereuropäische und damit selbstverständlich auch für die innerdeutsche Datenverarbeitung greifen. Sofern Daten in Drittländer übermittelt werden, finden die neuen Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c DSGVO Anwendung (vgl. Nr. 3.2.2.2).

Querverweise:

3.2.2 EDSA Schwerpunkt Drittlandübermittlung

11 https://edpb.europa.eu

3.2.5 Leitlinien Recht auf Auskunft Art. 15 DSGVO

3.2.5.1 Auskunftsanspruch bei den Sozialleistungsträgern

Obwohl die Vorschriften der DSGVO bereits seit dem 25. Mai 2016 in Kraft getreten und seit dem 25. Mai 2018 als unmittelbar geltendes Recht anzuwenden sind, können eine Vielzahl von Sozialleistungsträgern dem datenschutzrechtlichen Auskunftsanspruch als Betroffenenrecht noch immer nicht ordnungsgemäß Rechnung tragen.

Gemäß Art. 15 Abs. 3 S. 3 DSGVO sind die Informationen im Rahmen des Auskunftsanspruchs durch den Verantwortlichen 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. Diesen Rechtsanspruch machten im Berichtszeitraum mehrere Beschwerdeführende in ihrem elektronischen Antrag auf Auskunft gegenüber der Deutschen Rentenversicherung Bund (DRV Bund) geltend. Die entsprechenden Auskünfte nach Art. 15 Abs. 3 S. 3 DSGVO wurden von der DRV Bund jedoch nicht in dem gesetzlich vorgeschriebenen elektronischen Format zur Verfügung gestellt. Dies führte zu zahlreichen Eingaben, in Folge derer ich die DRV Bund zur Stellungnahme aufforderte. Daraufhin teilte mir die DRV Bund mit, dass sie derzeit kein geeignetes elektronisches Verfahren zur Verfügung stellen kann, durch welches eine Auskunft nach Art. 15 Abs. 3 S. 3 DSGVO beantragt und erteilt werden kann. Dies verstößt nachhaltig gegen die DSGVO. Hinzu kommt, dass die DRV Bund seit Geltung der DSGVO (25. Mai 2018) ausreichend Zeit hatte, ein gängiges elektronisches Auskunftsverfahren zur Auskunftserteilung nach Art. 15 Abs. 3 S. 3 DSGVO zu implementieren. Aufsichtsrechtliche Maßnahmen werden derzeit vorbereitet.

3.2.5.2 Auskunftserteilung nach Art. 15 DSGVO durch Krankenkassen

Im Berichtszeitraum erreichten mich zahlreiche Beschwerden, die Unsicherheiten der Krankenkassen im Umgang mit dem Auskunftsrecht ihrer Versicherten gemäß Art. 15 DSGVO offenbarten.

Das Auskunftsrecht gemäß Art. 15 DSGVO ist ein zentrales Instrument des Datenschutzes zur Herstellung von Transparenz in der Datenverarbeitung. Doch obwohl die DSGVO nunmehr seit dem 25. Mai 2018 gilt, herrscht im Hinblick auf die praktische Umsetzung des Auskunftsrechts bei vielen Krankenkassen noch immer große Unsicherheit. Dies zeigen die vielen Beschwerden gemäß Art. 77 DSGVO der Versicherten, die mich um Unterstützung bei der Durchsetzung ihres Rechts ersuchten.

Folgende Beispiele sind typisch für einige Fehlerquellen bei der Bearbeitung von Auskunftsersuchen durch die Krankenkassen:

- **Ablehnung der Auskunftserteilung unter Berufung auf § 83 Abs. 2 SGB X**
  § 83 Abs. 2 SGB X schränkt den Auskunftsanspruch auf nationaler Ebene ein, indem er den Anspruchsberechtigten anhält („soll“), grundsätzlich die Art der Sozialdaten, über die Auskunft erbeten wird, näher zu bezeichnen. Bei großen Organisationseinheiten – wie den Krankenkassen – ist dies die Regel, da sie über komplexe Datenverarbeitungen verfügen. Von daher ist die angeblich mangelnde Konkretisierung des Auskunftsbegehrens durch den Betroffenen kein absoluter Ausschlussgrund für die Auskunftserteilung. Wenn die Sozialdaten jedoch nicht automatisiert oder nicht in automatisierten Datenverarbeitungsanlagen gespeichert sind, d. h. analog in Papierform vorliegen, wird aus dem „soll“ ein „muss“. D. h. in diesem Fall muss die Krankenkasse nur dann Auskunft geben, wenn der Antragsteller so präzise Angaben macht, dass die Sozialdaten aufgefunden werden können (Art. 83 Abs. 2 S. 2 SGB X). Zudem kann die Krankenkasse das Informationsinteresse und den Aufwand zum Auffinden der Sozialdaten gegeneinander abwägen und soweit letzteres unverhältnismäßig ist, die Auskunft verweigern. Danach kann der Krankenkasse beispielsweise nicht zugemutet werden, in großen Papierarchiven nach den begehrten Informationen zu suchen. Angesichts des Umfangs der Digitalisierung bei den Krankenkassen dürfte diese Regelung allerdings nur noch selten anwendbar sein.

- **Ausschluss der mit dem Versicherten geführten Korrespondenz**
  Soweit der Auskunftsersuchende gemäß Art. 15 Abs. 3 DSGVO Kopien der personenbezogenen Daten anfordert, die Gegenstand der Verarbeitung sind, schließt der Verantwortliche hiervon gelegentlich den mit dem Anspruchsteller geführten Schriftverkehr aus. Dies erfolgt unter Berufung auf Erwägungsgrund (EG) 62 der DSGVO, wonach sich die Pflicht, Informationen zur Verfügung zu stellen, erübrigt, wenn die betroffene Person die Information bereits hat. Verkannt wird hierbei, dass sich der genannte Erwägungsgrund nicht auf den hier maßgeblichen Art. 15 DSGVO bezieht, sondern auf die Art. 13 und 14 DSGVO (Informationspflichten des Verantwortlichen). Der Anspruch aus Art. 15 DSGVO beinhaltet also grundsätzlich auch die mit dem Betroffenen geführte Korrespondenz.

- **Keine Differenzierung zwischen Auskunftsanspruch und Akteneinsichtsrecht**
  In einigen Fällen musste ich feststellen, dass Auskunftsersuchen mit der Begründung abgelehnt wurden, es bestehe kein berechtigtes Interesse an einer Auskunft. Der Betroffene muss jedoch kein berechtigtes Interesse darlegen. Sein Auskunftsanspruch gemäß Art. 15 DSGVO liegt – soweit keine Ausschlussgründe vorliegen – grundsätzlich nicht im Ermessen des Verantwortlichen. Der Grund für die fehlerhafte Rechtsauslegung der Krankenkassen lag häufig in der falschen Einordnung der Auskunftsersuchen als Anträge auf Akteneinsicht gemäß § 25 SGB X. Dieses Recht unterliegt tatsächlich strengeren Anspruchsvoraussetzungen und verlangt unter anderem ein berechtigtes Interesse, dass die Kenntnis des Akteninhalts erforderlich ist, um die rechtlichen Interessen des Betroffenen geltend machen zu können. Zur Vermeidung von Verfahrensverzögerungen rate ich deshalb den Betroffenen, sich bei Antragsstellung ausdrücklich auf Art. 15 DSGVO zu berufen.

- **Verweigerung der Anspruchserfüllung in elektronischer Form**
  Vereinzelt haben sich Betroffene darüber beschwert, dass Krankenkassen ebenso wie andere Träger von Sozialleistungen Kopien personenbezogene Daten nicht in einem elektronischen Format zur Verfügung stellten. Darauf hat der Antragsteller oder die Antragstellerin aber dann einen Anspruch, wenn der Antrag selbst ebenfalls elektronisch gestellt wurde (Art. 15 Abs. 3 S. 3 DSGVO). Der Einwand angeblich fehlender technischer Voraussetzungen oder eines unverhältnismäßigen Aufwands lässt die DSGVO bei der elektronischen Anspruchserfüllung nicht gelten. Die Krankenkassen sind zu dieser Form der Auskunftserteilung verpflichtet.

- **Fristversäumnis**
  Wiederholt erreichten mich im Berichtszeitraum Beschwerden von Versicherten darüber, dass die Krankenkasse ihre Auskunftsersuchen nicht innerhalb der Monatsfrist gemäß Art. 12 Abs. 3 DSGVO bescheiden. Häufiger Grund hierfür sind interne Kommunikations- und Ablaufmängel. In den meisten Fällen konnte ich hier eine kurzfristige Erledigung der Angelegenheit erreichen.

3.2.6 Leitlinien für Streitbeilegungsverfahren vor dem EDSA

Leitlinien für Streitbeilegungsverfahren vor dem EDSA beschreiben Verfahren, um zu einem verbindlichen Beschuss für die europäischen Datenschutzbehörden zu gelangen.

Die Leitlinien "Guidelines 03/2021 on the application of Article 65(1)(a) GDPR" beschreiben den Ablauf eines Streitbeilegungsverfahrens durch den EDSA gemäß Art. 65 Abs. 1 lit. a) DSGVO. Das Streitbeilegungsverfahren hat das Ziel, Streitigkeiten zwischen der federführenden Aufsichtsbehörde und den beteiligten Aufsichtsbehörden durch den EDSA verbindlich entscheiden zu lassen. Derartige Streitigkeiten können entstehen, wenn europäische Aufsichtsbehörden bei einer grenzüberschreitenden Verarbeitung von personenbezogenen Daten im Rahmen ihrer von der DSGVO vorgesehenen Zusammenarbeit im Kooperationsverfahren keinen Konsens finden konnten. In solchen Fällen muss die Angelegenheit dem EDSA vorgelegt werden, der sodann einen verbindlichen Beschluss erlässt und damit dem Ziel einer einheitlichen Rechtsanwendung auch in Einzelfällen Rechnung trägt. Die Leitlinien beschreiben u. a. den Ablauf des Verfahrens und die Voraussetzungen, unter denen der EDSA einen verbindlichen Beschluss erlassen kann, sowie seine Entscheidungsbefugnis. Sie stellen damit wichtige Regeln auf und haben in den 2021 durchgeführten Streitbeilegungsverfahren bereits Anwendung gefunden.

3.3 Global Privacy Assembly

3.3.1 Allgemeiner Bericht

Der BfDI war im Berichtsjahr Mitglied im Leitungsgremium der Global Privacy Assembly (GPA). Dieses Executive Committee nimmt wichtige Aufgaben wahr, die für die GPA und dessen Stimme in der Welt von wesentlicher Bedeutung sind. Die diesjährige Vollversammlung der GPA hat zahlreiche Datenschutzthemen bearbeitet und wegweisende Entschließungen verabschiedet.

Wie ich bereits in meinem letzten TB berichtet habe, wurde ich im Oktober 2020 in das Executive Committee (ExCo) GPA gewählt. Zusätzlich zu den fünf gewählten Mitgliedern sind jeweils der vergangene und der aktuelle Gastgeber der Jahreskonferenz Mitglieder im Executive Committee[12].

Das ExCo hat als Leitungsgremium der GPA den Überblick über die Themen der einzelnen Arbeitsgruppen

12 Die Mitglieder des ExCo´s samt Lebensläufe sind auf der Internetseite der GPA veröffentlicht: https://globalprivacyassembly.org/the-assembly-and-executive-committee/executive-committee/

und darüber, wie die Ziele der GPA vorangebracht werden. Der Auftrag und die politischen Schwerpunkte werden in der GPA durch Entschließungen festgelegt. Im Berichtsjahr wurden die Umsetzung der Strategischen Planung 2019-2021 sichergestellt und die Weichen für die Strategische Planung in den kommenden Jahren (2021-2023) gestellt.

Eine weitere bedeutende Aufgabe des ExCo ist die Vertretung der GPA nach außen. So kann es beispielsweise gemeinsame Stellungnahmen (joint statement) zu globalen Themen abgeben. Dies war im Berichtsjahr der Fall, als Gesundheitsdaten bei nationalen und internationalen Reisen verarbeitet wurden. Hier hat sich das ExCo nicht generell gegen deren Verarbeitung ausgesprochen, sondern vielmehr auf die Bedeutung von wesentlichen Datenschutzgrundsätzen und Praktiken hingewiesen.

Höhepunkt der Arbeit der GPA ist die Jahreskonferenz, die im Berichtsjahr aufgrund der Einschränkungen durch Covid-19 nur digital stattfinden konnte. Sie wurde von der mexikanischen Aufsichtsbehörde organisiert. Das Motto war: „Privacy and Data Protection: A human centric approach"; der Mensch soll beim Datenschutz in den Mittelpunkt gestellt werden. Bei den vielfältigen Programmpunkten haben Covid-19 und neue Technologien – insbesondere KI – eine bedeutende Rolle eingenommen.

Die GPA hat auch wichtige Entschließungen verabschiedet, an deren Ausarbeitung ich mitgewirkt habe. Einen besonderen Stellenwert hat hier der Strategieplan für die Jahre 2021-23. Immer bedeutsamer wird der stetig zunehmende internationale Datentransfer. Der zunehmende Datenfluss darf aber nicht zu einer Aufweichung oder gar einer Abschaffung des Datenschutzes führen. Hier will die GPA praktische Herangehensweisen erarbeiten, wie Personen geschützt werden können, deren personenbezogene Daten verarbeitet werden. Damit soll sichergestellt werden, dass in Zeiten des technologischen Fortschritts und datenbasierter Geschäftsmodelle die GPA-Stimme weiterhin gehört wird. Eine weitere Entschließung stammt aus der Covid-19-Arbeitsgruppe der GPA. Der Fokus ihrer Arbeit lag zunächst auf unmittelbaren Maßnahmen der Pandemiebekämpfung. Daran anknüpfend richtet die Gruppe ihren Blick stärker in die Zukunft über den engen Bezug zur COVID-19-Pandemie hinaus.

Das Mandat der Gruppe wird erweitert um sämtliche Aspekte der Datenverarbeitung zu Zwecken des Allgemeinwohls. Ein für die GPA als Organisation wichtiger Entschluss war die Entscheidung, ein durch Mitgliedsbeiträge finanziertes GPA-Sekretariat einzurichten. Schließlich ist die Entschließung zum „Government Access" zu nennen, welche die Problematik des Zugriffs auf private Daten durch Nachrichtendienste und Sicherheitsbehörden behandelt und dafür datenschutzrechtliche Grundsätze aufzeigt (s. Nr. 3.4.3).

Die GPA Jahreskonferenz 2022 wird von der türkischen Datenschutzbehörde (KVKK) ausgerichtet.

Querverweise:

3.3.2 Reference Panel, 3.4.2 Berlin Group, 3.4.3 Datenschutzgrundsätze für den staatlichen Zugriff auf personenbezogene Daten im internationalen Bereich, 4.2 Künstliche Intelligenz – Regulierung als gesamtgesellschaftliche Aufgabe

3.3.2 Reference Panel

Die Global Privacy Assembly – eine weltweite Vereinigung von Datenschutzbehörden – hat im März 2021 mit dem „Reference Panel" ein neues Gremium mit unabhängigen Fachexpertinnen und -experten geschaffen. Ich habe den ersten Vorsitz im Panel übernommen.

Die Global Privacy Assembly (GPA), die bis 2019 unter dem Namen „International Conference of Data Protection and Privacy Commissioners" bekannt war, hatte bei ihrer 40. Konferenz 2018 in Brüssel eine Reihe von Maßnahmen beschlossen, um sich selbst zu modernisieren und den Anforderungen des digitalen Zeitalters besser gerecht zu werden. Neben einem neuen Namen – Global Privacy Assembly – gehörte zu diesen Maßnahmen die Einrichtung eines Gremiums mit unabhängigen Expertinnen und Experten, die verschiedene Bereiche, z. B. Wissenschaft, Nichtregierungsorganisationen, freie Wirtschaft oder öffentliche Behörden, vertreten sollen. Dieses neue Gremium externer Fachleute hat die Aufgabe, zusätzliche Expertise und Sichtweisen von außerhalb in die GPA einzubringen. Damit soll sichergestellt werden, dass die Arbeiten der GPA für alle beteiligten Stellen und Akteure in der digitalen Gesellschaft relevant und nützlich sind.

Nachdem die 42. Jahresversammlung der GPA im Herbst 2020 ein Konzept und den Namen für das neue Gremium – GPA Reference Panel – beschlossen hatte, begann zu Beginn des Berichtsjahres der Auswahlprozess geeigneter Panel-Mitglieder unter Federführung einer zu diesem Zweck eingesetzten „GPA Reference Panel Assessment Group", die vom Vorsitz der GPA, der britischen Datenschutzbehörde UK Information Commissioner (ICO), geleitet wurde und deren Arbeiten ich unterstützt habe. Dabei ist es gelungen, insgesamt 16 namhafte Datenschutz-Expertinnen und Experten aus Deutschland und aus Europa in diese internationale Gruppe zu berufen. Den beiden Mitgliedern aus Deutschland, Herrn Andreas Mundt, Präsident des Bundeskartellamt, und Frau Prof. Franziska Böhm vom Karlsruher Institut für

Technologie (KIT), danke ich ganz besonders für Ihre Bereitschaft, an dem GPA Reference Panel mitzuwirken.

In meiner Eigenschaft als Mitglied des „Executive Committee“ der GPA, dem ich seit Oktober 2020 angehöre, habe ich den Vorsitz im GPA Reference Panel übernommen. Dessen erste Aufgabe bestand darin, den Gastgeber des 43. Jahrestreffens der GPA, die mexikanische Datenschutzbehörde INAI, im Herbst 2021 bei der Erstellung des inhaltlichen Programms der Tagung zu unterstützen. Eine weitere wesentliche Aufgabe des GPA Reference Panels besteht darin, die Berichte und Papiere der thematischen Arbeitsgruppen der GPA einer kritischen Prüfung im Sinne einer „peer review“ zu unterziehen, sofern dies von den Vorsitzenden der betreffenden Arbeitsgruppen oder einem Autoren-Team eines solchen Berichts gewünscht wird. Auch in Bezug auf diese Aufgabe des Panels begrüße ich, dass hierzu eine rege Nachfrage von Seiten der GPA-Arbeitsgruppen bereits in der ersten Zeit seines Bestehens bestand. So haben verschiedene Mitglieder des GPA Reference Panels einen umfassenden Bericht der Policy Strategy Working Group – Workstream 3 zum Thema „Datenschutz und andere Grundrechte bzw. im Verhältnis zu anderen Grundrechten“ analysiert und den Verfasserinnen und Verfassern ausführlich geantwortet.

Aus meiner Sicht ist es für die Global Privacy Assembly von entscheidender Bedeutung, dass sie „über den Tellerrand“ hinaus blickt und die Verbindung zur Zivilgesellschaft sowie zu wichtigen Akteuren des digitalen Zeitalters sucht. Nur dann wird die GPA weiterhin am Puls der Zeit bleiben und in der Lage sein, sich frühzeitig neuen Entwicklungen zu widmen und sich für datenschutzfreundliche Lösungen einzusetzen. Als Vorsitzender des GPA Reference Panels möchte ich dazu beizutragen, diese Ziele zu erreichen.

Querverweise:

3.3.1 Allgemeiner Bericht

3.4 Weitere internationale Gremien

3.4.1 G7

Die britische Datenschutzbeauftragte hat im Berichtsjahr die Datenschutzbehörden der G7-Staaten zu einem Gespräch am Runden Tisch eingeladen. Hintergrund dieser Einladung war der Vorsitz des Vereinigten Königreichs beim G7-Gipfel 2021. In dem Gespräch wurden Möglichkeiten für eine fortgesetzte engere Zusammenarbeit in dieser Gruppe erörtert.

Weltweit werden immer mehr Daten generiert, gesammelt und genutzt. In einer zunehmenden globalisierten und digitalisierten Welt fließen die Daten über die Grenzen der Länder und Kontinente hinweg. Hier müssen die Datenschutzaufsichtsbehörden international zusammenarbeiten, um den Datenschutz zu wahren. Wenn die Daten von deutschen und europäischen Bürgerinnen und Bürgern den jeweiligen Rechtsraum verlassen, dürfen sie nicht schutzlos sein. Um diesen Schutz zu verbessern, ist eine Vertiefung und Erweiterung der internationalen Zusammenarbeit unerlässlich.

Im September 2021 trafen sich die Behörden für den Datenschutz und den Schutz der Privatsphäre der G7-Staaten auf Einladung der damaligen britischen Datenschutzbeauftragten, Frau Elizabeth Denham, erstmalig zu einem gemeinsamen Gespräch am Runden Tisch. An diesem neuen internationalen Format nahmen auch das Weltwirtschaftsforum und die OECD teil. Das Treffen stand in Zusammenhang mit dem britischen Vorsitz des G7-Gipfels 2021 der Staats- und Regierungschefs.

Im April 2021 haben die Digital und Technologieminister der G7-Staaten einen Fahrplan für die Zusammenarbeit zur Förderung des freien und vertrauenswürdigen Datenflusses (Data Free Flow with Trust) beschlossen. Hier sollen Gemeinsamkeiten bei den Regulierungen des internationalen Datentransfers identifiziert sowie gute Regulierungspraktiken und Kooperationsmöglichkeiten ausgetauscht werden. Der Runde Tisch war ein Beitrag der Datenschutzbehörden zu diesem wichtigen Thema.

Die Erklärung der G7-Digital und Technologieminister zum freien und vertrauenswürdigen Datenfluss 2021 basiert auf

- der Erklärung der Staats- und Regierungschefs der G20-Staaten 2019 in Osaka (Osaka Leader´ Declaration),
- der Ministererklärung zum Handel und der digitalen Wirtschaft (2019 G20 Ministerial Statement on Trade and Digital Economy)

- sowie der Erklärung der Staats- und Regierungschefs der G20 Staaten in Riad (2020 G20 Leaders' Riyadh Declaration).

Der freie und vertrauenswürdige Datenfluss ist seit mehreren Jahren ein Thema in den Abschlusserklärungen der G7 und G20 Treffen. Dies zeigt noch einmal dessen wachsende Bedeutung.

Erörtert wurden am Runden Tisch Möglichkeiten für eine engere Zusammenarbeit der Datenschutzbehörden der G7-Staaten. In einem gemeinsamen Kommuniqué[13] wurden Kernthesen zu folgenden Themen festgehalten:

- Datenschutz und Wettbewerb
- Online Tracking
- Künstliche Intelligenz
- Neugestaltung von Abhilfemöglichkeiten für das digitale Zeitalter
- pandemiegetriebene technologische Innovationen
- „Government Access" und die
- Entwicklung eines Rahmens für den Internationalen Datentransfer.

Zu den einzelnen Bereichen wurde ein fortgesetzter Dialog zwischen den Behörden und ein Roundtable im Jahre 2022 vereinbart, den ich anlässlich der deutschen G7-Präsidentschaft organisieren möchte. Angesichts der Bedeutung der Digitalisierung bitte ich die Bundesregierung im Rahmen ihrer G7-Präsidentschaft, den Dialog mit den Datenschutzbehörden im G7-Format fortzuführen.

Querverweise:

3.4.3 Datenschutzgrundsätze für den staatlichen Zugriff auf personenbezogene Daten im internationalen Bereich, 4.2 Künstliche Intelligenz – Regulierung als gesamtgesellschaftliche Aufgabe, 6.3 Kooperation zwischen Kartell- und Datenschutzaufsichtsbehörden

3.4.2 Berlin Group

Seit 1983 besteht die Internationale Arbeitsgruppe zum Datenschutz in der Technologie, die unabhängige Expertinnen und Experten versammelt. Im März 2021 habe ich den Vorsitz von der Berliner Datenschutzbeauftragten übernommen.

Im März des Berichtsjahres habe ich den Vorsitz der internationalen Arbeitsgruppe zu Datenschutz in Technologie „International Working Group Data Protection in Technology" (IWGDPT) dauerhaft übernommen. Da die Gruppe 1983 auf Veranlassung des damaligen Berliner Datenschutzbeauftragten gegründet worden war und zunächst häufig in Berlin tagte, wurde die IWGDPT auch als „Berlin Group" bekannt.

Das Besondere der IWGDPT ist – neben ihrer langen Tradition – ihre Unabhängigkeit und Diversität. Hier wirken neben Angehörigen von Datenschutzbehörden auch Expertinnen und Experten aus den Bereichen Wissenschaft und Forschung, von Nichtregierungsorganisationen oder datenschutzbezogenen Denkfabriken („Think-Tanks"). Auch Behörden oder Einrichtungen, die mit der Regulierung datenschutzrelevanter Bereiche oder Dienstleistungen befasst sind, gehören dazu.

Die IWGDPT ist zwar von der GPA unabhängig und bestimmt selbst über ihre thematischen Schwerpunkte und ihre Ausrichtung. Gleichwohl steht sie in einem näheren Verhältnis zur GPA. So berichtet der Vorsitz der IWGDPT im Plenum der GPA-Jahreskonferenz regelmäßig über die Tätigkeiten der Gruppe.

Die IWGDPT konnte ihre Arbeiten im Berichtszeitraum mit Einschränkungen auch während der Corona-Pandemie fortsetzen. So hat die Gruppe ein Arbeitspapier zu sensorischen Netzwerken finalisiert, an einem Dokument zu sprachgesteuerten Geräten" weitergearbeitet und mit neuen Arbeiten zu den Themen intelligente Stadt („Smart Cities") sowie Gesichtserkennungstechnologie begonnen. In meiner neuen Funktion als Vorsitzender der IWGDPT werde ich mich sehr dafür einsetzen, die Intensität des Dialogs und die hohe Qualität der Arbeitspapiere und Empfehlungen der IWGDPT fortzuführen.

Querverweise:

3.3.1 Global Privacy Assembly

3.4.3 Datenschutzgrundsätze für den staatlichen Zugriff auf personenbezogene Daten im internationalen Bereich

In verschiedenen internationalen Foren sollen gemeinsame Datenschutzprinzipien für den Zugriff von Strafverfolgungs- und Sicherheitsbehörden auf personenbezogene Daten privater Stellen vereinbart werden. Solche gemeinsamen Grundsätze für „Government Access" können einen wichtigen Beitrag für eine rechtlich befriedigende Gestaltung des grenzüberschreitenden Datenaustauschs leisten und das Datenschutzniveau auch außerhalb der EU anheben.

13 Kurzmeldung des BfDI vom 14. September 2021 zu finden unter: www.bfdi.bund.de/kurzmeldungen

Der staatliche Zugriff auf personenbezogene Daten, die durch private Stellen verarbeitet werden, stand im Jahr 2020 im Mittelpunkt verschiedener datenschutzrechtlicher Initiativen.

Unter dem Stichwort „Government Access“ wurde vor allem der Zugriff von Strafverfolgungs- und Sicherheitsbehörden im Kontext grenzüberschreitender Datenverarbeitungen in mehreren internationalen Foren behandelt. Das gilt insbesondere für die Arbeiten im Rahmen der Global Privacy Assembly (GPA) und der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD). Darauf aufbauend haben auch die Datenschutzaufsichtsbehörden der G7-Staaten das Thema „Government Access“ diskutiert. Hintergrund sind die Bemühungen, auf internationaler Ebene gemeinsame Datenschutzprinzipien für „Government Access“ zu vereinbaren. Anlass dieser Bemühungen ist auch die Schrems II-Rechtsprechung des EuGH. Das Gericht stellt für die Bewertung des Datenschutzniveaus in Drittländern maßgeblich auf den Schutz personenbezogener Daten vor Zugriffen durch Sicherheitsbehörden ab.

Der Zugriff der Sicherheitsbehörden auf Daten privater Stellen ist ein sensibles Thema. Berührt werden Fragen der nationalen Sicherheit der einzelnen Staaten. Zugleich zeigt sich die Bedeutung des freien Datenverkehrs für die weltweite digitale Wirtschaft. Die Entwicklungen der letzten Jahre haben deutlich gezeigt, dass fehlende oder unzureichende internationale Datenschutzgarantien nicht allein ein Risiko für den Schutz personenbezogener Daten sind. Sie haben auch erhebliche wirtschaftliche Auswirkungen.

Für das europäische Datenschutzrecht sind diese Initiativen eine Herausforderung. Es ist einerseits erstrebenswert, gemeinsame internationale Datenschutzgrundsätze zu schaffen. Andererseits gibt das europäische Datenschutzrecht einen verbindlichen rechtlichen Rahmen für die Übermittlung personenbezogener Daten in Drittstaaten vor. Daraus ergibt sich für meine Arbeit ein Spannungsfeld: Die Vereinbarung internationaler Prinzipien kann zwar einen wichtigen Beitrag leisten, grenzüberschreitenden Datenaustausch nachhaltig zu ermöglichen und das Datenschutzniveau außerhalb der EU anzuheben. Europäische Datenschutzstandards dürfen dabei jedoch nicht unterschritten werden.

Die GPA hat auf ihrer Jahreskonferenz im Oktober 2021 eine Entschließung zur Stärkung datenschutzrechtlicher Grundsätze für „Government Access“ verabschiedet. An der Ausarbeitung der „Resolution on government access to data, privacy and the rule of law: principles for governmental access to personal data held by the private sector for national security and public safety purposes“ habe ich aktiv mitgewirkt. Im Rahmen der OECD werden sog. „Principles on government access to personal data held by the private sector“ verhandelt, die bislang jedoch noch nicht beschlossen werden konnten.

Ich begrüße es, dass die GPA die gemeinsamen Datenschutzprinzipien im Oktober angenommen hat. Zugleich hoffe ich, dass die Arbeiten innerhalb der OECD im Sinne des Datenschutzes vorangebracht werden können und dabei die von der GPA gefundenen Ergebnisse berücksichtigt werden.

Auf Ebene der G7 habe ich mich für einen weiteren intensiven Meinungsaustausch eingesetzt. Dadurch sollen die von der GPA entwickelten Grundsätze sowie die OECD-Initiative datenschutzpolitisch unterstützt werden.

Querverweise:

3.2.2.1 Taskforce Supplementary Measures/Umsetzung Schrems II, 3.3.1 Allgemeiner Bericht, 3.4.1 G7

4 Schwerpunktthemen

4.1 Corona

4.1.1 Corona-Warn-App

Seit dem 16. Juni 2020 ermöglicht die Corona-Warn-App (CWA) der Bundesregierung ihren Nutzenden, sich gegenseitig schnell und datenschutzfreundlich über Risikobegegnungen zu warnen. Neben der Kontaktnachverfolgung sind seitdem weitere Funktionen hinzugekommen. Beim Datenschutz verhindert die Abhängigkeit von den Betriebssystemherstellern Apple und Google weitere Verbesserungen. Ob die CWA ihre Zwecke erfüllt, hat das Robert Koch-Institut (RKI) evaluiert.

Ich habe dem RKI auch nach dem 16. Juni 2020 bei der Einführung der neuen Funktionen, unter anderem der Kontaktverfolgung beim Besuch von Lokalitäten (Eventregistrierung) und der Integration der Test- und Impfzertifikate in die CWA, beratend zur Seite gestanden. Darüber hinaus habe ich die datenschutzrechtliche Aufsicht wahrgenommen und Beschwerden aus der Bevölkerung bearbeitet. Besonders viele Beschwerden bezogen sich auf fehlende Möglichkeiten, die CWA z. B. auch direkt vom RKI und nicht nur über die Plattformen der Firmen Apple und Google beziehen zu können sowie die „Zwangsinstallation" des für die Abstandsmessung nötigen Google/Apple Exposure Notifications (GAEN), das jedoch Teil der Betriebssysteme ist und deshalb nicht in meinen rechtlichen Zuständigkeitsbereich fällt.

Datenschutz erleichtert akzeptierte und bedarfsgerechte Lösungen

Mit annähernd 39 Millionen Downloads bis Ende 2021 ist die CWA europaweit die größte und eine der am meisten akzeptierten Apps dieser Art. Am Vertrauen, dass die CWA genießt, hat der Datenschutz einen wichtigen Anteil. Er verhindert keinesfalls den Erfolg, sondern ist im Gegenteil ein Erfolgsfaktor.

Die CWA belegt auch, dass datenschutzfreundliche Lösungen nicht zulasten der Funktion gehen müssen: Keine geeignete geplante Funktion musste aus Gründen des Datenschutzes eingeschränkt werden oder gar entfallen.

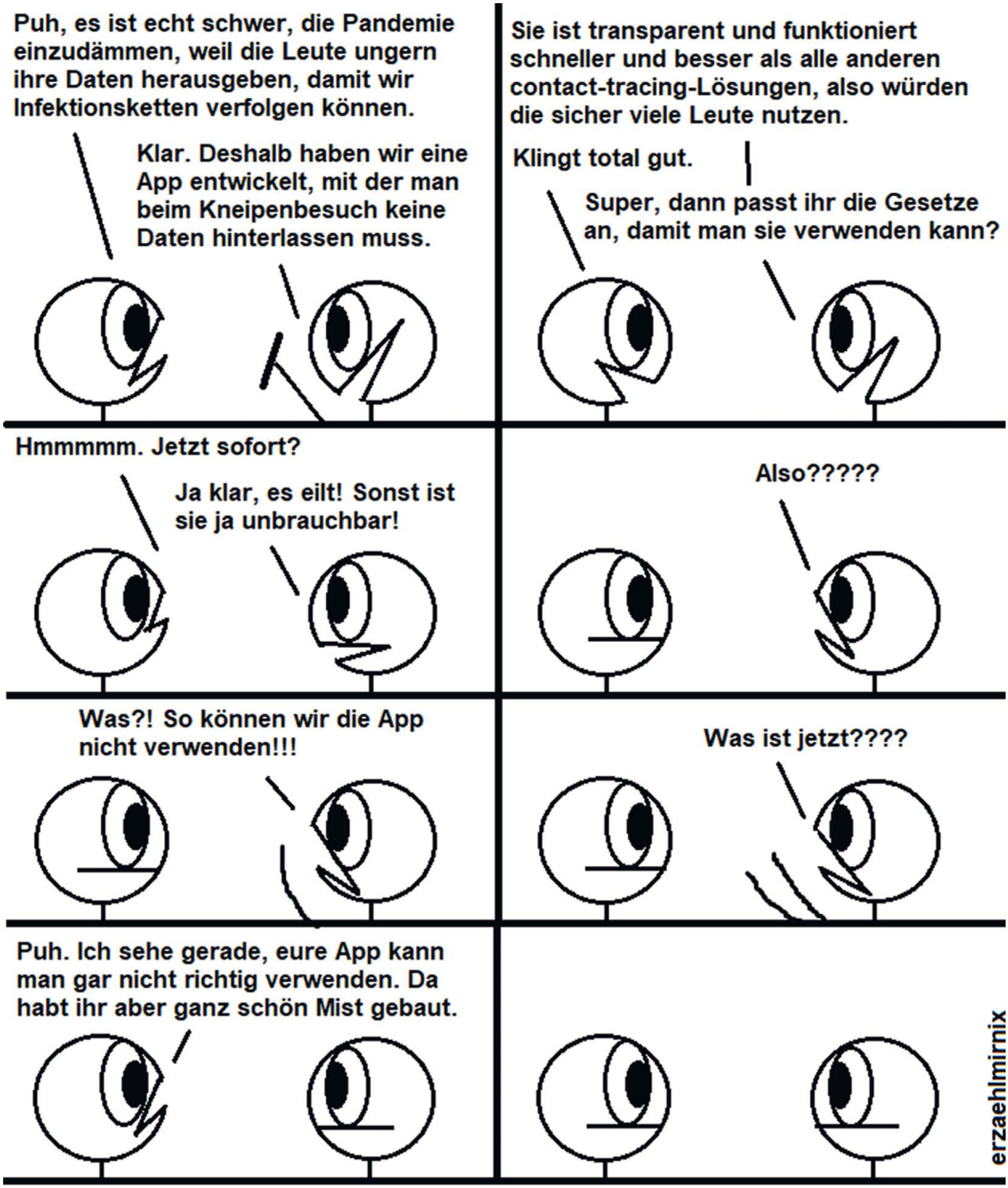
Datenschutz braucht „digitale Souveränität"

Ohne das GAEN der Betriebssystemhersteller Apple und Google wäre die CWA im vergangenen Jahr nicht realisierbar gewesen. Die allgemeine Kritik an der Verwendung des GAEN und insbesondere der Vorwurf eines unberechtigten Abgreifens von Daten wurden zunächst nicht durch nachvollziehbare Belege behauptet. Am 12. April 2021 jedoch veröffentlichte das Unternehmen „appcensus" eine Sicherheitslücke in Googles API for Exposure Notifications. Danach konnten installierte Apps auf die Daten des GAEN zugreifen. Zwar sicherte Google mir in der Folge zu, die Lücke geschlossen zu haben; ob die Lücke ausgenutzt wurde, ist aber nicht bekannt.

Leider blieb das GAEN nicht die einzige Funktion der beiden Betriebssystemhersteller, die in der CWA verwendet wird. Anlässlich der Datenerhebungen zur Evaluierung der CWA wurde die Integritätsprüfung der Firmen Apple und Google in die CWA integriert. Welche Daten dabei an die beiden Betriebssystemhersteller zur Prüfung gesendet werden, ist nicht bekannt. Geplant ist auch, die aufgrund eines Smartphonewechsels durchaus wünschenswerte Funktion des Exports und anschließenden Imports der CWA-Nutzerdaten mit Hilfe betriebssystemeigener Funktionen zu realisieren. Apple und Google könnten dann Zugriff auf die Daten der CWA nehmen.

Die Gründe für den Rückgriff auf Dienste der Betriebssystemhersteller Apple und Google reichten dabei von „zwingend notwendig" (GAEN) über „im Sinne der Validierung notwendig und der Nutzerregistrierung vorzuziehen" (bei der Evaluierung) bis zum „nachvollziehbaren Nutzerwunsch" (Daten-Im- und -Export).

Ich habe dem RKI in diversen Stellungnahmen stets deutlich gemacht, wenn möglich auf die Dienste der Betriebssystemhersteller zu verzichten und Alternativen vorgeschlagen. Das dies bislang auf keinerlei Resonanz gestoßen ist, bleibt aus meiner Sicht das größte Manko beim Datenschutz der CWA. Ich halte es für geboten, die Folge- und Weiterentwicklung der CWA so weit wie möglich unabhängig von den Betriebssystemherstellern Apple und Google zu machen, um die fehlende digitale Souveränität in der EU nicht noch weiter zu zementieren.



Erfüllt die CWA ihre Zwecke?

Das RKI legte bereits zum Start der CWA fest, dass deren Zwecke zu evaluieren sind. Dieser Aufgabe kam das RKI mit zwei Berichten im April und September 2021 nach. Danach sehe ich durchaus Verbesserungspotentiale für künftige Entwicklungen.

Damit ein PCR-Testergebnis auf das SARS-Cov-2 Virus schnell und direkt in die CWA gelangt, muss der oder die Nutzende den Test mit einem QR-Code registrieren (QR-Code-Verfahren). Außerdem muss das Testlabor diesen QR-Code verarbeiten können. Auch im Jahr 2021 war dies nicht bei allen Laboren der Fall. Die Nutzenden mussten dann telefonisch eine „tele-TAN“ anfragen um ihr positives Testergebnis zu teilen. Dieses aufwändigere und aus Sicht des Datenschutzes eher unerwünschte Verfahren (die Nutzenden müssen ihre Rufnummer hinterlegen) vermindert die Teilungsquote der positi

ven Testergebnisse. Ob das „tele-TAN“-Verfahren auch künftig nötig sein wird und welche Maßnahmen geplant sind, um dieses obsolet zu machen, hat das RKI bislang nicht evaluiert.

Das QR-Code-Verfahren hat sich in der Praxis gut bewährt: Laut RKI erhielten rund drei Viertel derjenigen, die diese Verfahren nutzten, ihr Ergebnis innerhalb von 24 Stunden. In den allermeisten Fällen ist damit die Voraussetzung erfüllt, die Testergebnisse rechtzeitig zu teilen.

Ein Zweck der CWA besteht darin, andere Nutzende aufgrund einer Begegnung mit einer infizierten Person zu warnen. In diesen Fällen zeigt die CWA der Empfangenden eine „rote Kachel“. Das RKI erklärte laut Evaluierungsbericht, dass „die überwiegende Zahl kritischer Kontakte von der Corona-Warn-App richtig erkannt werde“.

Die Erhebungen des RKI bei den Nutzenden der CWA bestätigen diese These zumindest teilweise: Nutzende, die aufgrund einer „roten Kachel“ der CWA einen SARS-CoV-2 Test machten, hatten häufiger ein positives Testergebnis als der Schnitt aller Getesteten.

Ich vermisse im Evaluationsbericht Erkenntnisse über die Möglichkeiten und Grenzen der Kontaktnachverfolgung mit Hilfe der CWA. Sollte die Kontaktnachverfolgung aus epidemiologischer Sicht auch bei künftigen Pandemien eine wichtige Rolle spielen, wäre dies dringend nachzuholen, auch um die Treffsicherheit der Warnungen weiter zu erhöhen

Zusammenfassend ist die CWA aus meiner Sicht im internationalen Vergleich und national zu einer erfolgreichen Referenz bei der Bekämpfung der Pandemie mit Smartphone-Apps geworden. Mein Fazit fällt daher positiv aus, auch weil – nach anfänglichem Zögern – weitere nützliche Funktionen wie die Eventregistrierung sowie der Impf- und Testnachweis mit der CWA hinzugekommen sind.

Dennoch sehe ich auch Grenzen beim Einsatz und der Wirkung solcher Apps. Eine Evaluierung sollte Unzulänglichkeiten und Verbesserungsmöglichkeiten ebenso enthalten wie die mögliche Rolle einer CWA in einem Gesamtkonzept zur Pandemiebekämpfung, bei der sie mit anderen Maßnahmen zusammenwirkt. Vor allem hier scheint noch ein großes Verbesserungspotenzial vorhanden zu sein.

4.1.2 SORMAS

Um endlich von Papier und Fax zu einer effizienten und datenschutzkonformen digitalen Kontaktnachverfolgung in den Gesundheitsämtern zu kommen, war eine intensive Begleitung des Projektes erforderlich.

Bei der Software SORMAS handelt es sich um ein Kontaktpersonenmanagement im Rahmen der SARS-CoV-2-Pandemie, über die ich in meinem 29. Tätigkeitsbericht (Nr. 4.1.3) berichtet habe. Die Gesundheitsämter sollen durch die Software bei der Identifizierung und Überwachung von Kontaktpersonen unterstützt werden, indem Symptomangaben von Kontaktpersonen ohne telefonische Rückfragen erfasst und Daten zu Fallmeldungen mit anderen Gesundheitsämtern ausgetauscht werden können. Neben dem digitalen Empfang von Labormeldungen sollen darüber hinaus auch Falldaten digital an die Landesbehörden gemeldet werden. Bereits auf der Ministerpräsidentenkonferenz am 16. November 2020 wurde der bundesweite Einsatz von SORMAS in den Gesundheitsämtern beschlossen.

In Abstimmung mit den beteiligten Datenschutzaufsichtsbehörden der Länder habe ich nach gemeinsamer Erörterung der eingereichten Unterlagen im Januar 2021 einem Betrieb von SORMAS-X in den Gesundheitsämtern unter Vorbehalt zugestimmt. Voraussetzung dafür war eine schriftliche Zusicherung, dass die Unterlagen im laufenden Betrieb nachgebessert und vervollständigt werden. Das sollte ermöglichen, im Zuge der Risikobewertung Risiken zu erkennen und nötige technische und organisatorische Maßnahmen zu ergreifen. Dieses sollte schnellstmöglich unter Einsatz hinreichender Ressourcen erfolgen. Die Datenschutzfolgeabschätzung wurde nur als Entwurf vorgelegt. Nötig war auch ein Kryptographiekonzept. Die Beratung wurde ab Juli 2021 noch einmal intensiviert und eine Arbeitsgruppe unter meiner Beteiligung und der mehrerer Landesdatenschutzbeauftragten eingerichtet. Hintergrund war, dass die Fortschritte seitens des Helmholtz-Zentrum für Infektionsforschung (HZI) über einen längeren Zeitraum nicht den Erwartungen entsprachen, die die Landesbeauftragten und ich an ein solches Projekt gestellt haben. So wurden Fristen zur Vorlage von Dokumenten, hinsichtlich derer noch erheblicher Beratungsbedarf besteht, wie beispielsweise das Löschkonzept, die Datenfeldertabelle sowie die Datenschutzfolgenabschätzung, mehrfach über mehrere Monate verschoben. Zum Ende des Berichtszeitraums hat sich die Zusammenarbeit des HZI mit den Datenschutzaufsichtsbehörden des Bundes und der Länder verbessert. Ich gehe davon aus, dass die Beratung dieses hochagilen Projektes im Laufe der ersten Jahreshälfte 2022 abgeschlossen werden kann.

4.1.3 Digitales COVID-Zertifikat der EU

Ursprünglich ging es um Reiseerleichterungen auf europäischer Ebene. Am Ende standen datenschutzfreundliche Nachweise der Covid-19-Zertifikate im Alltag.

Am 17. März 2021 hat die EU-Kommission einen Verordnungsentwurf zum Digital Green Certificate vorgelegt. Die EU-VO soll grenzüberschreitende Reiseerleichterungen für EU-Bürger und -Bürgerinnen während der Corona Pandemie innerhalb der EU ermöglichen.

Der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDSB) haben hierzu am 31. März 2021 eine gemeinsame Stellungnahme (Joint Opinion) verabschiedet. Demnach sollte jede auf nationaler Ebene oder auf EU-Ebene erlassene Maßnahme, die die Verarbeitung personenbezogener Daten beinhaltet, im Einklang mit den allgemeinen Grundsätzen der Wirksamkeit, Notwendigkeit und Verhältnismäßigkeit stehen. Außerdem sollten die Datenverarbeitungen auf einer angemessenen Rechtsgrundlage in den Mitgliedstaaten basieren. Gleichzeitig ersuchten der EDSA und der EDSB die EU-Kommission klarzustellen, dass die Mitgliedstaaten alle drei Arten von Zertifikaten (geimpft, genesen oder getestet) akzeptieren sollten. Sollten sie dies nicht tun, läge eine Diskriminierung aufgrund von Gesundheitsdaten und somit eine Verletzung der Grundrechte vor.

Die Verordnung über das digitale COVID-Zertifikat der EU ist am 1. Juli 2021 in Kraft getreten. Drei Zertifikate werden definiert: Impfung, Test und Genesen. Die Mitgliedstaaten müssen die Zertifikate in Papierform und digital anbieten. Die Verwendung der Zertifikate ist freiwillig. Sie sind diskriminierungsfrei, da sie keine Reisebeschränkungen in Europa schaffen, sondern vielmehr den grenzüberschreitenden Verkehr für die Inhaber erleichtern, indem gegebenenfalls auf weitere Maßnahmen der einzelnen Mitgliedstaaten während der Corona Pandemie (z. B. Quarantäneregelungen) verzichtet werden kann. Es findet weder Tracking (zeitgleiche Nachverfolgung) noch Tracing (nachträgliche Nachverfolgung) statt. Die Zertifikate dienen der Authentifizierung sowie der Feststellung des Status der Inhaber beim Grenzübertritt. Personenbezogene Daten werden von den kontrollierenden Stellen nicht gespeichert.

Die Verordnung und damit die Zertifikate sind zeitli ch befristet. Sobald die WHO die Corona-Pandemie für beendet erklären wird, setzt die EU-Kommission die Verordnung mit einem legislativen Akt außer Kraft. Die Verordnung selbst erlaubt die Nutzung der Zertifikate lediglich zu einem Zweck – die Erleichterung der Reisefreiheit. Sie eröffnet den Mitgliedstaaten zusätzlich die Möglichkeit einer weiteren Nutzung (z. B. Zugang zu Veranstaltungen, öffentlichen Einrichtungen etc.). Davon hat der deutsche Gesetzgeber Gebrauch gemacht und ebenfalls zeitlich befristete Regelungen im Infektionsschutzgesetz getroffen, beispielsweise für den Zugang

von Einrichtungen des Gesundheits- und Sozialwesens, des Nah- und Fernverkehrs oder im Hotel- und Gaststättenbereich.

In Deutschland werden die Zertifikate im Auftrag des Robert Koch-Instituts (RKI) technisch generiert. Dabei werden keine Daten gespeichert. In der CovPassApp und der Corona-Warn-App können die Zertifikate angezeigt werden. Eine Kontrolle der Gültigkeit der Nachweise kann mit der CovPassCheck-App erfolgen. Die Entwicklung dieser Anwendungen habe ich über alle Programmversionen hinweg datenschutzrechtlich begleitet und neben dem BMG auch das RKI als Verantwortlicher für die Apps intensiv beraten.

Querverweise:

4.1.1 Corona-Warn-App

4.1.4 Coronamelde-Verordnung

Die Coronamelde-Verordnung ist komplexer, als sie sein müsste. Ein Weniger an Daten hätte eine schnellere Verarbeitung ermöglicht.

Am 29. Juni 2021 – mit Frist zur Stellungnahme bis zum 1. Juli 2021 – erreichte mich erstmals der Entwurf des Bundesgesundheitsministeriums (BMG) einer „Verordnung über die Erweiterung der Meldepflicht nach § 6 Abs. 1 Satz 1 Nummer 1 des Infektionsschutzgesetzes (IfSG) auf Hospitalisierungen in Bezug auf die Coronavirus-Krankheit-2019“. Hinter dem sperrigen Titel verbirgt sich eine zusätzliche Pflicht für Krankenhäuser und Gesundheitsämter. Ziel ist die Ermittlung der Hospitalisierungsinzidenz als Orientierungswert für Schutzmaßnahmen. Krankenhäuser müssen danach die Aufnahme von Patienten namentlich an das Gesundheitsamt melden, auch wenn die Corona-Infektion dieser Person dort schon bekannt ist. In der Folge müssen die Gesundheitsämter die Meldung prüfen, zuordnen und dann im üblichen Verfahren unter einer Kennnummer an die Landesbehörde melden, die die Meldung an das Robert Koch-Institut (RKI) weiterleitet. Ich hatte erhebliche Zweifel, ob die Voraussetzungen der Ermächtigungsgrundlage (§ 15 Abs. 1 IfSG) erfüllt sind. Demnach kann das BMG die Meldepflicht nach § 6 IfSG erweitern, soweit die epidemische Lage dies erfordert. Warum hier eine zusätzliche Mitteilung an das Gesundheitsamt nötig sein sollte, war aber nicht ersichtlich. Stattdessen ging es laut Begründung um die Anzahl der Krankenhausaufnahmen – also um rein statistische Angaben. Relevant sind diese Angaben wohl weniger für die Arbeit im Gesundheitsamt, sondern für die Bewertung der pandemischen Lage durch das RKI. Aus Gründen der Datenminimierung wäre es angezeigt gewesen, dass die Krankenhäuser die Aufnahme von Patienten statistisch – also anonym, ohne persönliche Angaben – direkt an das RKI melden. Daher hatte ich dem BMG in meiner Stellungnahme empfohlen, sich am inzwischen bewährten Verfahren zur Meldung der Intensivpatienten zu orientieren. Dies begnügt sich mit der reinen Anzahl und wenigen weiteren Angaben. Dennoch wurde das umständliche Verfahren beibehalten und es verwundert daher nicht, dass immer wieder über Meldeverzug berichtet wird.

4.1.5 Die Bundesnotbremse und die Ausnahmeverordnung

Die Pandemiebekämpfung macht Gesundheitsdaten quasi zur Eintrittskarte. Dabei mildern digitale Lösungen die Risiken nur teilweise. Klare Maßgaben zur Vertraulichkeit wären erforderlich gewesen. Zulässig sind solche Nachweispflichten nur soweit und solange, wie sie zur Gefahrenabwehr erforderlich sind.

Im letzten Tätigkeitsbericht habe ich über die durch Corona bedingten Änderungen des Infektionsschutzgesetzes durch das erste, zweite und dritte Pandemie-Schutz-Gesetz berichtet (29. TB, 4.1.4). Im weiteren Verlauf der Pandemie gab es neue Gesetzesänderungen und Verordnungen, bedauerlicherweise erneut mit unnötig kurzen Fristen für Beratung und Prüfung.

Bundesnotbremse

Von der sogenannten „Bundesnotbremse“ im Entwurf des „Vierten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite“, einem Gesetzentwurf der Koalitionsfraktionen (BT-Drs. 19/28444), erfuhr ich erst am 13. April 2021 über die Tagesordnung des Ausschusses für Gesundheit. Im Vorfeld wurde ich nicht beteiligt. Die darin enthaltenen Schutzmaßnahmen selbst, wie Kontakteinschränkungen und Betriebsuntersagungen, sind dabei ohne Datenschutzrelevanz. Allerdings war in § 28c des Gesetzentwurfs auch eine Verordnungsermächtigung enthalten, die Erleichterungen oder Ausnahmen für Immunisierte und negativ Getestete umfasste. Der damit verbundene Nachweis und dessen Kenntnisnahme stellen eine Verarbeitung von Gesundheitsdaten dar und sind nach Art. 9 DSGVO nur unter besonderen Voraussetzungen und mit besonderen Maßgaben zum Schutz der Betroffenen zulässig. Dies wird im Entwurf und seiner Begründung jedoch nicht erwähnt. Das Gesetz wurde am 22. April 2021 veröffentlicht (BGBl. 2021 I, S. 802).

Ausnahme bei Nachweis

Aufgrund der Verordnungsermächtigung hat die Bundesregierung am 4. Mai 2021 den Entwurf einer „Verordnung zur Regelung von Erleichterungen und Ausnahmen von Schutzmaßnahmen zur Verhinderung der Verbreitung von COVID-19 (COVID-19-Schutzmaßnah

men-Ausnahmenverordnung – SchAusnahmV)“ (BT-Drs. 19/29257) vorgelegt, der mir wiederum erst durch die Tagesordnung des Ausschusses für Gesundheit bekannt wurde. Dass ich nicht vorher beteiligt wurde, verstößt gegen § 21 Abs. 1 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO). Die am 8. Mai 2021 ausgefertigte Verordnung (BAnz AT 08. Mai 2021 V1) enthält Vorgaben, wie der Nachweis der Immunisierung oder der negativen Testung beschaffen sein muss und welche Voraussetzungen erfüllt sein müssen. Dann nennt die Verordnung diejenigen Regelungen der „Bundesnotbremse“ in § 28b IfSG, die für Personen nicht gelten, die diesen Nachweis erbringen können. Mit dieser Verordnung wurden persönliche Gesundheitsinformationen zur Zugangsvoraussetzung und Geschäftsinhaber, Hoteliers, Restaurantinhaber und Vereine zu – mehr oder weniger gewissenhaften – Kontrolleuren. Auch wenn datenschutzfreundlich mittels CovPassCheckApp kontrolliert wird, hat der Nachweis zur Folge, dass die Person, der gegenüber der Nachweis geführt wird, Name und Geburtsdatum erfährt. Daher hätte ich hier eine flankierende Maßgabe zur Wahrung der Vertraulichkeit durch die Kontrollierenden erwartet.

Nachweispflicht als Schutzmaßnahme

Mit dem Aufbauhilfegesetz 2021 vom 10. September 2021 (BGBl 2021, S. 4147) – Art. 12 – wurde dann eine Verpflichtung zur Vorlage eines Impf-, Genesenen- oder Testnachweises zusätzlich als unmittelbare Schutzmaßnahme in den Katalog möglicher Maßnahmen in § 28a IfSG aufgenommen. Wieder fehlte in der Begründung zum Gesetzentwurf ein Bezug darauf, dass es sich bei den Nachweisen um Gesundheitsdaten handelt, die nach Art. 9 DSGVO einem besonderen Schutz unterliegen. Die Nachweispflicht führt zu Situationen, die sowohl von nachweisenden als auch von den kontrollierenden Personen als unangenehm wahrgenommen werden. Dieser Eingriff in das Recht auf informationelle Selbstbestimmung wurde trotz meiner Hinweise nicht durch Maßgaben oder Erläuterungen flankiert. Dies blieb demnach den Ländern überlassen. Es wurde nicht einmal ein Hinweis darauf aufgenommen, dass eine Anordnung dieser Maßnahmen besonders geprüft werden müsste und diese Daten vertraulich zu behandeln seien. Nach Art. 9 Abs. 2 DSGVO ist die Verarbeitung von Gesundheitsdaten nur unter bestimmten Voraussetzungen ausnahmsweise möglich. Dass die Pandemielage eine solche Ausnahmesituation darstellt, hätte transparenter gemacht werden sollen. Ich wies das BMG daher darauf hin, dass die Maßnahmen zur Pandemiebekämpfung fortlaufend zu überprüfen und gesetzliche Verpflichtungen zur Verarbeitung personenbezogener Daten so früh wie möglich wieder aufzuheben sind. In der Folge erreichten mich weitere Gesetzes- und Verordnungsentwürfe, bei denen mir die Ministerialverwaltung zur Prüfung und Stellungnahme meist nur ein kurzes Zeitfenster, teilweise nur Stunden, eingeräumt hat. Soweit ich innerhalb der kurzen Fristen datenschutzrechtliche Probleme erkennen konnte, habe ich diese geltend gemacht. Gleichwohl war und ist mir bewusst, dass unter den gegebenen Umständen eine umfassende Prüfung und Bewertung der Gesetzes- und Verordnungsentwürfe nicht möglich war. Umso mehr werde ich die weitere gesetzgeberische Entwicklung sowie die spätere Umsetzung in die Praxis beobachten. Mögliche gesetzgeberische Defizite dürften sich nicht zuletzt auch in einer erhöhten Anzahl an Beschwerden und Eingaben niederschlagen, aber auch in einer erhöhten Gefahr des Scheiterns bei gerichtlicher Überprüfung. Bereits im Berichtszeitraum hat die Zahl der bei mir zum Gesundheitsbereich eingegangenen Beschwerden und Eingaben ein neues Rekordhoch erreicht.

Querverweise:

4.1.3 Digitaler Impfnachweis

4.1.6 Coronavirus-Testverordnung

Auch für die Bürgerteststellen gilt: bei der Verarbeitung von Gesundheitsdaten bedarf es besonderer Sicherheiten – wie beispielsweise der beruflichen Schweigepflicht. Wenn also Nicht-Ärzte Aufgaben übernehmen sollen, sind alternative Vorgaben nötig.

Die „Verordnung zum Anspruch auf Testung in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 (Coronavirus-Testverordnung – TestV)“ wurde erstmals im Mai 2020 erlassen und danach – zeitweise im Monatstakt – geändert. Ich wurde erstmals im Januar 2021 in die Ressortabstimmung einbezogen. Die in der Folge vorgelegten Entwürfe für Änderungsverordnungen hatten unnötig extrem kurze Stellungnahmefristen, meist bis zum gleichen oder bis zum nächsten Tag, im Einzelfall bis zur nächsten Woche. Bei der Prüfung war für mich entscheidend, wer die Daten der getesteten Personen verarbeitet und welche Regeln für deren Speicherung und Übermittlung gelten.

Bei den frühen Fassungen gab es keinen Anlass zu Bedenken: Mit den Testungen waren zunächst neben dem Gesundheitsamt nur Arztpraxen und später auch Apotheken befasst, also Personen, die einer beruflichen Schweigepflicht unterliegen. Zudem sollte die Abrechnung gerade ohne Angaben zu den getesteten Personen auskommen. Zeitgleich mit Einführung der – für die Getesteten kostenfreien – Bürgertestung wurde der Kreis auf „weitere geeignete Dritte“ erweitert: Das Gesundheitsamt kann auch „weitere Anbieter, die eine ordnungsgemäße Durchführung, insbesondere nach einer Schulung nach § 12 Abs. 4, garantieren“, beauftra

gen. Da die Testanbieter neben Name und Adresse auch Gesundheitsdaten verarbeiten und eine positive Testung zudem die Pflicht zur Meldung ans Gesundheitsamt auslöst, hatte ich erwartet, dass die Landesbehörden bei der Umsetzung der Verordnung den Teststellen Vorgaben zu Datenschutz und Datensicherheit machen. Dies war jedoch nicht durchgehend der Fall. Der „insbesondere"-Zusatz erweckte offenbar den Eindruck, dass die Schulung das wesentliche Kriterium für eine zulässige Beauftragung ist. Jedenfalls entstanden in der Folge eine Vielzahl von Schnelltestzentren – in Zelten, Containern, leerstehenden Veranstaltungsräumen oder Ladenlokalen. Ob die Datenverarbeitung der jeweiligen Verantwortlichen im Einklang mit den Vorgaben der DSGVO für Gesundheitsdaten stand, war zuweilen zweifelhaft; es wurden verschiedene, auch größere Pannen bekannt. Erst mit der Änderungsverordnung vom 12. November 2021 wurde auf meinen Hinweis hin die Vorgabe aufgenommen, dass auch die weiteren Leistungserbringer zur Verschwiegenheit verpflichtet sein müssen.

Unklarheiten bedingte auch die – unverändert gebliebene – Pflicht, die Auftrags- und Leistungsdokumentation aufzubewahren. Für Ärztinnen und Ärzte entspricht diese Vorgabe der üblichen Praxis. Was sie allerdings für die „geeigneten Dritten" bedeutet und ob darin eine hinreichende Grundlage für die Speicherung von personenbezogenen Gesundheitsdaten lag, war zweifelhaft. Es führte außerdem zu Unsicherheit bei den Anwendern und Diskussionen bei den Datenschutzbehörden. Unter dem Eindruck bekannt gewordenen vermuteten Abrechnungsbetrugs enthielt die TestV in der Fassung vom Juni allerdings eine konkretisierende Aufzählung zur Dokumentation, um die Abrechnungsprüfung zu ermöglichen. Sogar das Testergebnis, ein besonders zu schützendes Gesundheitsdatum, sollte danach bis Ende 2024 aufbewahrt werden. Der Sinn erschließt sich nicht: Die Vergütung gibt es unabhängig vom Testergebnis und die Prüfung der zuverlässigen Meldung positiver Tests ist nur zeitnah zielführend. Eine Aufbewahrung wäre daher allenfalls für einige Monate erforderlich. Auf meine entsprechenden Hinweise wurde in der Fassung vom Oktober wenigstens eigens für die Testergebnisse eine verkürzte Frist bis Ende 2022 vorgesehen.

Nach Wegfall der Bürgertestung mussten berechtigte Personen ihren Anspruch auf eine kostenfreie Testung geltend machen und ein medizinisches Impfhindernis oder eine Schwangerschaft nachweisen. Hier stellte ich gegenüber dem BMG klar: Auch Schwangere haben Anspruch auf ein Attest, das nur die nötigen Angaben enthält; sie müssen nicht den Mutterpass mit einer Vielzahl von Befunden verwenden. Und ein Attest über eine medizinische Kontraindikation darf keine Diagnose enthalten, da diese hier nicht erheblich ist.

Querverweise:

4.1.8 Infektionsschutzgesetz

4.1.7 Das „EpiLage-Fortgeltungsgesetz"

Pandemische Pflichten und Eingriffe ohne Pandemielage? Die pandemiebedingten Regelungen wurden durch das EpiLage-Fortgeltungsgesetz entfristet und vom Bestehen der epidemischen Lage abgekoppelt. Dies gilt auch für die Übermittlung von Nachweisen aufgrund der Anmeldepflicht nach der Einreiseverordnung.

Am 2. Februar 2021 versandte das Bundesministerium für Gesundheit (BMG) den Entwurf einer Formulierungshilfe für den „Entwurf eines Gesetzes zur Fortgeltung der die epidemische Lage von nationaler Tragweite betreffenden Regelungen – (EpiLage-Fortgeltungsgesetz)" mit der wiederholt extrem kurzen Frist zur Stellungnahme bis zum 3. Februar 2021 16.00 Uhr. Die Formulierungshilfe beinhaltete den Erhalt der Regelungen, die aufgrund der Feststellung der epidemischen Lage von nationaler Tragweite erlassen wurden und die überwiegend mit deren Aufhebung oder aber spätestens zum 31. März 2021 außer Kraft treten würden, über das Ende der epidemischen Lage hinaus. Die epidemische Lage selbst sollte danach jeweils befristet gelten und eines Verlängerungsbeschlusses bedürfen.

Diese nun beabsichtigte zeitliche Begrenzung der epidemischen Lage ermöglichte die verfassungsrechtlich gebotene erneute Prüfung und Befassung mit den pandemiebedingten Regelungen durch den Deutschen Bundestag, was auch aus meiner Sicht zu begrüßen ist. Für verschiedene Verordnungsermächtigungen sollte die bislang festgelegte zusätzliche Befristung dagegen wegfallen, so dass sie automatisch ebenso lange wie die Feststellung der epidemischen Lage gelten würden. Dies betraf auch die Coronavirus-Einreiseverordnung. Nach der mehrfach geänderten Verordnung gab es zu dieser Zeit eine Anmeldepflicht für Einreisende unabhängig vom genutzten Verkehrsmittel. Verschiedene Angaben zur Person und zum Aufenthaltsort waren dem Gesundheitsamt zu übermitteln. Allerdings ist es denkbar, dass diese Pflicht in bestimmten Konstellationen keinen substanziellen Beitrag zur Pandemiebekämpfung mehr leisten kann, auch wenn die Feststellung der epidemischen Lage weiter besteht oder verlängert wird. Ich machte daher geltend, dass nur die Befristung der Verordnung unabhängig von der epidemischen Lage eine regelmäßige Überprüfung gewährleistet, ob die Datenübermittlungspflichten erforderlich sind und den Datenschutzvorgaben entsprechen.

Eine überarbeitete Fassung der Formulierungshilfe wurde am Samstag, den 6. Februar 2021 am frühen Nachmit

tag, übersandt mit Frist zur Stellungnahme bis Sonntag, den 7. Februar 2021. Sollte dann keine Rückmeldung vorliegen, gehe das BMG von einer Zustimmung aus, hieß es bemerkenswerterweise weiter. Ein solches Verfahren mit kürzesten Fristen unter Einbeziehung des Wochenendes entbehrt jeglicher Grundlage und macht mir meine Aufgabe zur Beratung von Bundesregierung und Bundestag unnötig schwer. Eine solche Vorgehensweise lässt sich auch mit den Regelungen der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) nicht in Einklang bringen. Dieses Verfahren war auch der verfassungsrechtlichen Bedeutung der vorgesehenen Regelungen nicht angemessen, ermöglichen einige doch umfangreiche Eingriffe in grundrechtlich geschützte Rechtspositionen der Bürgerinnen und Bürger.

Ich wandte mich daher an den Gesundheitsausschuss und machte auch hier meine Bedenken an der automatischen Verlängerung und die Erforderlichkeit der laufenden Überprüfung auf Erforderlichkeit geltend. Zu meinem Bedauern wurden meine Hinweise nicht berücksichtigt. Mit dem vierten Pandemie-Schutzgesetz wurde im Juli 2021 stattdessen eine weitere Änderung vorgesehen: die Verordnung gilt demnach sogar bis längstens ein Jahr über die Dauer der epidemischen Lage hinaus. Grundsätzlich impliziert das Auslaufen der epidemischen Lage, dass die pandemiebegingt eingeführten Regelungen entbehrlich werden. Inwiefern die Pflichten und Eingriffe auch nach Wegfall der epidemischen Lage noch erforderlich sein sollten, bedarf daher erst recht fortlaufend der sorgfältigen Überprüfung.

Corona-Einreiseverordnung

Die Corona-Einreiseverordnung wurde am 12. Mai 2021 neugefasst und galt für die Dauer der Feststellung der epidemischen Lage. Vor Erlass dieser Neufassung wurde ich leider überhaupt nicht beteiligt und erlangte erst im Nachhinein Kenntnis. In der Folgezeit wurden Regelungen bereits in der Presse thematisiert, obwohl die Ressortabstimmung nicht abgeschlossen war.

Nach den Regelungen in der Neufassung mussten einreisende Personen zusätzlich die Nachweise als geimpft, genesen oder getestet über das Portal für die digitale Einreiseanmeldung an das zuständige Gesundheitsamt übermitteln. Dabei wird die Tatsache des Vorliegens des Nachweises („ob“) bereits bei der Anmeldung angegeben. Zuvor war die Vorlage daher nur auf Anforderung der Behörde vorgesehen.

Leider erschöpft sich die Begründung für die Änderung hier entgegen §§ 62, 43 GGO in der Beschreibung der Regelung und erläutert nicht, warum eine stichprobenhafte Kontrolle nicht mehr ausreichen soll. Zu dieser Ausweitung der vorsorglichen Datenübermittlungen bei der Einreise war daher nicht ersichtlich, dass der Nutzen der Neuregelung die stärkere Eingriffstiefe rechtfertigen konnte. In der Fassung vom Juli wurde die Verordnung dann unabhängig vom Bestehen der Pandemielage bis zum Ende des Jahres 2021 befristet.

Bei der folgenden Neufassung im September, bei der meine Beteiligung bedauerlicherweise wieder versäumt wurde, blieb die Frist unverändert. Dennoch ist fortlaufend zu überprüfen, ob die mit der Anmeldepflicht verbundene Datenübermittlung zur Pandemiebekämpfung geeignet und erforderlich ist.

4.1.8 Zweites IfSG-Änderungsgesetz: digitale Nacherfassung der Impfungen und 3G am Arbeitsplatz

Die Nacherfassung und 3G am Arbeitsplatz als eine der datenschutzrechtlichen Herausforderungen der Pandemiebekämpfung – Deutschland digitalisiert die Impfbescheinigung mit Risiken für die Vertrauenswürdigkeit und weist Arbeitgebern eine wesentliche Rolle bei der Pandemiebekämpfung zu.

Unmittelbar folgend auf das Vierte Bevölkerungs-Schutz-Gesetz vom 22. April 2021 wurde bereits die nächste Änderung des Infektionsschutzgesetzes angegangen. Am Freitagnachmittag, den 23. April 2021, wurde der Entwurf eines „Gesetzes zur Änderung des Infektionsschutzgesetzes und anderer Gesetze“ mit erneut extrem kurzer Frist zur Stellungnahme bis Montag, 26. April 2021, vorgelegt. Mit der Änderung sollten Nachtragungen im Impfausweis und die Ausstellung digitaler Impfnachweise auch durch Apothekerinnen und Apotheker möglich sein. Dies sollte offenbar dazu dienen, den geimpften Personen möglichst schnell zu dem von der EU konzipierten Digitalen Zertifikat zu verhelfen, ohne die Impfzentren und Hausarztpraxen übermäßig zu belasten. Denn die Impfkampagne war bereits in vollem Gange: Durch Impfteams und Impfzentren hatten die Angehörige von Risikogruppen ihre Impfung bereits erhalten, bevor die technischen Vorgaben und die nötigen Anschlüsse und Übermittlungswege für die Generierung des digitalen Impfnachweises zur Verfügung standen.

Dieses Ziel ist nachvollziehbar. Die Regelung geht jedoch weit darüber hinaus: Sie ist allgemein gefasst und damit nicht auf die Corona-Impfungen beschränkt. Die Nachtragung oder Bestätigung durch eine Person, die die Impfung nicht selbst vorgenommen hat, birgt dabei immer ein Risiko hinsichtlich der inhaltlichen Richtigkeit.

Dem Infektionsschutz kann jedoch nur ein Impfnachweis dienen, der eine tatsächlich durchgeführte Impfung bescheinigt. Es waren zu diesem Zeitpunkt bereits Fälschungen von Impfnachweisen in erheblichem Umfang im Umlauf. Durch die Nacherfassung durch Apotheken unter der eigenen elektronischen Signatur übernimmt die jeweils nacherfassende Person die

Verantwortung auch für die inhaltliche Richtigkeit. Das Risiko, in erheblichem Umfang hierdurch inhaltlich falsche digitale Impfnachweise zu generieren, hielt ich für beachtlich und ein Interesse an falschen Nachweisen aufgrund der damit verbundenen Vorteile für hoch.

Diesem signifikanten Risiko wurde durch den Gesetzentwurf in keiner Weise begegnet. Erst mit dem „Gesetz zur Änderung des Infektionsschutzgesetzes und weiterer Gesetze anlässlich der Aufhebung der Feststellung der epidemischen Lage von nationaler Tragweite“ vom 22. November 2021 (BGBl 2021, S. 4906) wurden flankierend die Straftatbestände im Strafgesetzbuch angepasst, um gegen bekannt gewordene Fälschungen vorgehen zu können. Es wurde leider nicht geprüft, ob eine anderweitige Unterstützung von Impfzentren und Arztpraxen möglich wäre, die – entsprechend meiner Empfehlung – eine zuverlässige, inhaltlich richtige Nacherfassung durch die impfende Institution selbst gewährleisten würde. Ebenso wurde entgegen meiner Empfehlung die Nacherfassung allgemein zugelassen; es wurde darauf verzichtet, sie auf besondere Fälle – wie die Impfungen vor der Möglichkeit zur digitalen Erfassung oder besondere Ausnahmen oder auch nur auf Corona-Impfungen – zu begrenzen oder zu befristen. Hier soll eine risikogeneigte Datenverarbeitung zur Methode werden. Bei der zu erwartenden Evaluation des Infektionsschutzgesetzes sollte dieser Passus auf der Agenda stehen.

3G am Arbeitsplatz

In demselben Gesetzgebungsverfahren vom 22. November 2021 (BGBl 2021, S. 4906) wurden erstmals Regelungen zur Verarbeitung sog. 3G-Daten („geimpft, genesen, getestet“) am Arbeitsplatz aufgenommen. Schon lange vorher habe ich den zuständigen Bundesministerien geraten, datenschutzgerechte Rechtsgrundlagen zu schaffen, die die Verarbeitung von 3G-Daten am Arbeitsplatz ermöglichen.

Die gesetzliche Regelung sieht nun allerdings eine Pflicht zur Prüfung des 3G-Status vor Zutritt zur Arbeitsstätte vor. Arbeitgeberinnen und Arbeitgeber dürfen die sensiblen 3G-Daten aus den Impf-, Genesenen- oder Testnachweisen ihrer Beschäftigten verarbeiten, soweit dies für den Zweck der Zugangskontrolle zur Arbeitsstätte und für die Dokumentation, dass die gesetzlichen Zutrittsvoraussetzungen eingehalten wurden, erforderlich ist. Außerdem dürfen die Daten für die Anpassung von Hygienekonzepten auf Grundlage der Gefährdungsbeurteilung verarbeitet werden.

Die Fristen zur Stellungnahme waren auch in diesem Gesetzgebungsverfahren wieder sehr kurz bemessen. Ich hätte mir für eine Beratung eine deutlich frühere Beteiligung gewünscht, die nach meinen frühen Hinweisen unproblematisch möglich gewesen wäre. Ich halte eine datenschutzkonforme Anwendung der gesetzlichen Vorgaben für unabdingbar: Arbeitgeberinnen und Arbeitgeber haben sorgfältig zu prüfen, welche der sensiblen Gesundheitsdaten ihrer Beschäftigten sie unter welchen Bedingungen für den jeweiligen Zweck unbedingt erheben, speichern oder anderweitig verarbeiten müssen. Dabei sind die Grundsätze der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und der Speicherbegrenzung (Art. 5 Abs. 1 und 17 lit. e DSGVO) sowie die besonderen Vorgaben für die Verarbeitung sensibler Gesundheitsdaten nach dem Bundesdatenschutzgesetz und der Datenschutzgrundverordnung zu berücksichtigen. Wird beispielsweise der genaue 3G-Status der Beschäftigten mittels Sichtkontrolle oder CovPassCheck-App vor Zutritt zum Gebäude erhoben, so ist es für die Zutrittskontrolle regelmäßig nicht erforderlich, den 3G-Status personengenau längerfristig zu speichern. Für die Erfüllung der Dokumentationspflicht genügt es, nachprüfbare Prozesse zu etablieren, auf welche Weise der 3G-Status der Beschäftigten durch die Arbeitgeber geprüft wird. Für die Anpassung betrieblicher Hygienekonzepte sind personenbezogene 3G-Daten der Beschäftigten im Regelfall nicht erforderlich. Zu prüfen ist, ob die Verarbeitungszwecke auch mit anonymisierten, pseudonymisierten und aggregierten Daten erreicht werden können. Wichtig ist zudem, dass die Erhebung durch Personen erfolgt, die gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet sind, beispielsweise nicht durch unmittelbare Vorgesetzte, und dass die 3G-Daten durch technisch-organisatorische Maßnahmen vor der unbefugten Kenntnisnahme durch Dritte geschützt sind. Dazu gehören auch Kolleginnen und Kollegen. Sobald der Zweck für die Speicherung der Gesundheitsdaten entfallen ist, müssen sie gelöscht werden. Die maximal zulässige Speicherdauer von sechs Monaten nach Erhebung, die § 28b Abs. 3 Satz 9 IfSG vorsieht, kann also auch wesentlich kürzer ausfallen.

Querverweise:

4.1.3 Digitales COVID Zertifikat

4.1.9 Digitales Impfquotenmonitoring

Von der Schwierigkeit, in der Pandemie mit digitalen Mitteln die Übersicht über die Impfungen zu behalten oder: (Zu) viele Wege führen zum Robert Koch-Institut. Die mit dem Masernschutz eingeführte und pandemiebedingt ausgeweitete Meldepflicht erfüllt ihren Zweck nicht vollständig und sollte zusammen mit dem Meldeverfahren grundlegend überarbeitet werden.

Mit dem Dritten Bevölkerungs-Schutz-Gesetz (Drittes Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite vom 18. November 2020, 29. TB Nr. 4.1.4) wurde in § 13 Abs. 5 Infektions

schutzgesetz (IfSG) eine Pflicht der Kassenärztlichen Vereinigungen und der Impfzentren zur Meldung von Daten zu Impfung und Impffolgen vorgesehen, die sowohl an das Robert Koch-Institut (RKI) als auch das Paul-Ehrlich-Institut (PEI) zu übermitteln wären.

Die von mir als nicht erforderlich und nicht datensparsam kritisierte Doppelung gab es dann in der Praxis tatsächlich nicht: die Daten werden dem RKI übermittelt, das diese aggregiert an das PEI leitet. Eine Korrektur der entsprechenden gesetzlichen Regelung erfolgte nicht, obwohl ich das in meiner Stellungnahme zum EpiLage-Fortsetzungsgesetz (siehe Nr. 4.1.7) angemahnt hatte. Übrigens: schon im Zusammenhang mit dem Masernschutzgesetz (vgl. 28. TB Nr. 5.6) hatte mir das Bundesministerium für Gesundheit (BMG) eigentlich zugesagt, Datenkranz und Übermittlungsverfahren zu überprüfen. Stattdessen wird das Konzept auf Basis der bedenklichen Regelung weiter ausgebaut.

Im März wurde durch eine Änderung der Verordnung zum Anspruch auf Schutzimpfung gegen das Coronavirus SARS-CoV-2 (Impfverordnung) der Kreis der zum Impfen Berechtigten und zur Meldung Verpflichteten auf Arztpraxen und Betriebsärzte erweitert. Der Entwurf der Änderungsverordnung wurde mir am 22. März mit Frist zur Stellungnahme zum 25. März zugeleitet. Die kurze Frist erschwerte auch hier die sachgemäße Prüfung, ebenso wie unzureichende Erläuterungen in der Begründung. Dies wäre wegen der verschiedenen Meldewege erforderlich gewesen: Die Meldungen laufen teils aggregiert direkt an das RKI, teils personenbezogen an die Kassenärztliche Vereinigung, teils unter Nutzung des elektronischen Meldesystems der Kassenärztlichen Bundesvereinigung, teils unter Verwendung des Deutschen Elektronischen Melde- und Informationssystems gem. § 14 IfSG (DEMIS), das das RKI zur Verfügung stellt. Hier stellte sich die Frage, ob insgesamt eine aggregierte, anonyme und unmittelbare Übermittlung ausgereicht hätte. Tatsächlich entstanden später trotz – oder wegen – der umfassenden Regelung bekanntlich erhebliche Unsicherheiten über die tatsächliche Impfquote.

Schon im Jahr 2020 hatte ich damit begonnen, das RKI zur technischen Umsetzung des Meldeverfahrens, das in Zusammenarbeit mit der Bundesdruckerei realisiert werden sollte, zu beraten. Die Angaben zur Impfung werden in den Impfzentren über eine Web-Applikation der Bundesdruckerei erfasst; alternativ kann über eine von der Bundesdruckerei zur Verfügung gestellte Schnittstelle eine Einbindung in die in den jeweiligen Impfzentren genutzte Software zur Erfassung genutzt werden. Prüfbedürftig war hierbei das angewandte Pseudonymisierungsverfahren, bei dem die Bundesdruckerei – bei Verwendung der o. g. Schnittstelle – nicht für das RKI, sondern für die Impfzentren tätig wird, so dass eine zuverlässige Trennung der Aufgabenwahrnehmung zu gewährleisten war.

Ich empfehle, die Wege und den Datenkranz bei der Meldung von Impfungen – Impfquotenmonitoring – zu überprüfen.

Querverweise:

4.1.7 Das „EpiLage-Fortgeltungsgesetz“

4.2 Künstliche Intelligenz – Regulierung als gesamtgesellschaftliche Aufgabe

Künstliche Intelligenz (KI) ist eine Schlüsseltechnologie der Digitalisierung. Algorithmenbasierte Entscheidungsprozesse und lernende Systeme dringen in alle Lebensbereiche vor und versprechen Lösungsansätze, an die ohne KI kaum zu denken wäre. Es ist eine wesentliche gesellschaftliche und politische Aufgabe, diese Technologie so zu gestalten, dass sie den Menschen und seine Rechte in den Mittelpunkt stellt und dabei gleichzeitig innovative Entwicklungen und einen breiten Einsatz in vielen Bereichen ermöglicht.

Der Innovationswert, der sich aus Anwendungen der KI ergibt, ist unbestreitbar. Ihre immer stärkere Verbreitung bringt jedoch nicht nur Vorteile mit sich. Sie kann auch zu grundlegenden und tiefgreifenden Verletzungen von Grundrechten führen. Beispielsweise helfen KI-basierte medizinische Verfahren dabei, dass Krebserkrankungen früher erkannt werden können. Sprach- oder Gesichtserkennungssoftware, die Personen auf der Grundlage ihrer biometrischen Merkmale identifiziert, kann zur Kriminalitätsbekämpfung und Aufklärung von Straftaten zum Einsatz kommen. Sie kann aber genauso repressiv zur Überwachung und Kontrolle der Bürgerinnen und Bürger eingesetzt werden.

Gleichzeitig verändert KI die Interaktion von Mensch und Technik in der Arbeitswelt. So können Assistenzsysteme Beschäftigte beispielsweise von anstrengenden oder gefährlichen Tätigkeiten entlasten und bei komplexen Prozessen und Entscheidungen unterstützen. Trotz dieser Chancen darf KI nicht um jeden Preis Eingang in die Arbeitswelt finden. Denn ihre Anwendung in der Arbeitswelt, zum Beispiel in Bewerbungsverfahren, ist mit einem besonders hohen Risiko für die Persönlichkeitsrechte von Bewerbern und Beschäftigten verbunden. Spezifische gesetzliche Regelungen für den Einsatz von KI in diesem Bereich sind notwendig, fehlen jedoch

bislang. Im Beirat Beschäftigtendatenschutz (vgl. Nr. 4.3) habe ich mich daher dafür eingesetzt, den Einsatz von KI im Beschäftigtenkontext in Deutschland gesetzlich zu regeln.

KI kann häufig leicht in bestehende Systeme und Anwendungen integriert werden. Solche Systeme und Anwendungen enthalten vielfach bereits biometrisch auswertbare Informationen wie etwa Fotos, Videos oder Stimmaufzeichnungen. Sie können mit geringem Aufwand durch KI so ergänzt werden, dass biometrische Auswertungen möglich werden. Der Einsatz von KI besonders zur biometrischen Datenanalyse muss daher sehr sorgfältig auf seine individuellen, aber auch gesamtgesellschaftlichen Auswirkungen überprüft werden. Gerade in Bezug auf den Einsatz von KI ist es wichtig, die Bedeutung des Datenschutzes für die Achtung von Versammlungsfreiheit, Meinungs- und Meinungsäußerungsfreiheit und Vereinigungsfreiheit anzuerkennen.

Es ergibt sich an vielen Stellen also durchaus ein Spannungsverhältnis. Der Datenschutz kann hier einen wichtigen Beitrag für einen Interessenausgleich leisten: durch Aspekte wie Risikoabwägung, Transparenz, Überprüfbarkeit und Intervenierbarkeit trägt er dazu bei, dass sich der Fortschritt so gestalten lässt, dass KI gleichzeitig effizient, innovativ, datenschutzkonform und am Gemeinwohl orientiert ist. Datenschutz ist damit ein maßgebliches Erfolgskriterium für KI-Anwendungen.

KI lässt sich kaum mehr in nationalstaatlichen Grenzen denken. Eine so globalisierte Technologie erfordert auch eine verstärkte internationale Zusammenarbeit. Um hier einen entsprechenden Rahmen zu schaffen und den Gestaltungsprozess im Sinne einer positiven Technikentwicklung zu beeinflussen, bei der die Rechte und Interessen des Individuums geschützt werden, engagiere ich mich aktiv in nationalen und internationalen Gremien, die sich mit der KI-Entwicklung befassen.

KI auf internationaler Ebene

Die Europäische Kommission hat im vergangenen Jahr den weltweit ersten Entwurf für einen Rechtsrahmen zur KI vorgelegt. Der umfassende Regulierungsentwurf soll die Entwicklung von KI fördern, ein hohes Schutzniveau für öffentliche Interessen gewährleisten und eine Vertrauensbasis für KI-Systeme schaffen. In einer Stellungnahme zum Regulierungsentwurf hat sich der Europäische Datenschutzausschuss (EDSA) dafür ausgesprochen, dass der Einsatz von KI verboten wird, wenn Persönlichkeit und Würde des Menschen nicht geachtet werden. Als Teil des Berichterstatter-Teams des EDSA habe ich mich hier nachdrücklich für die herausragende Bedeutung des Datenschutzes bei der Gestaltung von KI eingesetzt (vgl. Nr. 4.2.1). Der EDSA wird im Jahr 2022 Richtlinien für den Einsatz von Gesichtserkennungstechnologie durch Polizei- und Strafverfolgungsbehörden veröffentlichen. Auch hier bringe ich mich als einer der Berichterstatter aktiv ein.

Darüber hinaus bin ich in der sogenannten „Working Group Artificial Intelligence“ der Global Privacy Assembly (GPA) engagiert. Dabei handelt es sich um eine Unterarbeitsgruppe der internationalen Datenschutzkonferenz, die regelmäßig datenschutzpolitische bzw. datenschutzrechtliche KI-Themen diskutiert und dazu Entschließungen und Empfehlungen erarbeitet. Bereits im vergangenen Jahr wurde eine Resolution zum Umgang mit der Nutzung von KI verabschiedet, die die grundsätzlichen Anforderungen für die Entwicklung und Nutzung von KI darlegt, die erforderlich sind, um den gebotenen Rechenschaftspflichten nachzukommen. Aktuell arbeite ich innerhalb dieses Gremiums u. a. intensiv an einem Papier mit, das sich mit den Risiken für die Rechte und Freiheiten des Individuums durch KI-Systeme beschäftigt. Ziel ist es hierbei, den Blick für die individuellen, aber auch gesellschaftlichen Risiken für Datenschutz und Ethik im Zusammenhang mit KI zu schärfen.

Eine weitere Zusammenarbeit im KI-Bereich wurde während des G7- Regulatory Cooperation Roundtable beschlossen. Dabei sind die Datenschutzaufsichtsbehörden der G7-Mitgliedsstaaten im September 2021 unter dem Vorsitz der britischen Datenschutzbeauftragten Elizabeth Denham erstmalig zusammengekommen (vgl. Nr. 3.4.1). In einem gemeinsamen Kommuniqué wurde die zentrale Bedeutung der Menschenwürde bei der Gestaltung von KI hervorgehoben. Es bestand Einigkeit darüber, dass die wesentlichen Grundsätze der Zweckbindung und der Datenminimierung gelten müssen und KI transparent, verständlich und erklärbar sein muss. Auf dieser Grundlage wurde vereinbart, auch künftig in einer eigenen Arbeitsgruppe zum Thema KI die Entwicklung interoperabler Konzepte für die Regulierung über alle Rechtsordnungen hinweg und vor dem Hintergrund eines menschenzentrierten Ansatzes zu fördern.

Ohne automatisierte, intelligente Analyse- und Entscheidungssysteme kann die in einer digitalisierten Welt anfallende Menge an Daten kaum effizient genutzt werden. Es ist unsere Aufgabe, gemeinsam mit Politik, Gesellschaft, Wissenschaft und Wirtschaft diese Nutzung von auf KI basierenden Systemen auf tragfähige Beine zu stellen. Damit soll ein Gerüst geschaffen werden, das einen mit demokratischen Grundsätzen zu vereinbarenden, rechtskonformen und gemeinwohlorientierten Einsatz von KI ermöglicht.

Querverweise:

3.4.1 G7, 4.2.1 KI-Regulierungsentwurf, 4.3 Interdisziplinärer Beirat Beschäftigtendatenschutz

4.2.1 KI-Regulierungsentwurf

In seiner Stellungnahme zum Regulierungsentwurf der Europäischen Kommission unterstreicht der EDSA die herausragende Bedeutung des Datenschutzes bei der Nutzung von KI.

Ich habe mich im EDSA und ganz besonders auch als Teil des Berichterstatter-Teams aktiv dafür stark gemacht, dass der Einsatz von KI verboten wird, wenn sie die Persönlichkeit und Würde des Menschen nicht achtet oder hohe Risiken für Leben und Gesundheit von Personen bestehen. Zudem habe ich mit Nachdruck die Forderung nach einem allgemeinen Verbot der Verwendung von KI zur automatischen Erkennung von personenbezogenen Merkmalen in öffentlich zugänglichen Räumen unterstützt. Die Nutzung von KI darf nicht an den Grundfesten unseres gesellschaftlichen Miteinanders rühren.

Mit dem Entwurf für einen Rechtsrahmen zur KI verfolgt die Kommission einen risikobasierten Ansatz, der grundsätzlich auch vom EDSA in seiner Stellungnahme begrüßt wird. Für Anwendungen, die mit einem hohen Risiko einhergehen, werden bestimmte Qualitätsanforderungen vorgesehen, z. B. Protokollierungs- und Dokumentationsvorgaben, eine weitreichende Information der Nutzer, eine hohe Qualität der Datensätze oder auch eine menschliche Aufsicht zur Minimierung der Risiken.

Der EDSA begrüßt diese Vorgaben, sieht in den Vorschlägen aber noch Veränderungsbedarf, den er im Rahmen der Stellungnahme deutlich macht.

Besorgnis besteht etwa darüber, dass die internationale Zusammenarbeit auf dem Gebiet der Strafverfolgung nicht in den Anwendungsbereich des Vorschlags fällt. Hinterfragt wird unter anderem auch die Tatsache, dass der Europäischen Kommission im Europäischen Ausschuss für künstliche Intelligenz eine übergeordnete Stellung eingeräumt werden soll. Aus unserer Sicht wird vielmehr eine europäische Stelle benötigt, die unabhängig von politischer Einflussnahme ist. Um die Unabhängigkeit des Ausschusses zu gewährleisten, sollte diesem mehr Selbstständigkeit zuerkannt und es ihm ermöglicht werden, von sich aus initiativ zu werden.[14]

Dass die Europäische Kommission die grundsätzliche Beschäftigung mit einem Regulierungsrahmen auf diesem Weg angestoßen hat, ist ein wichtiger Schritt. Es wird aber noch viel Arbeit notwendig sein, bis der Vorschlag einen gut funktionierenden Rechtsrahmen hervorbringt, der die geltenden Regeln zum Datenschutz, wie etwa die Datenschutz-Grundverordnung, beim Schutz der grundlegenden Menschenrechte wirksam ergänzt und gleichzeitig KI-Innovationen fördert.

Im vorgelegten Entwurf kommt der Aspekt KI im Gesundheitswesen nur am Rande vor. Lediglich die Risiken der Nutzung von KI für die Gesundheit werden häufig betont. Positive Wirkungen und Chancen der Nutzung von KI im Gesundheitsbereich sollen in einem eigenen Rechtsakt zum europäischen Raum für Gesundheitsdaten geregelt werden (vgl. Erwägungsgrund 45). Die Vorlage eines Entwurfs eines Rechtsaktes zum Europäischen Gesundheitsdatenraum war zunächst für den Herbst 2021 geplant, wurde dann aber auf das Frühjahr 2022 verschoben.

Es stellen sich grundlegende Fragen, die nur in einem breiten gesellschaftlichen Dialog sinnvoll zu beantworten sind. Außerdem muss das Zusammenspiel zwischen der neuen KI-Verordnung und bestehendem Recht, insbesondere der Datenschutz-Grundverordnung, sowie Fragen der Ausgestaltung von Aufsicht und Rechtsdurchsetzung geklärt werden. Dafür werde ich mich auch weiterhin einsetzen.

Querverweise:

3.4.1 G7, 4.3 Interdisziplinärer Beirat Beschäftigtendatenschutz

4.2.2 KI-Konsultationsverfahren

Der Einsatz von Künstlicher Intelligenz (KI) muss sich immer am Maßstab des Verfassungsrechts messen lassen. Das Konsultationsverfahren zum Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr soll die Öffentlichkeit in die Meinungsbildung einbeziehen.

Im Bereich der Strafverfolgung und der Gefahrenabwehr wird der Einsatz von KI erforscht, erprobt und teilweise praktiziert. Die datenschutzrechtlichen und verfassungsrechtlichen Vorgaben sind noch nicht geklärt. Sie müssen deshalb konkretisiert werden. Der Einsatz von KI kann sich auf die Arbeit der Sicherheitsbehörden und die Freiheiten für die betroffenen Personen erheblich auswirken. Deshalb ist eine breite öffentliche Debatte notwendig. Ich habe daher ein Konsultationsverfahren zum Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr eingeleitet. Folgende Thesen habe ich zur Diskussion gestellt:

- KI erfordert eine ausführliche empirische Bestandsaufnahme und eine umfassende gesellschaftspolitische Diskussion, um einerseits die Auswirkungen

14 Die Stellungnahme ist abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_de.

dieser Technologie auf die Freiheiten der Bürgerinnen und Bürger zu klären und andererseits die Erforderlichkeit ihres Einsatzes zu Strafverfolgungs- und Gefahrenabwehrzwecken festzustellen. Die Risiken sind dem Nutzen umfassend gegenüberzustellen. Mögliche Diskriminierungen und überindividuelle Folgen sowohl für bestimmte Personengruppen als auch für demokratische und rechtsstaatliche Abläufe insgesamt sind wirksam auszuschließen. Der Gesetzgeber soll alle derzeit existierenden Befugnisse der Strafverfolgungs- und Gefahrenabwehrbehörden in eine Gesamtrechnung einbeziehen („Überwachungs-Gesamtrechnung“).

- Der Einsatz von KI kann nicht auf polizeiliche Generalklauseln gestützt werden. Vielmehr erfordert der Einsatz von KI grundsätzlich eine spezifische gesetzliche Regelung.
- Die Einhaltung der allgemeinen Datenschutzgrundsätze ist eine unabdingbare Voraussetzung für den datenschutzrechtlich zulässigen Einsatz von KI. Der Einsatz von KI darf die effektive Ausübung der Betroffenenrechte nicht schmälern.
- KI muss erklärbar sein. Die Qualität der schon zu Trainingszwecken eingesetzten Datensätze ist sicherzustellen.
- Der Kernbereich privater Lebensgestaltung bzw. die Menschenwürdegarantie dürfen beim Einsatz von KI nicht berührt werden.
- KI muss durch Datenschutzaufsichtsbehörden umfassend kontrolliert werden können.
- Dem Einsatz von KI muss eine umfassende Datenschutzfolgen-Abschätzung vorangehen.

Nach Auswertung der eingegangenen Stellungnahmen werde ich über die Ergebnisse berichten.

4.3 Interdisziplinärer Beirat Beschäftigtendatenschutz

Ein Beschäftigtendatenschutzgesetz ist dringend notwendig!

Bereits in meinem letzten Tätigkeitsbericht (s. 29. TB, Nr. 2.3; 7.2) habe ich dem Gesetzgeber empfohlen, von der in der DSGVO eingeräumten Möglichkeit zeitnah Gebrauch zu machen, nationale Regelungen zum Beschäftigtendatenschutz zu erlassen. Seit vielen Jahren fordern die Datenschutzaufsichtsbehörden von Bund und Ländern ein Beschäftigtendatenschutzgesetz. Heute ist dies umso dringender: Die rasant fortschreitende Digitalisierung in Betrieben und Verwaltungen führt zu tiefgreifenden Veränderungen der Arbeitswelt. Datengetriebene Prozesse prägen mittlerweile den Arbeitsalltag vieler Beschäftigter. In Betrieben und Verwaltungen entstehen immer mehr und immer detailliertere Datensätze. Verbunden mit den neuen Möglichkeiten der Datenverknüpfung und –auswertung bietet dies einerseits Chancen für eine effizientere Gestaltung der Arbeitsorganisation. Andererseits erhöht sich für Beschäftigte zugleich das Risiko, ihre Privatsphäre bis hin zu einer totalen Überwachung einzubüßen.

Der vom Bundesministerium für Arbeit und Soziales im Sommer 2020 eingesetzte interdisziplinäre Beirat Beschäftigtendatenschutz (siehe 29. TB, Nr. 7.2), dem auch ich angehöre, prüft u. a., inwieweit Regelungen für den Schutz der Rechte von Beschäftigten in der digitalen Arbeitswelt notwendig sind. Die Kurzfassung des Beiratsberichts wurde dem Bundesminister für Arbeit und Soziales im Januar 2022 übergeben.

Im Rahmen meiner Beiratstätigkeit habe ich mich dafür eingesetzt, dass beschäftigtendatenschutzrechtliche Regelungen geschaffen werden. In vielen Konstellationen genügt die gegenwärtige Fassung des § 26 BDSG aufgrund ihrer Interpretationsbedürftigkeit nicht, um einen effektiven, rechtssicheren Schutz vor eingriffsintensiven Datenverarbeitungen in der digitalisierten Arbeitswelt zu gewährleisten. Der Einsatz künstlicher Intelligenz in Bewerbungsverfahren, das Beschäftigtenscreening oder GPS-Tracking sind nur einige beispielhafte Aspekte für die Herausforderungen bei der Digitalisierung der Arbeitswelt. Sie machen die Regelungslücken sichtbar und einen besseren Schutz der Beschäftigten wichtiger denn je. Rechtssicherheit für alle Beteiligten ist erforderlich. Daher braucht es ein Beschäftigtendatenschutzgesetz, das spezifische Datenverarbeitungen im Beschäftigtenkontext und Eckpunkte im Beschäftigungsverhältnis regelt. Dazu gehören beispielsweise ein Verbot der Totalüberwachung, Grenzen einer Verhaltens-und Leistungskontrolle, Hinweise zu Beweisverwertungsverboten sowie der Einsatz neuer Technologien, insbesondere algorithmische Systeme. Wichtig sind neben einer starken Datenschutzaufsicht auch Instrumente individuellen Schutzes, z. B. hinsichtlich der Durchsetzung der Betroffenenrechte sowie des kollektiven Schutzes.

Ich begrüße, dass der Koalitionsvertrag 2021 ein Bekenntnis zur Schaffung von Regelungen zum Beschäftigtendatenschutz enthält, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen und hoffe sehr, dass diese Chance in der 20. Legislaturperiode endlich ergriffen wird.

5 Gesetzgebung

5.1 Telekommunikationsgesetzgebung TKG/TTDSG

Nach langer Wartezeit gibt es seit Dezember 2021 das Telekommunikationsmodernisierungsgesetz. Zeitgleich werden andere Gesetze im Telekommunikationsbereich an das europäische Recht angepasst.

In meinem letzten Tätigkeitsbericht (Nr. 5.10) konnte ich bereits über einen ersten Gesetzesentwurf berichten.

Das neue Telekommunikationsgesetz wurde im Rahmen des Telekommunikationsmodernisierungsgesetzes (TKMoG) überarbeitet und trat am 1. Dezember 2021 zeitgleich mit dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft. Hierbei werden die bisherigen Datenschutzvorschriften aus dem neuen TKG ausgeklammert und in das TTDSG überführt. Die Novelle dient zugleich der Umsetzung der Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation.

Der Begriff des Telekommunikationsdienstes wird hierbei deutlich erweitert und umfasst nun auch Messenger-Dienste, E-Mail-Dienste und Videokonferenzdienste. Daher ergibt sich hier grundsätzlich seit dem 1. Dezember 2021 eine einheitliche Zuständigkeit des BfDI auf nationaler Ebene sowohl für Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) als auch bei der Verletzung des Schutzes von Verkehrsdaten (vgl. im Einzelnen §§ 29, 30 TTDSG).

Bislang war der Begriff des Telekommunikationsdienstes in § 3 Nr. 24 TKG (alte Fassung) definiert als „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen“ (sogenannter technischer Ansatz). Sowohl der Verordnungsgeber auf europäischer Ebene als auch der deutsche Gesetzgeber gehen nun von einem funktionalen Ansatz aus, da es aus der Sicht des Endnutzers keinen Unterschied mache, ob dieser zum Beispiel einen SMS-Dienst oder einen Messenger-Dienst verwenden würde. Die neue Definition findet sich nun in § 3 Nr. 61 TKG: „Telekommunikationsdienste [sind] in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen:

- Internetzugangsdienste, (§ 3 Nr. 23 TKG)
- interpersonelle Telekommunikationsdienste (im Sinne des § 3 Nr. 24 TKG) und
- Dienste, die überwiegend in der Übertragung von Signalen bestehen wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden;“

Insbesondere durch den Begriff des interpersonellen Telekommunikationsdienstes werden daher in Zukunft neben der Internettelefonie sogenannten Over-the-Top-Dienste, wie Messenger-Dienste und Gruppenchats, sowie auch webgestützte E-Mail-Dienste und Videokonferenzdienste als Telekommunikationsdienst definiert.

Im Laufe der Ressortabstimmung zum TKMoG habe ich durch zahlreiche Stellungnahmen auf die datenschutzrechtlichen Defizite des Gesetzesentwurfs hingewiesen. Einige noch weitgehendere Vorstöße zur Erhebung und Weiterleitung von personenbezogenen Daten durch die TK-Anbieter an Sicherheitsbehörden konnten dadurch verhindert werden. Dennoch enthält das Gesetz noch zahlreiche kritisch zu beurteilende Regelungen, von denen ich beispielhaft zwei herausgreifen möchte.

In § 172 Abs. 3 TKG ist festgelegt, dass nummernunabhängige Dienste die Kennung des Dienstes, den Namen, die Anschrift, das Geburtsdatum sowie das Datum der Vergabe der Kennung speichern müssen, soweit sie diese Daten erheben. Ursprünglich war sogar eine Erhebungspflicht für noch weitere Daten geplant. Eine allgemeine Erhebungspflicht für Identifikationsdaten,

wie sie in § 111 Abs. 1 TKG (alte Fassung) angelegt war, hätte jedoch die grundsätzlich anonyme Nutzbarkeit entsprechender Dienste konterkariert. Eine entsprechende Erhebungspflicht erschien trotz des angestrebten sicherheitspolitischen Zwecks unverhältnismäßig und wurde von mir abgelehnt. Daher habe ich für eine mit der zuvor geltenden Regelung des § 111 Abs. 2 TKG (alte Fassung) vergleichbare Norm plädiert, die für elektronische Post gilt. Diese sieht zwar eine Speicherpflicht für einzelne erhobene Daten, aber keine zusätzliche Erhebungspflicht vor. Dennoch ist durch die Speicherpflicht zum Beispiel des Geburtsdatums ein zusätzliches Datum eingeführt worden, durch das die anonyme Nutzbarkeit der Dienste zumindest eingeschränkt wird. Gerade für bestimmte Berufsgruppen, wie Anwältinnen und Anwälte oder Journalistinnen und Journalisten, ist die anonyme Nutzbarkeit moderner Kommunikationsmittel wie E-Mail und Messenger-Dienste ein wichtiger Bestandteil ihrer täglichen Arbeit. Die Erweiterung der gesetzlichen Regelung in § 172 Abs. 3 TKG folgt hierbei nicht etwa – wie man meinen könnte – aus dem Kodex für elektronische Kommunikation, der mit der Gesetzesnovelle in nationales Recht umgesetzt wurde, sondern folgt allein den Änderungswünschen des deutschen Gesetzgebers. Dies sehe ich unter einem weiteren Gesichtspunkt kritisch: Die Übernahme von und die Anpassung an Begrifflichkeiten, wie sie etwa in der Richtlinie (EU) 2018/1972 oder sonst in Bezug auf die anderen Teile des TKG vorgesehen sind, ist kein Automatismus. Diese Begrifflichkeiten dienen im Wesentlichen anderen Zielsetzungen, wie etwa der Marktregulierung, der Frequenzpolitik, dem Schutz der Endnutzenden, dem institutionellen Gefüge oder einer Grundversorgung mit Telekommunikationsdiensten. Hiervon zu unterscheiden ist die Erweiterung der Befugnisse der Sicherheitsbehörden z. B. hinsichtlich des Zugriffsrechts auf Daten im Rahmen der Auskunftsverfahren nach § 173 und § 174 TKG, etwa durch eine Ausweitung des Kreises der verpflichteten Telekommunikationsanbieter. Diese folgt nicht automatisch aufgrund Änderungen von Vorschriften zur Marktregulierung oder zur Sicherstellung der Grundversorgung. Erweiterungen der Befugnisse müssen im Rahmen des Gesetzgebungsprozesses im Einzelnen begründet werden. Dazu sind entsprechende Sachverhalte und Erkenntnisquellen darzustellen (vgl. § 43 Abs. 1 Nr. 1 und 2 Gemeinsame Geschäftsordnung der Bundesministerien). Dies ist vorliegend beim neuen TKG aber nicht geschehen.

Als ein weiteres Beispiel weise ich auf die Regelung des § 170 Abs. 11 TKG (neue Fassung) hin: Diese Vorschrift sieht vor, dass die Betreiber von elektronischen Kommunikationsdiensten sicherstellen müssen, dass eine durch einen anderen europäischen Betreiber veranlasste Verschlüsselung zu dessen Nutzern aufgehoben wird. Erfasst wären somit die verschlüsselten Gespräche. Zu beachten ist zunächst, dass keinesfalls über die Anforderung aus § 8 Abs. 3 TKÜV hinausgegangen werden darf. Wenn ein verschlüsseltes Gespräch unverschlüsselt ausgeleitet werden muss, bedeutet dies automatisch eine Schwächung der Verschlüsselung. Dies bedingt eine Verschlechterung der Datensicherheit. Verschlüsselung ist die Basis für den Schutz der Privatsphäre eines jeden Einzelnen und fast jeder wirtschaftlichen Betätigung in der digitalen Welt. Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist es erforderlich, Daten wirkungsvoll vor Zugriffen Unberechtigter schützen zu können. Der Einsatz von Kryptographie ist hierbei ein ganz elementares Instrument. Ich bewerte jede Form der Senkung des Schutzniveaus kritisch, insbesondere des Kryptoniveaus. Zudem ist zu erwarten, dass es bei den zwischen den Unternehmen zu treffenden Vereinbarungen im Gegenzug dazu kommen wird, dass auch die ausländischen Unternehmen verlangen werden, dass ihnen ein Abhören deutscher Staatsbürgerinnen und Staatsbürger während eines Auslandsaufenthalts ermöglicht wird.

Auch das „Telekommunikation-Telemedien-Datenschutz-Gesetz“ (TTDSG) ist zum 1. Dezember 2021 in Kraft getreten. Dieses enthält die Datenschutzvorschriften, die vormals im TKG zu finden waren sowie Regelungen zu Telemedien aus dem Telemediengesetz (TMG). Erfreulich ist, dass der Gesetzgeber meine Forderung zu Cookies umgesetzt hat. Der neue § 25 TTDSG setzt die ePrivacy-Richtlinie endlich richtlinienkonform um, da das Erfordernis einer Einwilligung als Regelfall im Gesetz normiert ist. Auch bei meinen Zuständigkeiten wurde mehr Klarheit geschaffen. Leider gibt es auch einige Mängel im Gesetz. Dies passiert, wenn ein Gesetzgebungsverfahren „in letzter Minute“ vor Ende der Legislaturperiode kommt. So werden einige Definitionen wie „Teilnehmer“ oder „Nutzer“ nicht durchgängig verwendet und einzelne Querverweise im Gesetz sind fehlerhaft. Ich habe in meinen Stellungnahmen gegenüber dem federführenden Ministerium und dem Parlament mehrfach auf diese Fehler hingewiesen – in manchen Fällen leider vergeblich. Nun musste kurz nach Verkündung des Gesetzes ein Berichtigungsverfahren folgen.

Neu eingeführt werden „Anerkannte Dienste zur Einwilligungsverwaltung“. Hiermit sollen Internetnutzende ihre Einwilligungen z. B. bei Cookies nutzerfreundlich verwalten können. Das TTDSG setzt hierfür nur einen sehr groben Rahmen. Die Details müssen noch in einer Rechtsverordnung festgelegt werden. Erst dann wird sich zeigen, ob dies einen Beitrag zur Eindämmung der „Cookie-Banner“ leisten kann.

5.2 Lobbyregistergesetz

Das Lobbyregistergesetz soll ab 2022 mehr Transparenz über die Interessenvertretung bei Bundestag und Regierung bringen.

Das Gesetz zur Einführung eines Lobbyregisters für die Interessenvertretung gegenüber dem Deutschen Bundestag und gegenüber der Bundesregierung vom 16. April 2021 (Lobbyregistergesetz – LobbyRG) tritt am 1. Januar 2022 in Kraft. Entgegen erster Entwürfe gilt das Gesetz nicht nur für die Interessenvertretung gegenüber dem Deutschen Bundestag, sondern auch gegenüber der Bundesregierung.

Das Gesetz bedeutet einen Fortschritt für die Informationsfreiheit. Die bisherigen Transparenzregelungen des Deutschen Bundestages bezogen sich lediglich auf Interessenverbände und stellten keine verbindlichen Regelungen auf. Auch die Regelungen zum Informationszugang auf Bundesebene, wie das Informationsfreiheitsgesetz (IFG) oder das Umweltinformationsgesetz (UIG), sparen den originär parlamentarischen Bereich bisher aus. Neben einer Registrierungspflicht für einen erweiterten Kreis von Interessenvertretern stellt das neue Gesetz nunmehr bindende Grundsätze für eine integre Interessenvertretung auf.

Die 37. Konferenz der Informationsfreiheitsbeauftragten in Deutschland hatte am 12. Juni 2019 unter meiner Mitwirkung eine Entschließung zur Einrichtung von verpflichtenden Lobbyregistern verabschiedet. Diese grundsätzliche Forderung wurde mit dem Gesetz nunmehr erfüllt. Bestrebungen hinsichtlich weitergehender Regelungen verfolge ich mit Interesse.

5.3 Open-Data-Gesetz

Mit der Verabschiedung des 2. Open-Data-Gesetzes wurde der Anwendungsbereich der Open-Data Regelungen des E-Government-Gesetzes sowohl hinsichtlich der zur Veröffentlichung verpflichteten Stellen, als auch hinsichtlich der zu veröffentlichenden Daten erweitert.

Änderungen bei der Bereitstellung offener Daten

Ziel der Regelungen des Gesetzes zur Änderung des E-Government-Gesetzes und zur Einführung des Gesetzes für die Nutzung von Daten des öffentlichen Sektors (sog. „2. Open-Data-Gesetz“) ist es, den Umfang der von der Bundesverwaltung bereitgestellten offenen Daten zu erweitern. Der Anwendungsbereich des § 12a E-Government-Gesetzes (EGovG) wurde deshalb auf alle Behörden des Bundes mit Ausnahme der Selbstverwaltungskörperschaften erstreckt. Die Bundesbehörden sind grundsätzlich verpflichtet, unbearbeitete maschinenlesbare Daten, die sie zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben erhoben haben, in maschinenlesbarer Form zur Verfügung zu stellen. Eine weitere Neuerung stellt die Verpflichtung der Bundesbehörden dar, eine Stelle zu schaffen, die intern die Identifizierung und Bereitstellung offener Daten koordiniert. Schließlich sind nunmehr auch Forschungsdaten grundsätzlich von der Bereitstellungspflicht erfasst.

§ 12a EGovG sieht indes weiterhin umfangreiche Ausnahme von diesen Regelungen vor. So besteht u. a. für Hauptzollämter oder vergleichbare örtliche Bundesbehörden und die Geheimdienste keine Verpflichtung, eine koordinierende Stelle einzurichten. Ferner sind Beliehene nicht vom Anwendungsbereich der Bereitstellungspflicht erfasst.

Zu meinem Bedauern wurden die Ausnahmen in § 12a EGovG noch erweitert, die Daten von der Bereitstellungspflicht ausnehmen. Im Ergebnis stellen die Ausnahmen einen vertretbaren Kompromiss zwischen dem Interesse an der möglichst weitgehenden Bereitstellung offener Daten und dem Schutz insbesondere personenbezogener oder personenbeziehbarer Daten dar. Es

bleibt abzuwarten, ob die neuen Regelungen auch mit „Leben gefüllt“ werden, und eine aktive und breite Bereitstellung offener Daten erfolgen wird. Die im Gesetz vorgesehene Evaluierung sollte zum Anlass genommen werden, sich einen klaren Überblick über die Umsetzung des Gesetzes zu verschaffen. Insbesondere sollte ggf. die Einführung von Sanktionsmöglichkeiten geprüft werden, um die Verpflichtung zur Datenbereitstellung nachdrücklich zu betonen oder es sollte ein Anspruch auf die Bereitstellung der Daten gesetzlich geregelt werden.

Mit dem Gesetz wurde ferner die neugefasste Richtlinie (EU) 2019/1024 (PSI-Richtlinie) umgesetzt. Das Informationsweiterverwendungsgesetz (IWG) wurde dabei durch das Datennutzungsgesetz (DNG) ersetzt. Das DNG gilt auch für Länder und Kommunen sowie bestimmte öffentliche Unternehmen der Daseinsvorsorge. Es regelt die Weiterverwendung von auf der Grundlage anderer gesetzlicher Regelungen bereitgestellten öffentlichen Daten.

5.3.1 Open-Data-Strategie der Bundesregierung

Die Bundesregierung hat mit ihrer Open-Data-Strategie erstmals Leitlinien für die proaktive Bereitstellung von Verwaltungsdaten definiert. Positiv ist neben der Initiative selbst das ausdrückliche Bekenntnis zum Datenschutz.

Die Open-Data-Strategie der Bundesregierung soll den Rahmen für eine Verbesserung des „Open-Data-Ökosystems“ des Bundes schaffen. Die Bereitstellung offener Daten wird als wichtiges Element für offenes Regierungshandeln beschrieben, das geeignet sei, das Vertrauen in die politischen Institutionen zu stärken. Der Datenbestand der Bundesbehörden solle weiter geöffnet und entgeltfrei zur freien Nutzung zu Verfügung gestellt, der Umfang und die Qualität der bereitgestellten Daten ferner erhöht werden. Schließlich ziele die Open-Data-Strategie auch darauf, eine Bereitstellung offener Daten durch Wirtschaft, Wissenschaft und Zivilgesellschaft zu fördern.

In der Open-Data-Strategie werden sechs Leitlinien formuliert, an denen sich die Maßnahmen zur Bereitstellung und Nutzung offener Daten orientieren sollen. Dabei wird u. a. die Realisierung des wirtschaftlichen Potentials offener Daten, die Verbesserung der Datenkompetenz in der Verwaltung und der Bereitstellung offener Daten sowie eine verantwortungsvolle und gemeinwohlorientierte Nutzung der Daten unter Beachtung von Datenschutz und Datensouveränität betont.

In drei hervorgehobenen Bereichen werden beispielhaft Anwendungsmöglichkeiten dargestellt. Das datengetriebene Wirtschaftswachstum umfasse beispielsweise die Entwicklung von Apps und anderer datenbasierter und anwenderbezogener Lösungen. Die Open-Data-Strategie erwartet hier ein großes Potential für wirtschaftliches Wachstum und die Schaffung von Arbeitsplätzen. Die Nutzung offener Daten stelle ferner eine Möglichkeit für zivilgesellschaftliche und ökologische Initiativen dar, technische Lösungen für bislang nicht berücksichtigte Belange zu finden. Nicht zuletzt seien Effizienzgewinne in der Verwaltung zu erwarten. Der Datenaustausch reduziere bspw. Suchaufwand und lasse mögliche Mehrfacherhebungen entfallen. Auch die Entwicklung digitaler Verwaltungsdienstleistungen könne sich vorteilhaft auf die Steuerlast der Bürgerinnen und Bürger auswirken.

Abschließend werden konkrete Maßnahmen aufgelistet, die drei Handlungsfeldern zugeordnet werden. Teilweise wurden diese Maßnahmen bereits umgesetzt (u. a. Änderungen des § 12a E-Government-Gesetz, siehe Nr. 5.2.) oder sind derzeit in der Umsetzung (z. B. der Aufbau des Kompetenzzentrums Open Data (CCOD) beim Bundesverwaltungsamt).

Ich begrüße die Vorhaben und Initiativen der Open-Data-Strategie und hoffe, dass das Konzept „open by default“ bei mehr und mehr Behörden zur Selbstverständlichkeit wird.

Es freut mich, dass der Aspekt des Datenschutzes ausdrücklich in die Leitlinien aufgenommen wurde. Datenschutz und Open-Data schließen sich nicht aus, sondern ergänzen sich. Ein falsch verstandener Datenschutz sollte nicht dazu verleiten, die Bereitstellung offener Daten vorsorglich zu beschneiden. Datenschutz ist keine Ausrede für mangelnde Offenheit.

Eine Ausweitung der Bereitstellung offener Daten, insbesondere auch über technische Schnittstellen (API), sollte weiter vorangetrieben werden. Wie in der Open-Data-Strategie vorgesehen, könnte auch hier der Austausch mit zivilgesellschaftlichen Initiativen, die schon gezeigt haben, welche Ergebnisse mit einfachen Mitteln zu erreichen sind, sinnvolle Anregungen ergeben.

5.4 Änderungen am Ausländerzentralregistergesetz

Mit dem Gesetz zur Weiterentwicklung des Ausländerzentralregisters soll das Ausländerzentralregister (AZR) zum zentralen Ausländerdateisystem ausgebaut werden. Die Daten für ausländerrechtliche Fachverfahren sollen aktuell und synchron gehalten sowie den befassten Behörden digital zur Verfügung gestellt werden. Doppelte Datenspeicherungen sollen damit künftig vermieden werden.

Speicherung von Dokumenten im Volltext

Mit dem Gesetz zur Weiterentwicklung des Ausländerzentralregisters besteht künftig die Möglichkeit, Dokumente im Volltext im AZR abzuspeichern, wie etwa asyl- und aufenthaltsrechtliche Entscheidungen sowie ausländische Identitätspapiere. Eine Speicherung darf jedoch nur erfolgen, soweit keine besonderen gesetzlichen Verarbeitungsregelungen oder überwiegende schutzwürdige Interessen der ausländischen Person entgegenstehen. Im Rahmen meiner Beteiligung im Gesetzgebungsverfahren habe ich mich kritisch zu der Volltextspeicherung ohne entsprechende technisch-organisatorische Sicherungsmaßnahmen geäußert (s. meine Stellungnahme an den Innenausschuss des Deutschen Bundestages vom 30. April 2021, www.bfdi.bund.de/stellungnahmen). Es hätten Regelungen zur Zugriffsberechtigung und Beschränkungen des Zugriffs auf den Volltext getroffen werden können. Als Reaktion auf meine Kritik hat der Gesetzgeber folgende Lösung favorisiert: Erkenntnisse aus dem Kernbereich persönlicher Lebensgestaltung sind nunmehr in den Dokumenten unkenntlich zu machen. Es wird für mich aufwendig sein zu kontrollieren, ob die entsprechenden Schwärzungen auch in angemessener Weise vorgenommen werden.

Speicherung ausländischer Personenidentitätsnummer

Entgegen meiner Kritik ist im Gesetz die Speicherung ausländischer Personenidentitätsnummern aufgenommen worden. Bei diesen handelt es sich um lebenslänglich unveränderliche Personenkennzeichen, die in vielen Staaten vergeben werden. Das Erfordernis dieses Speicherdatums im AZR ist meiner Auffassung nach nicht überzeugend begründet worden. Es erfolgte im Laufe des Gesetzgebungsprozesses zumindest eine Klarstellung, dass die von der Registerbehörde übermittelte ausländische Personenidentifikationsnummer nur zum Zweck der eindeutigen Identifizierung einer Person genutzt werden darf.

Ich freue mich darüber, dass der Gesetzgeber einige meiner Hinweise aufgegriffen und den Gesetzentwurf ab geändert hat. Wie die praktische Umsetzung im Bereich der Bundesbehörden erfolgt, werde ich bei künftigen Kontrollen in den Blick nehmen.

5.5 Bundespolizeigesetz

Das Bundespolizeigesetz (BPolG) wurde nach wie vor nicht an die zwingenden europarechtlichen Vorgaben der JI-Richtlinie angepasst. Ein Entwurf der damaligen Regierungsfraktionen im Deutschen Bundestag, der dem Europarecht allenfalls in Teilen Rechnung getragen, gleichzeitig aber verfassungsrechtlich problematische neue Eingriffsbefugnisse für die Bundespolizei geschaffen hätte, scheiterte im Bundesrat.

Bereits in meinem 29. Tätigkeitsbericht habe ich darüber berichtet, dass die zwingenden europarechtlichen Vorgaben beim BPolG noch nicht umgesetzt wurden, obwohl dies bis zum 6. Mai 2018 hätte erfolgen müssen (vgl. 29. TB Nr. 6.7). Die damaligen Regierungsfraktionen haben dann im letzten Jahr einen eigenen Änderungsentwurf im Bundestag eingebracht. Bei dieser Initiative aus der Mitte des Parlaments, die auf Formulierungshilfen aus der Bundesregierung beruhte, fand zuvor keine formale Ressortbefassung im Kreis der Bundesregierung statt, in die ich eingebunden worden wäre. Meine datenschutzrechtlichen Bedenken konnte ich daher erst spät bei der Anhörung des Gesetzentwurfs gegenüber dem Ausschuss für Inneres und Heimat einbringen.

Dem Ausschuss gegenüber habe ich deutlich gemacht, dass ich die Erweiterung der Befugnisse der Bundespolizei für verfassungsrechtlich bedenklich halte, weil es sich bei der Bundespolizei um eine Sonderpolizei mit begrenztem Aufgabenspektrum für Bahnhöfe, Flughäfen und die Landesgrenzen handelt; im Übrigen liegt die Zuständigkeit bei den Ländern. Auch die im Entwurf vorgesehene Ermächtigung zur präventiven Überwachung der Telekommunikation und vor allem die Möglichkeit einer sog. „Quellen-TKÜ“ halte ich für sehr problematisch. Für Letztere müssten gezielt offengehaltene Sicherheitslücken ausgenutzt werden, was im Ergebnis das Sicherheitsniveau für digitale Kommunikation senkt.

Die europarechtlichen Vorgaben zu den Aufsichtsbefugnissen der Datenschutzbehörden wurden überdies im Entwurf nur zum Teil umgesetzt. Damit wären mir unnötige Hürden für die Ausübung meiner Datenschutzkontrolle auferlegt worden.

Da der Entwurf letztlich im Bundesrat am Votum der Länder gescheitert ist, bleibt abzuwarten, wie das BPolG in der neuen Legislaturperiode überarbeitet wird.

5.6 Änderungen am BND-Gesetz treten in Kraft

An den ursprünglichen Vorschlägen der Bundesregierung zur Umsetzung verfassungsgerichtlicher Vorgaben im BND-Gesetz haben die Koalitionsfraktionen im Laufe des parlamentarischen Beratungsverfahrens schlussendlich nur marginale Änderungen vorgenommen. Das im Großteil zum 1. Januar 2022 in Kraft tretende Gesetz bringt somit allenfalls strukturelle Anpassungen in der Kontrolllandschaft über den Bundesnachrichtendienst.

Der Bundestag hat am 25. März 2021 Gesetzesänderungen am bestehenden BND-Gesetz mit der Zielrichtung der Umsetzung der Vorgaben des Bundesverfassungsgerichts vom 19. Mai 2020 (Az. 1 BvR 2835/17) sowie des Bundesverwaltungsgerichts vom 13. Dezember 2017 (Az. BVerwG 6 A 6.16 und 6 A 7.16) beschlossen. Bereits am 26. März 2021 hat der Bundesrat das Gesetz gebilligt. Die ersten Vorschriften insbesondere zum Unabhängigen Kontrollrat sind bereits zum 22. April 2021 in Kraft getreten. Die weiteren Vorschriften treten zum 1. Januar 2022 in Kraft.

Mit Änderungsantrag der Fraktionen CDU/CSU und SPD, der nach der Sachverständigenanhörung im Innenausschuss vorgelegt wurde, gab es im Ergebnis lediglich einige wenige materiell-rechtliche Änderungen am BND-Gesetz. Hervorzuheben sind die leichte Erhöhung der Eingriffsschwellen für die gezielte Erhebung von Daten aus Vertraulichkeitsbeziehungen im Wege der strategischen Ausland-Fernmeldeaufklärung und des Eingriffs in informationstechnische Systeme. Danach ist nun ein Eingriff in jene Vertraulichkeitsbeziehungen möglich, wenn Tatsachen die Annahme eines Verdachts rechtfertigen, dass gewisse Straftaten oder Gefahren vorliegen. Ergänzend wurde eine Dokumentationspflicht über die Feststellung der Zugehörigkeit von Personen zum geschützten Personenkreis von Vertraulichkeitsbeziehungen vorgesehen. Zu diesem Kreis zählen laut BND-Gesetz Geistliche, Verteidiger, Rechtsanwälte und Journalisten, deren Vertraulichkeitsbeziehung dem Schutz des § 53 Abs. 1 S. 1 Nr. 1, 2, 3 und 5 sowie S. 2 der Strafprozessordnung unterfallen würde.

Im Übrigen bleibt es bei strukturellen Anpassungen in der Kontrolllandschaft über den Bundesnachrichtendienst. Das Parlamentarische Kontrollgremium wurde durch den Änderungsantrag in das Zentrum verschiedener Informationsflüsse zwischen den Kontrollorganen gerückt. Ein von mir befürworteter inhaltsbezogener Austausch jedenfalls zwischen der G10-Kommission, dem Unabhängigen Kontrollrat und meiner Behörde wurde nicht vorgesehen.

Trotz einiger Anpassungen bleibt meine Kritik, die ich im Lauf des BND-Gesetzgebungsverfahrens geäußert habe, weitestgehend bestehen. Hierzu verweise ich auf meine öffentlich zugängliche Stellungnahme an den Ausschuss für Inneres und Heimat des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung zur Änderung des BND-Gesetzes vom 18. Dezember 2020, s. www.bfdi.bund.de/stellungnahmen

5.7 Evaluierung des BDSG

Die Stellungnahme der DSK zur vom BMI durchgeführten Evaluierung des Bundesdatenschutzgesetzes (BDSG) hat punktuellen gesetzgeberischen Handlungsbedarf aufgezeigt. Dies gilt etwa für die Regelung zum Beschäftigtendatenschutz und zu den Durchsetzungsbefugnissen des BfDI sowohl im Anwendungsbereich der DSGVO, als auch im Anwendungsbereich der JI-Richtlinie sowie gegenüber den Geheimdiensten.

Das BMI führte im Berichtszeitraum entsprechend des Auftrags aus der Gesetzbegründung eine Evaluierung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs-und Umsetzungsgesetz EU – DSAnpUG-EU2) durch. Kernstück dieses Gesetzes ist das neue, an die europarechtlichen Vorgaben aus DSGVO und JI-Richtlinie angepasste BDSG.

Zwar ergeben sich die wesentlichen datenschutzrechtlichen Regelungen im Anwendungsbereich der DSGVO unmittelbar und EU-weit einheitlich aus dieser Verordnung. Das BDSG enthält aber Präzisierungen bzw. Modifikationen, die sich auf Öffnungsklauseln in der DSGVO stützen. Im Bereich Polizei und Justiz dient das BDSG der Umsetzung der entsprechenden Richtlinie (JI-Richtlinie). Auch hier ergeben sich die wesentlichen materiellen Regelungen aus der europarechtlichen Grundlage, die allerdings nur eine Mindestharmonisierung vorsieht.

Die deutschen Aufsichtsbehörden wurden vom BMI im Rahmen der Evaluierung des BDSG beteiligt und haben eine umfangreiche Stellungnahme abgegeben[15]. Einige wesentliche Punkte der DSK-Stellungnahme sind:

15 Stellungnahme der DSK zur Evaluierung des BDSG vom 02.03.21, abrufbar unter https://www.datenschutzkonferenz-online.de/stellungnahmen.html

- Das BDSG zeigt sich hinsichtlich der Rechtsgrundlagen für die Verarbeitung sowie die Weiterverarbeitung personenbezogener Daten und der Vorschrift des § 29 BDSG über die Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten als teilweise unionsrechtswidrig (§ 4 Abs. 1 S. 1 Nr. 3, § 23 Abs. 1 Nr. 2 und § 29 Abs. 3 S. 1 BDSG) und in weiten Teilen als wenig normenklar und zu unbestimmt.
- § 26 BDSG wird in seiner aktuellen Fassung seiner Aufgabe im Beschäftigtendatenschutz nicht gerecht. In der Praxis resultieren aus dem weiten Interpretationsspielraum für alle Beteiligten Unklarheiten. Um den besonderen Herausforderungen des Schutzes der datenschutzrechtlichen Grundrechtsposition im Beschäftigtendatenschutz gerecht zu werden, müssten diese normenklarer geregelt werden (vgl. oben 4.3).
- Die Anhebung des Schwellenwerts in § 38 Abs. 1 BDSG zur Benennung von Datenschutzbeauftragten auf 20 Beschäftigte hat weder eine Entbürokratisierung, noch eine sonstige Entlastung von Unternehmen und Vereinen erreicht. Es traten vielmehr gegenteilige Effekte ein (vgl. 28. TB Nr. 5.1).
- Mit einigen Einschränkungen der Betroffenenrechte in den §§ 32 bis 37 wird das BDSG den europarechtlichen Vorgaben nicht gerecht und stellt bestehende datenschutzrechtliche Standards in Frage. Die Rechte der betroffenen Personen (Information, Auskunft, Löschung, Widerspruch, automatisierte Einzelentscheidung/Profiling) werden in unzulässigem Maße eingeschränkt.
- Es ist dringend erforderlich, die aufsichtsbehördlichen Befugnisse im BDSG zu erweitern, indem gegenüber öffentlichen Stellen die Durchsetzung von Maßnahmen mit Zwangsmitteln sowie die Anordnung der sofortigen Vollziehung ermöglicht wird.
- Auch bleibt der BfDI im Bereich der JI-RL sowie außerhalb des Geltungsbereichs des EU-Rechts auf das Instrument der Warnung und der Beanstandung beschränkt, jedenfalls soweit weiterreichende Befugnisse nicht in spezifischen Vorschriften des Polizeirechts geregelt sind. Art. 47 Abs. 2 JI-RL enthält hingegen die Verpflichtung wirksame Abhilfebefugnisse zu gewähren. Diese Anforderung erfüllt die Regelung im BDSG nicht. Die nach wie vor nicht abgeschlossene Umsetzung im Fachrecht zeigt deutlich, dass die wirksamen Abhilfebefugnisse für den JI-Bereich ein heitlich im BDSG geregelt werden sollten. Ich fordere auch für den nachrichtendienstlichen Bereich aus den genannten Gründen schon seit längerer Zeit Abhilfe- und Sanktionsbefugnisse vergleichbar denen der DSGVO bzw. der JI-RL (vgl. 27.TB Nr. 1.2.1).

In einer ergänzenden Stellungnahme habe ich mich zudem dafür ausgesprochen, im Gesetzestext zu § 18 BDSG klarzustellen, dass es eines gemeinsamen Standpunkts der deutschen Aufsichtsbehörden in europäischen Angelegenheiten bereits im Kooperationsverfahren (Art. 60 ff DSGVO) und nicht erst im Kohärenzverfahren (Art. 63 ff.) bedarf. Die deutschen Aufsichtsbehörden sollten auf europäischer Ebene immer mit einer Stimme sprechen, um europäische Meinungsbildungsprozesse zu beschleunigen und deutsche Positionen dort besser vertreten zu können. Dies wird von einem Teil der Aufsichtsbehörden der Länder anders gesehen.

Das BMI hat seinen Bericht zur Evaluierung des BDSG im Oktober 2021 veröffentlicht.[16] Dabei werden die Ausführungen der deutschen Aufsichtsbehörden umfänglich erwähnt, in den Schlussfolgerungen aber leider nur teilweise aufgegriffen. Ich werde mich in der begonnenen Legislaturperiode weiter für die oben dargestellten Änderungen im BDSG einsetzen.

Ich empfehle der Bundesregierung, die im Koalitionsvertrag angekündigte Institutionalisierung der DSK und die verbesserte verbindliche Kooperation der deutschen Datenschutzaufsichtsbehörden durch die entsprechenden gesetzgeberischen Maßnahmen alsbald in Angriff zu nehmen.

16 Abrufbar unter https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/downloads/berichte/evaluierung-bdsg.pdf

5.8 IT-Sicherheitsgesetz

Mit dem IT-Sicherheitsgesetz 2.0 wurden viele neue Aufgaben und Befugnisse für das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingeführt. In einer Dialogreihe arbeiten das BSI und mein Haus gemeinsam an ihrer datenschutzkonformen Implementierung.

Am 27. Mai 2021 wurde das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" – oder kürzer das IT-Sicherheitsgesetz 2.0 – im Bundesgesetzblatt veröffentlicht. Ihm voraus ging ein langwieriges Gesetzgebungsverfahren von rund zwei Jahren, das trotz dieser Dauer von unangemessen kurzen Stellungnahmefristen geprägt war.

Viele meiner Hinweise wurden im Gesetzgebungsverfahren aufgegriffen und umgesetzt. Einige wichtige Forderungen wurden aber leider nicht übernommen: beispielsweise wurde mein klares Plädoyer gegen eine Ausweitung der Speicherung von sog. Protokolldaten von 3 auf 12 Monate nicht nur verworfen, sondern im Gegenteil sogar auf 18 Monate ausgeweitet. Dies wirft aus meiner Sicht ganz erhebliche Fragen der Verhältnismäßigkeit auf.

Für das BSI führt das IT-Sicherheitsgesetz zu einem erheblichen Verantwortungs- und Aufgabenzuwachs.[17] In gleicher Weise steigt auch der Mehraufwand meines Hauses für die datenschutzrechtliche Beratung und Kontrolle des BSI.

Mir war wichtig, das BSI bei der Umsetzung der neuen Vorgaben des IT-Sicherheitsgesetzes 2.0 von Anfang an proaktiv zu begleiten. Nach dem Credo: „Datenschutz von Anfang an" haben wir hierfür einen sehr erfolgreichen gemeinsamen Dialogprozess initiiert, um alle neuen Prozesse und Systeme des BSI direkt in ihrer Entwicklung datenschutzkonform auszugestalten und die Zusammenarbeit zwischen beiden Häusern bestmöglich zu operationalisieren.

5.9 EU Digitalgesetzgebung

Die EU-Kommission hat mit ihren Verordnungsvorschlägen zur Regulierung des europäischen Binnenmarkts für Daten weitere Schritte zu einem EU-weiten Regelwerk für den Digitalen Raum vorgelegt. Der BfDI begleitet die Verhandlungen zu den einzelnen Rechtsakten sowohl national im Rahmen von Ressortabstimmungen als auch durch Initiativen im Europäischen Datenschutzausschuss (EDSA).

Aufbauend auf ihrer Ende 2020 veröffentlichten Datenstrategie (COM/2020/66 final) hat die EU-Kommission im Berichtszeitraum mehrere Verordnungsvorschläge vorgelegt, die einen „einheitlichen Rechtsrahmen für Datenzugang und verantwortungsvolle Datennutzung" in der EU bilden sollen. Im Kern handelt es sich dabei um zwei Rechtsakte mit dem Ziel der Regulierung von bestehenden großen Datenplattformen sowie um Rechtsakte zur Förderung des Datenzugangs und des Datenaustauschs. Das Legislativpaket Digitale Dienste mit der Verordnung über digitale Dienste (Digital Services Act, DSA) und der Verordnung über digitale Märkte (Digital Markets Act, DMA) legt grundlegende Regeln für digitale Dienste fest, die auf ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld und faire Märkte für diese Dienste in der EU abzielen. Die Verordnung über Daten-Governance (Data Governance Act, DGA) hat zum Ziel, die Verfügbarkeit von Daten öffentlicher Stellen für Forschung und Wirtschaft in der EU zu erhöhen, sog. Datenmittler zu etablieren und Mechanismen für gemeinsame gemeinwohlbezogene Datennutzungen zu fördern.

Insbesondere der DGA soll Ende 2021 um den Entwurf des sog. Data Act (DA) ergänzt werden. Zu diesem geplanten Rechtsakt hat die EU-Kommission im Mai 2021 eine Folgenabschätzung (Inception Impact Assessment) veröffentlicht[18]. Daraus wird erkennbar, dass möglicherweise konkrete Zugangsrechte zu Daten, auch personenbezogenen Daten, geschaffen werden könnten, um sog. Datenmärkte zu fördern. Deutlich wird sowohl bei DGA als auch DA, dass im Mittelpunkt der Anstrengungen des EU-Gesetzgebers verbesserte Rahmenbedingungen für digitale Geschäftsmodelle und Verarbeitungsformen sowie zugleich der Datenanalyse durch sog. Künstlichen Intelligenz (KI) stehen. Beide Verarbeitungsformen stellen allerdings das bisherige Schutzkonzept des Datenschutzes vor erhebliche Herausforderungen. Umso mehr gilt es, diese geplanten Rahmenregelungen für sog.

17 Kerninhalte des Gesetzes können abgerufen werden unter https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

18 vgl. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en

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.

Die EU-Kommission betrachtet zwar die seit 2018 geltende DSGVO dabei als ersten Schritt auf dem Weg, für einen „soliden Rahmen für Vertrauen im digitalen Umfeld" zu sorgen. Sie soll von den neuen Rechtsakten unberührt bleiben. Es bestehen aber viele Unklarheiten im Verhältnis zur und in den Auswirkungen auf die DSGVO. Die Rechtsakte haben weitere Schnittstellen, die sich auf den Datenschutz in der EU insgesamt ganz erheblich auswirken werden. Ziel meiner Beratung ist es, auf diese Problempunkte hinzuweisen und auf eine möglichst datenschutzfreundliche Regulierung hinzuwirken. Dabei gilt es im Blick zu behalten, ob und inwieweit aus diesen neuen, weitreichenden EU-Rechtsakten auch weiterer gesetzlicher Regelungsbedarf zum Schutz der Datenschutzrechte der Bürgerinnen und Bürger erwachsen könnte.

DGA

Der DGA verfolgt in drei unterscheidbaren Handlungsfeldern die Schaffung von Rahmenbedingungen für eine sog. Datenökonomie.

Erstens werden Voraussetzungen für die Weitergabe von Daten durch öffentliche Stellen zur allgemeinen Nutzung (Open Data) geschaffen. Zukünftig sollen Behörden u. a. auch personenbezogene Daten etwa zur kommerziellen Weiterverwendung freigeben, das Konzept von Open Data erfährt damit eine erhebliche Ausweitung. Die Schaffung von Rechtsgrundlagen für die zulässige Weitergabe soll allerdings den Mitgliedstaaten überlassen und die DSGVO insgesamt unberührt bleiben.

Zweitens werden Dienste für die gemeinsame Datennutzung, sog. Datenintermediäre oder Datenmittler, definiert. Entsprechende Dienste sollen unter neutraler Vermittlung Datenanbieter und Datennutzer zusammenbringen. Für den Bereich der sog. PIMS (Personal Information Management Systems), also Dienstleistern zur Unterstützung von Bürgern bei der Ausübung ihrer Datenschutzrechte, werden in diesem Kontext Potentiale für eine Weiterentwicklung des Datenschutzes gesehen. Insgesamt bleibt in der Diskussion noch weitgehend offen, unter welchen Voraussetzungen solche Datenmittler für welche Zwecke tätig werden dürfen. Erst die nähere Ausgestaltung wird eine konkrete Bewertung erlauben. Den Risiken der Entwicklung eines nach Datenschut
zgrundsätzen unzulässigen Handels mit auch personenbezogenen Datenbeständen via Datenmittler muss entgegengetreten werden.

Drittens werden Rahmenbedingungen geschaffen, die Mitgliedstaaten zur Schaffung von sog. datenaltruistischen 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, hergeben. Auch hier gilt es, die Wahrung der Datenschutzgrundsätze bei der gesetzlichen Ausgestaltung sicherzustellen. Bei allen Regelungsansätzen stellt sich das Problem, dass neben der Datenschutzaufsicht eine eigene Aufsichtsstruktur geschaffen werden soll, obwohl in der Sache überlappende Zuständigkeiten bestehen werden.

Hierzu sowie zu weiteren kritischen Punkten habe ich gemeinsam mit meinen europäischen Kolleginnen und Kollegen und dem Europäischen Datenschutzbeauftragten (EDPS) im EDSA eine umfängliche Stellungnahme verfasst[19].

DSA

Der DSA definiert neu, welche Rechte und Pflichten Anbieter von Inhalten im Internet haben. Er legt Sorgfaltspflichten zu Inhaltsbeschränkungen und illegalen Inhalten fest und schafft Transparenz für Verbraucher im Hinblick auf Online-Kauf, Werbung und Empfehlungssysteme. Ich hätte mir, insbesondere im Hinblick auf personalisierte Werbung, ein mutigeres Vorgehen gewünscht und setze mich für ein Verbot von bestimmten Tracking- und Profilingpraktiken ein. Da bei der Umsetzung des DSA häufig auch Datenschutzfragen zu beantworten sind, z. B. beim vorgesehenen Zugriff von Forschenden auf Daten großer Online-Plattformen, sind die Datenschutzaufsichtsbehörden sowohl auf nationaler als auch auf europäischer Ebene zwingend einzubeziehen.

DMA

Der DMA verfolgt als allgemeines Ziel die wettbewerbsrechtliche Fairness und Bestreitbarkeit im digitalen Sektor und ist im Speziellen auf die Regulierung der großen zentralen Plattformdienste gerichtet. Er soll das grundsätzlich erst nach einer Rechtsverletzung greifende Wettbewerbsrecht gegenüber den großen Anbietern zentraler Plattformdienste durch eine ex ante Regulierung ergänzen. Erfüllt ein zentraler Plattformdienst die durch den DMA vorgegebenen Kriterien zur Einstu

19 Stellungnahme 03/2021, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_de.

fung als sog. Gatekeeper, werden ihm durch den DMA zusätzliche Verhaltenspflichten auferlegt, um unlautere Praktiken zu verhindern. Diese Verhaltenspflichten enthalten auch datenschutzrelevante Vorgaben, wie das Verbot, personenbezogene Daten mit solchen aus Drittdiensten oder mehreren von einem Unternehmen betriebenen zentralen Plattformen zusammenzuführen, wenn keine wirksame Einwilligung nach der DSGVO vorliegt. Zur effizienten und effektiven Durchsetzung der Regelungen gegenüber den Gatekeepern ist es unabdingbare Voraussetzung, dass für eine Kooperation zwischen der Vollzugsbehörde und den Datenschutzaufsichtsbehörden entsprechende Regelungen im DMA vorgesehen werden. Dabei setze ich mich dafür ein, dass EDSA und EDPS ebenfalls in diese Kooperation mit einbezogen werden. Des Weiteren stelle ich im Rahmen meiner Beratung sicher, dass bei Bezugnahmen auf datenschutzrechtliche Verpflichtungen im DMA das Schutzniveaus der DSGVO erhalten wird.

Fazit

Vor dem Hintergrund der vorliegenden Entwürfe zu DGA, DMA und DSA sowie dem Verlauf der bisherigen Verhandlungen der Mitgliedstaaten sowie des Europäischen Parlaments zu diesen Gesetzesakten habe ich als Ko-Berichterstatter die Initiative meines niederländischen Kollegen unterstützt, in der gemeinsamen Stellungnahme des EDSA vom 18. November 2021 alle drei Rechtsakte betreffende, übergreifende Kritikpunkte zu benennen und zu bündeln[20].

5.10 Entwicklungen bei Gesundheitsregistern

Bei der Umsetzung gesetzlicher Regelungen in die Praxis liegt die Tücke oft im Detail. Beim Organspenderregister betraf dies die Authentifizierung. Und auch beim Implantateregister war es nicht einfach, Betriebsverordnung und Bereitstellung der nötigen Serverkapazitäten mit den gesetzlichen Vorgaben in Einklang zu bringen. Beim Zentrum für Krebsregisterdaten lässt die Nutzung des erheblich erweiterten Datensatzes auch kommerzielle Forschung zu. Bei einem Antrag auf Datennutzung hat der neue wissenschaftliche Ausschuss u. a. das Reidentifikationsrisiko zu bewerten.

Organ- und Gewebespenderegister (OGR)

Im letzten Jahr hatte ich bereits das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) bei der technischen Umsetzung der Regelungen zum Online-Register zur Dokumentation der Erklärung zur Organspende beraten (29. TB, Nr. 7.3). Das Register soll im März 2022 den Betrieb aufnehmen. Im Berichtszeitraum ergab sich eine Vielzahl weiterer Einzelfragen, mit denen die Bundesdruckerei als Auftragsverarbeiter für das BfArM auf mich zukam.

Im Gesetz ist vorgesehen, dass die Erklärung in Pass- und Ausweisstellen, also etwa in den kommunalen Bürgerservicebüros, abgegeben werden kann. Hierzu sollten dort aufgestellte Terminals dienen. Dies erschien dann in der Praxis allerdings als zu aufwändig. Infolgedessen kann sich die erklärende Person dort demnächst lediglich authentifizieren. Sie erhält dann eine Nummer, unter der sie sich beim Registerportal anmelden und die eigentliche Erklärung abgeben kann. Dies halte ich für datenschutzrechtlich zulässig, weil die Authentifizierung als Teil der ursprünglich vorgesehenen Erklärungsabgabe auf gesetzlicher Grundlage beruht („Minus“). Eine Authentifizierung mittels AlVi, der alternativen Versichertenidentität (die ohne Verwendung der elektronischen Gesundheitskarte auskommt), hielt ich dagegen nicht für zulässig. Dieses Verfahren hat nur einen eng begrenzten Anwendungsbereich. Es betrifft allein die Anwendungen elektronische Patientenakte, elektronischer Medikationsplan und elektronische Patientenkurzakte. Für die „kartenfreie“ Authentifizierung der Versicherten zum Organspenderregister kommt daher nur die sog. Digitale Identität nach § 291 Abs. 8 SGB V in Betracht, die ab 2023 zur Verfügung stehen soll. Daneben ist die Authentifizierung mit der online-Funktion des Personalausweises möglich.

20 Statement on the Digital Services Package and Data Strategy, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-digital-services-package-and-data-strategy_en

Der Datensatz im Organspenderregister soll die Angaben des Organspendeausweises im Kartenformat abbilden. Da mir mitgeteilt wurde, dass auf dem Freitextfeld der Ausweiskarte oft Vorerkrankungen eingetragen werden, war ein weiteres Problem der Schutzbedarf dieser Daten. Bisher waren die Angaben zum OGR nicht als besonders schützenswerte Daten angesehen worden. Um zu verhindern, dass sich durch den Eintrag von solchen Gesundheitsdaten die Schutzkategorie und damit der technische Aufwand erhöht, habe ich empfohlen, ganz auf das Feld zu verzichten oder statt des Freitextfeldes häufige Einträge ohne Gesundheitsinformationen zur Auswahl anzubieten.

Implantateregister

Beim Implantateregister befasste ich mich vorrangig mit den Hostingdienstleistern der Registerstelle und der Vertrauensstelle. Die mit dem Hosting betrauten Einrichtungen stellen Serverkapazitäten bereit und übernehmen die Datenverarbeitung. Das BMG hatte für die bei ihm angesiedelte Registerstelle die D-Trust GmbH der Bundesdruckerei mit dem Hosting beauftragt. Das Robert Koch-Institut (RKI) war für die bei ihm angesiedelte Vertrauensstelle noch auf der Suche nach einem Hoster, der an die zur Übermittlung verwendete Telematikinfrastrukur (TI) angeschlossen werden konnte. Im Gesetz ist vorgesehen, dass die Vertrauensstelle von der Registerstelle getrennt sein muss. Das bedingt zugleich voneinander verschiedene Stellen, die das Hosting übernehmen. Es gibt jedoch wenige Anbieter mit genügend freien Serverkapazitäten, welche die strengen Sicherheitsanforderungen erfüllen können, die sich hier aus der Schutzkategorie und der enormen Menge der Daten ergeben. Daher wurde ich mehrfach gefragt, inwieweit Abstriche von den Anforderungen möglich wären, um den planmäßigen Start des Registers nicht zu gefährden. Auch stand ein mögliches Hosting der Vertrauensstelle bei der Bundesdruckerei GmbH, dem Mutterkonzern der D-Trust GmbH, bei der bereits die Registerstelle gehostet wurde, zur Diskussion. Hiervor konnte ich nur warnen: Bei einem so umfangreichen Register ist das Einhalten der Datenschutzvorgaben unabdingbare Grundlage für das Vertrauen der Betroffenen. Letztlich wurde erfreulicherweise eine Lösung gefunden, die Aufträge datenschutzkonform zu vergeben.

Ein weiteres Thema der Beratung waren die Datenflüsse zwischen den Beteiligten. Erste Ablaufpläne entsprachen nicht den Vorgaben im Implantateregistergesetz. Noch vor Abschluss dieser Beratungen erreichte mich überraschend bereits der Entwurf der Implantateregister-Betriebsverordnung, der einige Punkte enthielt, die noch Gegenstand der Diskussion waren. Unter anderem konnte ich den direkten Datenaustausch zwischen Register und Krankenhaus unter Verwendung eines Datensatzidentifikators verhindern. Der Datensatzidentifikator ist als personenbezogenes Datum einzuordnen, eine Übermittlung daher nur unter Einbindung der Vertrauensstelle zulässig. Schließlich bot das vorgesehene Abrufverfahren bei den Krankenkassen Anlass zur Kritik. Im Gesetz ist vorgesehen, dass die Krankenkassen für ihre Versicherten Änderungen mitteilen (Wechsel der Krankenkasse, Versterben etc.). Laut Verordnungsentwurf sollte das Register jedoch von sich aus turnusmäßig Abfragen bei allen Krankenkassen starten. Hier konnte ich erreichen, dass die Meldung durch die Krankenkassen den Regelfall darstellt und die von der Registerstelle initiierte Abfrage auf besonderen Fälle beschränkt bleibt. Unverändert ist die Registerstelle beim BMG angesiedelt, obwohl dies keine geeignete Registerbehörde ist, wie sich auch der Gesetzesbegründung entnehmen lässt. Dies ist nur so lange unproblematisch, wie der eigentliche Registerbetrieb noch nicht angelaufen ist. Ich werde die Situation beobachten und habe dem BMG dringend empfohlen, zeitnah eine geeignete Behörde vorzusehen, die den Registerbetrieb dauerhaft rechtssicher und datenschutzkonform übernehmen kann.

Zentrum für Krebsregisterdaten

Über Pläne zur Ausweitung des beim Zentrum für Krebsregisterdaten (ZfKD) beim RKI vorgehaltenen Datensatzes hatte ich bereits berichtet (29. TB Nr. 7.3 S. 69). Für mich kritisch war der große Kreis der Zugangsberechtigten, da auf Antrag auch Private, also auch Unternehmen der Pharmaindustrie, Zugang erhalten. In der Ressortabstimmung konnte ich allerdings erreichen, dass neben dem Beirat auch ein wissenschaftlicher Ausschuss an der Entscheidung über den Antrag beteiligt ist. Da dieser unter anderem das Reidentifikationsrisiko prüft, sollen ihm auch Datenschutz-Sachverständige angehören.

Weitere Regelungen waren jenen für das Forschungsdatenzentrum beim BfArM in § 303e SGB V angelehnt: vorrangig werden anonymisierte Daten übermittelt, der Zugang zu pseudonymisierten Datensätzen ist nur unter Kontrolle des Zentrums für Krebsregisterdaten zulässig, Fehlverhalten wird sanktioniert und bewilligte Anträge werden in einem Verzeichnis veröffentlicht. Das Gesetz trat Ende August in Kraft (Gesetz zur Zusammenführung von Krebsregisterdaten vom 18. August 2021, BGBl. I, S. 3890). Ich werde die Antragsbearbeitung im Blick behalten, um sicherzustellen, dass trotz der Zugangsberechtigung für kommerzielle Forschung der Schutz der Betroffenen gewahrt bleibt.

Ich empfehle dem BMG für den Betrieb des Implantateregisters eine geeignete Behörde vorzusehen – und gegebenenfalls zu schaffen –, die den Registerbetrieb dauerhaft rechtssicher und datenschutzkonform ohne Interessenkonflikte übernehmen kann.

5.11 Datenerhebungsbefugnisse der Krankenkassen im Krankengeldfallmanagement

Mit dem Gesetz zur Weiterentwicklung der Gesundheitsversorgung (Gesundheitsversorgungsweiterentwicklungsgesetz – GVWG) hat der Gesetzgeber klargestellt, dass der Datenerhebungsbefugnis der Krankenkassen bei der Prüfung, ob ein Gutachten des Medizinischen Dienstes (MD) beauftragt werden soll, Grenzen gesetzt sind. Meine seit Jahren vertretene Rechtsauffassung wurde damit bestätigt.

In meinem 29. TB (Nr. 7.15) hatte ich darüber berichtet, dass in Gesprächen mit dem GKV-Spitzenverband und dem Bundesministerium für Gesundheit (BMG) noch immer kein Konsens über den Umfang der Datenerhebungsbefugnisse der Krankenkassen vor der Beauftragung des MD zur Prüfung der Arbeitsunfähigkeit erzielt werden konnte. Nunmehr hat der Gesetzgeber mit einer Ergänzung des § 275 SGB V durch das am 20. Juli 2021 in Kraft getretene GVWG meine seit Jahren vertretene restriktive Rechtsauffassung zu den Datenerhebungsbefugnissen der Krankenkassen bestätigt.

Der neu eingefügte Abs. 1b konkretisiert die Datenerhebungsbefugnisse im Vorfeld einer MD-Beauftragung und beschränkt sie durch eine abschließende Aufzählung. So dürfen Krankenkassen für den Zweck der Feststellung, ob bei Arbeitsunfähigkeit eine gutachtliche Stellungnahme des MD einzuholen ist, im jeweils erforderlichen Umfang grundsätzlich nur die bereits nach § 284 Abs. 1 SGB V rechtmäßig erhobenen und damit bereits vorliegenden versichertenbezogenen Daten verarbeiten. Sollte die Verarbeitung bereits bei den Krankenkassen vorhandener Daten für die Beurteilung, ob der MD zur Prüfung der Arbeitsunfähigkeit eingeschaltet werden soll, nicht ausreichen, dürfen die Krankenkassen gemäß § 275 Abs. 1b S. 2 SGB V abweichend vom oben Ausgeführten bei den Versicherten nur versichertenbezogene Angaben

- dazu, ob eine Wiederaufnahme der Arbeit absehbar ist und gegebenenfalls zu welchem Zeitpunkt eine Wiederaufnahme der Arbeit voraussichtlich erfolgt, und
- zu konkret bevorstehenden diagnostischen und therapeutischen Maßnahmen, die einer Wiederaufnahme der Arbeit entgegenstehen,

im jeweils erforderlichen Umfang erheben und verarbeiten.

Auch auf meine erheblichen datenschutzrechtlichen Bedenken im Hinblick auf die von diversen Krankenkassen praktizierten telefonischen Versichertenanfragen, die teilweise unzulässige Fragen nach gesundheitlichen, sozialen oder familiären Problemen beinhalteten und unzulässigen Druck auf arbeitsunfähige Versicherte ausübten (vgl. ebenfalls 29. TB, Nr. 7.15), hat der Gesetzgeber reagiert. Nach § 275 Abs. 1b S. 3 SGB V dürfen Krankenkassen die oben genannten zulässigen Angaben nach einer absehbaren Arbeitswiederaufnahme sowie konkret bevorstehenden diagnostischen und therapeutischen Maßnahmen bei den Versicherten grundsätzlich nur schriftlich oder elektronisch erheben. Eine telefonische Erhebung ist nur zulässig, wenn die Versicherten in die telefonische Erhebung zuvor schriftlich oder elektronisch eingewilligt haben. Die Krankenkassen haben jede telefonische Erhebung beim Versicherten zu protokollieren. Hierauf und insbesondere auf das Auskunftsrecht nach Art. 15 DSGVO sind die Versicherten hinzuweisen.

Ich begrüße die gesetzlichen Klarstellungen ausdrücklich und werde im kommenden Berichtszeitraum mein Augenmerk auf die gesetzeskonforme Umsetzung der Vorgaben durch die Krankenkassen richten.

Querverweise:

6.6 Modellvorhaben Genomsequenzierung

6 Einzelthemen

6.1 Elektronische Patientenakte

Krankenkassen klagen gegen von mir verhängte datenschutzaufsichtsrechtliche Maßnahmen zur Durchsetzung einer europarechtskonformen Ausgestaltung der elektronischen Patientenakte (ePA) und damit gegen gleiche Rechte für alle Versicherten.

In meinem 29. Tätigkeitsbericht (TB) (Nr. 4.2) hatte ich über die europarechtswidrige Ausgestaltung der ePA auf Grundlage des Patientendaten-Schutz-Gesetzes (PDSG) berichtet. Insbesondere das Zugriffsmanagement ist mit europarechtlichen Vorgaben nicht vereinbar. Die nationalen gesetzlichen Vorgaben sehen vor, dass Zugriffe nur nach dem „Alles-oder –Nichts-Prinzip“ möglich sind. Erst ab dem 1. Januar 2022 kann die Benutzergruppe, die über ein geeignetes mobiles Endgerät verfügt, feingranular , d. h. dokumentenspezifisch Zugriffe erteilen. Die Versicherten, die kein eigenes geeignetes Gerät besitzen oder keines nutzen wollen, werden hiervon nicht erfasst. Sie können lediglich beim Leistungserbringer, z. B. in der ärztlichen Praxis, auf Kategorien von Dokumenten beschränkte Zugriffsrechte erteilen oder einem Dritten mit einem geeigneten technischen Gerät Vertretungsrechte einräumen, müssen dabei aber dieser Person gegenüber alle Daten offenlegen. Außerdem werden diejenigen, die weder ein geeignetes Endgerät nutzen können oder wollen, noch die Vertreterlösung für sich in Anspruch nehmen möchten, auf Dauer auch keinen Einblick in ihre eigene, von ihnen selbst zu führende ePA haben.

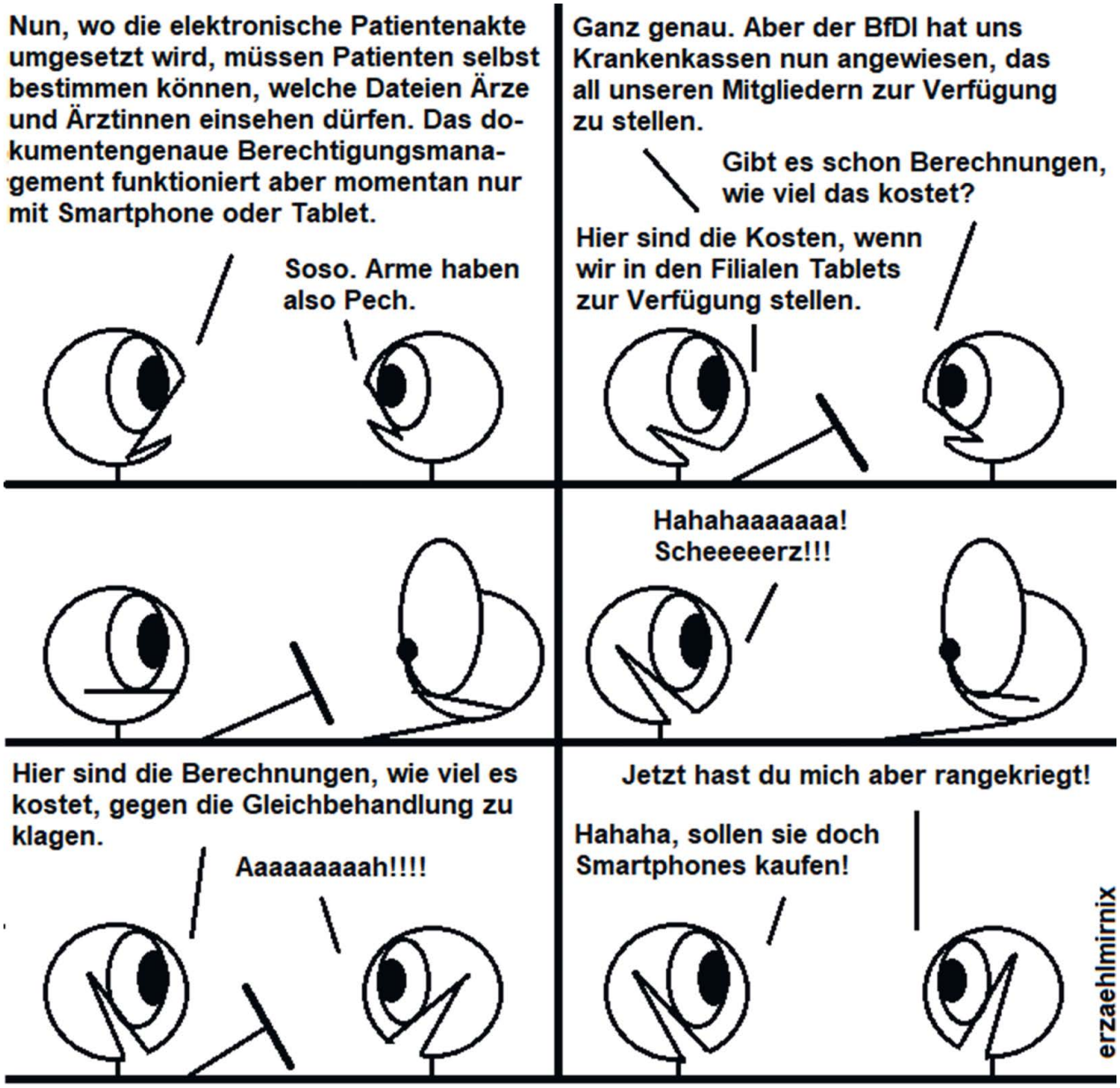
Diese gesetzlichen Vorgaben beschneiden die Souveränität der Versicherten empfindlich und stellen einen Verstoß gegen die für die Verarbeitung personenbezogener Daten geltenden Grundsätze der

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a) DSGVO),
- Zweckbindung (Art. 5 Abs. 1 lit. b) DSGVO),
- Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO,
- Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO)

dar, sowie einen Verstoß gegen Art. 25 Abs. 1 DSGVO, wonach der Verantwortliche unter Berücksichtigung unter anderem des Stands der Technik geeignete technische und organisatorische Maßnahmen treffen muss. Diese müssen dafür ausgelegt sein, die genannten Verarbeitungsgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Person zu schützen.

Nachdem die von mir im November 2020 gegenüber den meiner Datenschutzaufsicht unterliegenden gesetzlichen Krankenkassen ausgesprochene Warnung (vgl. ebenfalls 29. TB, Nr. 4.2) keine Änderung herbeigeführt hat, habe ich das angekündigte datenschutzaufsichtsrechtliche Maßnahmeverfahren vorangetrieben und im September 2021 fünf große gesetzliche Krankenkassen gemäß Art. 58 Abs. 2 lit. d) DSGVO angewiesen:

1. Das Zugriffsmanagement der ePA so auszugestalten, dass Versicherte eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 SGB V in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen („ feingranulares Zugriffsmanagement“) können. Dies kann für Versicherte, die keine Benutzeroberfläche eines geeigneten Endgeräts verwenden (Frontend-Nichtnutzer), insbesondere mittels der dezentralen Infrastruktur der Leistungserbringer oder durch sonstige technische Einrichtungen bei den Leistungserbringern bzw. in ihren Geschäftsräumen oder in Kooperation mit anderen Krankenkassen oder Stellen erfüllt werden.
2. Das Zugriffsmanagement der ePA so auszugestalten, dass auch Frontend-Nichtnutzer auch ohne die Bestellung eines Vertreters in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können. Dies kann ebenfalls insbesondere mittels der dezentralen Infrastruktur der Leistungserbringer oder durch sonstige technische Einrich



tungen bei den Leistungserbringern bzw. in ihren Geschäftsraumen oder in Kooperation mit anderen Krankenkassen oder Stellen erfüllt werden.

3. Für Versicherte, die die Benutzeroberfläche eines geeigneten Endgeräts verwenden (Frontend-Nutzer), hat die Umsetzung der Ziffer 1 bis zum 31. Dezember 2021, spätestens jedoch innerhalb von einem Monat nach Rechtskraft eines etwaigen abschließenden Urteils zu erfolgen.
4. Für Frontend-Nichtnutzer hat die Umsetzung der Ziffern 1 und 2 binnen eines Jahres zu erfolgen.

Gegen diese Anweisungen haben die adressierten Krankenkassen Klage erhoben.

6.2 Datenstrategie der Bundesregierung

Die Bundesregierung hat 2021 eine Datenstrategie vorgelegt, in der sie ihre Maßnahmen zur Förderung der Digitalwirtschaft bündelt. Dabei sollten auch Weiterentwicklungen beim Datenschutz berücksichtigt werden.

Die Bundesregierung hat Anfang 2021 eine sog. Datenstrategie beschlossen. Sie ist damit dem Vorbild der Europäischen Kommission gefolgt, die bereits zum 19. Februar 2020 die maßgebende EU-Datenstrategie vorgelegt hat (vgl. COM(2020) 66 final). Im Mittelpunkt der nationalen Datenstrategie (als auch der EU-Datenstrategie)

stehen Maßnahmen zur Förderung einer europäischen Digitalwirtschaft. Ein übergreifendes Ziel ist dabei die Sicherung der digitalen Souveränität.

Sowohl das Bundeskanzleramt (BKAmt) als auch der Deutsche Bundestag haben mir Gelegenheit zur Stellungnahme gegeben. Ich habe die Bemühungen der Bundesregierung begrüßt und zugleich Verbesserungen eingefordert. Strategien zu erstellen bedeutet, klare Ziele zu definieren und einen übergeordneten Plan zu entwickeln.

Laut Datenstrategie soll die innovative und verantwortungsvolle Datenbereitstellung und Datennutzung in Deutschland und Europa signifikant erhöht werden – in der Wirtschaft und Wissenschaft, in der gemeinwohlbezogenen Forschung sowie in der Zivilgesellschaft und in der Verwaltung. Gleichzeitig soll auf Basis europäischer Werte eine gerechte Teilhabe gesichert, Datenmonopole verhindert und zugleich Datenmissbrauch konsequent begegnet werden. Diese Zielsetzungen erscheinen mir, auch angesichts des klaren Bekenntnisses zur europäischen Datenschutz-Grundverordnung (DSGVO), weiterhin sachgerecht. Ein interessantes Anwendungsbeispiel für diese Bemühungen stellt etwa bereits das Projekt Gaia-X zum Aufbau einer sicheren und vertrauenswürdigen europäischen Infrastruktur für das Pooling und das Teilen von Daten dar. Die frühe Veröffentlichung einer Datenstrategie und eine transparente Vorgehensweise ermöglichen den Bürgerinnen und Bürgern und auch mir in meiner Aufsichtsfunktion, besser nachzuvollziehen, welche Auswirkungen digitalpolitische Planungen für den Datenschutz nach sich ziehen können.

Gleichwohl habe ich in einer Reihe von Punkten Kritik geübt. Denn insgesamt hat die Datenstrategie trotz einiger verbaler Bekenntnisse auch zum Datenschutz wenig Konkretes oder Neues vorgeschlagen. Verwiesen wurde stattdessen auf eine große Anzahl bereits laufender Vorhaben. Vermisst habe ich eine Einordnung und Vereinbarkeit des datenökonomischen Vokabulars (so etwa das Datenteilen, die verantwortungsvolle Datennutzung und der Datenzugang) mit den datenschutzrechtlichen Schutzkonzepten. Dementsprechend kommt es, auch in den auf Grundlage der EU-Datenstrategie geschaffenen europäischen Gesetzesvorhaben (DGA, DSA), zu zweideutigen Formulierungen, bei denen nicht klar wird, ob Datenschutz gilt, oder ob ausschließlich Verarbeitungen nicht-personenbezogener Daten geregelt werden. Bei den Anonymisierungsverfahren, die für den Datenaustausch etwa zwischen Unternehmen eine große Rolle spielen könnten, werden die Re-Identifizierungsrisiken nicht adressiert. Und übergreifend fehlt es letztlich an einer datenschutzrechtlichen Einordnung der geplanten Datenökonomie im Hinblick auf den neuen Ver

arbeitungsstandard aus Big Data in Kombination mit KI-Anwendungen. Die mit dem Massendatenaustausch verbundenen individuellen als auch überindividuellen Risiken (z. B. Abschaffung der Anonymität öffentlich zugänglicher Räume; flächendeckend zur Anwendung kommende statistische Vor-Urteile) bedürfen jedenfalls weiterer Untersuchung und auch gesetzlicher Anstrengungen sowie der Stärkung der Aufsichtsinstrumente. Zweifelhaft erscheinen jedenfalls Ansätze, bei denen allein auf die Marktgängigkeit bestehender datenschutzrechtlicher Konzepte wie der Einwilligung oder der Pseudonymisierung hingewirkt wird. Und auch vielversprechende neue Konzepte wie die sog. Datentreuhand (Datenmittler) bedürfen noch der weiteren Konkretisierung, bevor ihre Vereinbarkeit mit Datenschutzvorgaben besser beurteilt werden kann.

Querverweise:

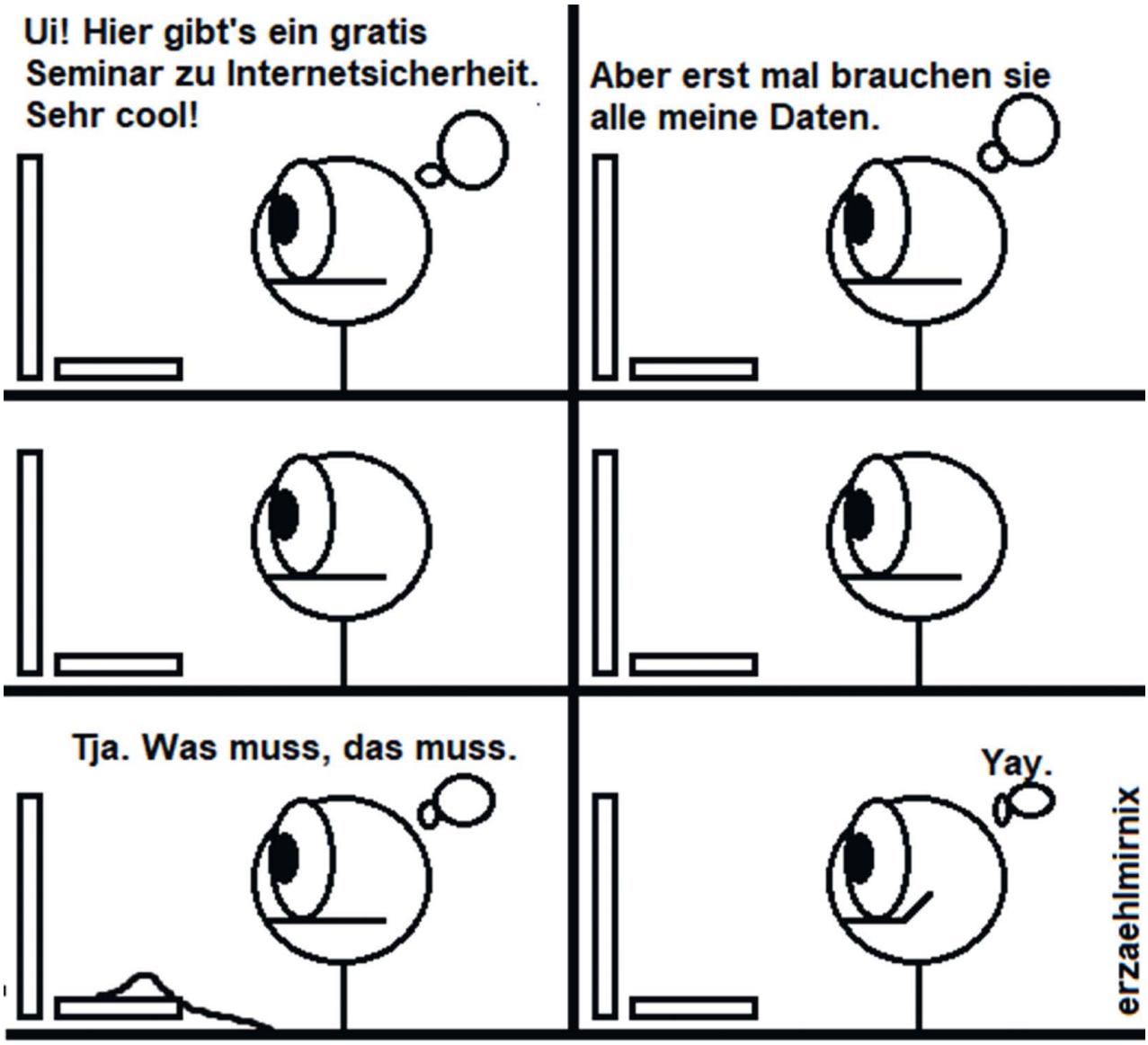
5.9 EU Digitalgesetzgebung

6.3 Kooperation zwischen Kartell- und Datenschutzaufsichtsbehörden

Die schnell fortschreitende Digitalisierung mit ihren immer größeren Auswirkungen bietet viele neue Möglichkeiten, aber auch Risiken, denen es zu begegnen gilt. Dem Datenschutz- und Kartellrecht kommt hierbei im Rahmen der Regulierung eine ganz besondere Rolle zu. Für eine effiziente und konsequente Durchsetzung der bestehenden Regelungen ist eine Kooperation der Behörden unabdingbar.

Die Marktaktivitäten insbesondere der internationalen Großunternehmen der Internetwirtschaft zeigen uns, wie durch die Digitalisierung mehr und mehr das gesellschaftliche und wirtschaftliche Leben durchdrungen und geprägt wird. Was vor nicht allzu langer Zeit möglicherweise noch als undenkbar erschien, ist vielfach zur Gewohnheit geworden. Dies zeigt Chancen auf, die Risiken, die damit verbunden sind, dürfen aber nicht vernachlässigt, sondern müssen stets mit in den Blick genommen werden. Datengetriebene Geschäftsmodelle der Unternehmen mit ihrer immanenten Verarbeitung personenbezogener Daten erhöhen die Risiken ihrer Marktmacht und stellen eine Gefährdung des informationellen Selbstbestimmungsrechts jeder einzelnen Person dar.

Mit seinem in 2019 eingeleiteten Verfahren gegen Facebook hat das Bundeskartellamt (BKartA) dieses Spannungsfeld erstmals wettbewerbsrechtlich aufgegriffen und Facebook untersagt, personenbezogene Daten u. a.



seiner Töchter WhatsApp und Instagram ohne datenschutzrechtlich wirksame Einwilligung zusammen zu führen. Ich habe dieses Verfahren von Anfang an eng begleitet und bei Datenschutzfragen unterstützt. Auch meine Kolleginnen und Kollegen im Europäischen Datenschutzausschuss (EDSA) habe ich hierzu regelmäßig unterrichtet. Inzwischen hat das Oberlandesgericht (OLG) Düsseldorf dem Europäischen Gerichtshof (EuGH) Auslegungsfragen zur Datenschutz-Grundverordnung (DSGVO) vorgelegt, u. a. auch zum Verhältnis der Datenschutz- und Kartellaufsicht. Ich bin der Auffassung, dass es hier keinen künstlichen Vorrang eines Aufsichtsbereichs geben kann. Vielmehr sollten diese Fragen im Fokus aller zuständigen Aufsichtsbehörden stehen und über einen regelmäßigen Austausch eine einheitliche Aufsichtspraxis ermöglicht werden.

Die 2021 in Deutschland in Kraft getretene Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB-Digitalisierungsgesetz) ermöglicht es, dass missbräuchliche Geschäftspraktiken, die vielfach auch mit datenschutzrechtlichen Vorgaben nicht in Einklang stehen, schnell und effektiv geahndet werden können. So stellt das GWB nun beispielsweise klar, dass die Verweigerung des Zugangs zu wettbewerbsrelevanten Daten ein verbotenes Verhalten von marktbeherrschenden Unternehmen begründen kann. In diesem Zusammenhang ist aber unbedingt zu beachten, dass neben dem wettbewerblichen Zugangsrecht auch die datenschutzrechtlichen Voraussetzungen für die Verarbeitung der Daten gegeben sein müssen. Daneben hat das BKartA auch zusätzliche Kompetenzen erhalten, um die Marktrelevanz großer Technologieunternehmen prüfen zu können und hat dazu bereits eine Reihe von Untersuchungen eingeleitet, bei denen Datenverarbeitungen ebenfalls eine zentrale Rolle spielen. Die mit § 50f GWB neu eingeführte Rechtsgrundlage für den Datenaustausch und die

Kooperation zwischen den Wettbewerbs-, Verbraucherschutz- und Datenschutzbehörden ist hier ein wichtiges Instrument, das das BKartA und ich erfolgreich nutzen.

Im Rahmen der Kooperation zwischen Kartell- und Datenschutzaufsichtsbehörden nimmt Deutschland dadurch eine Art Vorreiterrolle ein, die es aber auch auf europäischer und internationaler Ebene umzusetzen gilt. Ich setze mich deshalb mit Nachdruck dafür ein, auch in dem auf europäischer Ebene zurzeit verhandelten Digital Markets Act (DMA) eine solche Kooperation zu ermöglichen. Zudem begleite ich sowohl die Aktivitäten zur Förderung einer stärkeren Zusammenarbeit zwischen Kartell- und Datenschutzaufsichtsbehörden im Rahmen der Global Privacy Assembly (GPA), als auch beim Austausch der Datenschutzbehörden der G7-Staaten aktiv, um die anderen Aufsichtsbehörden zu einer entsprechenden Kooperation weiter zu ermutigen.

6.4 Neustart des Forschungsdatenzentrums beim Bundesinstitut für Arzneimittel und Medizinprodukte

Damit die Daten der Krankenkassen und aus den elektronischen Patientenakten datenschutzkonform zum Forschungsdatenzentrum gelangen, müssen eine Fülle technischer Festlegungen getroffen werden, darunter das Verfahren, nach dem die Vertrauensstelle die Pseudonymisierung dieser Daten durchführt.

Nach den Regelungen der §§ 303 a ff. SGB V und der Datentransparenzverordnung (DaTraV) laufen die Abrechnungsdaten der Krankenkassen pseudonymisiert im Forschungsdatenzentrum (FDZ) beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zusammen, wo sie u. a. zu Forschungszwecken genutzt werden können. Mit der inhaltlichen Erweiterung

der seit 2012 bestehenden Vorschriften und mit der zur Umsetzung erlassenen Verordnung habe ich mich bereits in den letzten Jahren befasst (28. TB Nr. 5.6; 29. TB Nr. 5.7). Nach den Regelungen aus dem Patientendaten-Schutz-Gesetz (PDSG) können ab dem Jahr 2023 zudem Daten aus der elektronischen Patientenakte (ePA) für das Forschungsdatenzentrum freigegeben werden (nach § 363 Abs. 1 bis 7 SGB V; 29. TB Nr. 4.2).

Im Berichtszeitraum ging es um die technische Umsetzung dieser Vorschriften. Beteiligt waren neben dem BfArM als „Registerstelle" das Robert Koch-Institut (RKI) als Vertrauensstelle, die gematik GmbH als Verantwortliche für die Übermittlung durch die Telematikinfrastruktur (TI) und das Bundesministerium für Gesundheit (BMG) selbst. Ein Schwerpunkt war neben dem Hosting des FDZ auch die sachgerechte Bildung des sog. periodenübergreifenden Pseudonyms (PüP). Dieses PüP wird von der Vertrauensstelle gebildet und dient zur Zuordnung der Krankenkassendaten über Jahre hinweg. Auch musste für die Daten aus der ePA ein Verfahren entwickelt werden, welches eine Zuordnung zum gleichen periodenübergreifenden Pseudonym sicherstellt. Für die Erzeugung des Übermittlungs-Pseudonyms soll ein asymmetrisches kryptografisches Verfahren eingesetzt werden. Bzgl. der Daten aus der ePA verwendet das Verfahren einen Public Key des RKI, der in der ePA-App liegt, und eine Arbeitsnummer, um die Daten zunächst verschlüsselt an die Vertrauensstelle zu leiten. Für die Freigabe aus der ePA war zudem festzulegen, wo die Einwilligung dokumentiert und die Freigabe auch dem Umfang nach protokolliert wird. Zudem war sicherzustellen, dass im Falle des Widerrufs der Einwilligung die Daten unverzüglich gelöscht werden. Das Thema FDZ wird mich auch im kommenden Jahr weiter begleiten, wo ich mich mit der konkreten Ausgestaltung einer Datenweitergabe aus der ePA an die Forschung in Form von Medizinischen Informationsobjekten (MIO) beschäftigen werde.

6.5 Nutzung der Krankenversichertennummer in der Telematikinfrastruktur

Die Verwendung der Krankenversichertennummer (KVNR) zur eindeutigen Identifizierung der Versicherten bei verschiedenen Anwendungen innerhalb der Telematikinfrastruktur (TI), wie z. B. dem TI-Messenger, stellt eine datenschutzfreundliche Lösung dar. Möglich ist dies jedoch nur auf Basis einer eindeutigen Rechtsgrundlage.

Mit dem am 9. Juni 2021 in Kraft getretenen Gesetz zur digitalen Modernisierung von Versorgung und Pflege (Digitale-Versorgung-und-Pflege-Modernisierungsgesetz – DVPMG) wurde u. a. die Rechtsgrundlage für die Implementierung eines Messenger-Dienstes für die Kommunikation zwischen Versicherten und Leistungserbringern innerhalb der TI geschaffen (§ 342 Abs. 2 Nr. 4 SGB V). Die gematik GmbH wurde mit der Entwicklung dieses TI-Messengers („TIM") beauftragt. Erforderlich ist dabei die Implementierung eines Verfahrens zur eindeutigen Adressierung der Versicherten. Gespräche zwischen BfDI, Bundesgesundheitsministerium (BMG) und gematik führten zu dem einvernehmlichen Ergebnis, dass die datenschutzfreundlichste Lösung die Errechnung einer nicht rückrechenbaren Matrix-Adresse aus der Krankenversichertennummer (KVNR) wäre. Die alternative Schaffung eines Verzeichnisses aller teilnehmenden Versicherten würde die größeren Datenschutzrisiken bergen. Dieses Ergebnis entspricht auch der Gesetzesbegründung zu § 342 Abs. 2 Nr. 4 SGB V, welche die Erstellung eines neuen Versichertenverzeichnisses ausschließt und stattdessen die Nutzung eines Pseudonyms aus der KVNR vorschlägt. Auch andere Anwendungen innerhalb der TI, wie die elektronische Patientenakte oder das e-Rezept, nutzen die KVNR zur Versichertenidentifizierung.

Datenschutzrechtlich zulässig ist die Verarbeitung aber nur auf Grundlage einer eindeutigen gesetzlichen Befugnisnorm, die gegenwärtig nicht vorliegt. Insbesondere lässt sich die Verarbeitung der KVNR durch die Leistungserbringer im Rahmen einer freiwilligen Anwendung der TI unter keine der in § 18 SGB IV – die Norm regelt die Zulässigkeit der Verarbeitung der Versicherungsnummer – aufgeführten Fallgruppen subsumieren. Auch das SGB V sieht keine spezialgesetzliche Regelung für die Verwendung der KVNR zu den beschriebenen Zwecken vor.

Zur Herstellung eines rechtskonformen und – sicheren Zustands ist die Schaffung einer eindeutigen Rechtsgrundlage für die Verarbeitung der KVNR innerhalb der TI zwingend erforderlich. Da die Möglichkeiten zur

Identifikation der Versicherten jedoch keine Alternativen im Hinblick auf die Datenschutzfreundlichkeit darstellen, habe ich dem BMG mitgeteilt, dass ich den gegenwärtigen Zustand zunächst dulde, im Gegenzug aber erwarte, dass zum nächstmöglichen Zeitpunkt eine entsprechende Rechtsgrundlage geschaffen wird.

Auch in einem anderen Punkt erweist sich die Verarbeitung der KVNR im Zusammenhang mit Anwendungen der TI als problematisch. So sieht § 362 Abs. 1 SGB V vor, dass die Unternehmen der Privaten Krankenversicherung (PKV) sowie weitere Kostenträger künftig für ihre Versicherten den unveränderbaren Teil der KVNR nach § 290 Abs. 1 S. 2 SGB V für die Nutzung der Anwendungen der TI sowie für die Meldungen nach dem Implantateregistergesetz (IRegG) verwenden. Dazu müssen die KVNR vorab durch die Vertrauensstelle gem. § 290 Abs. 2 S. 2 SGB V gebildet werden. Um eine Doppelvergabe auszuschließen, wird im Vergabeverfahren überprüft, ob für den jeweiligen Versicherten bereits eine KVNR vergeben wurde. Hierfür ist in der „Richtlinie zum Aufbau und zur Vergabe einer Krankenversichertennummer und Regelungen des Krankenversichertennummernverzeichnisses nach § 290 SGB V“ ein sog. Clearing-Verfahren zwischen den Krankenkassen vorgesehen. Dabei werden versichertenbezogene Daten wie die KVNR, die Rentenversicherungsnummer, Name, Vorname(n), Geschlecht, Geburtsdatum und Geburtsort zwischen den Krankenkassen ausgetauscht.

Wenn die PKV und die weiteren in § 362 SGB V genannten Kostenträger zukünftig die KVNR für die Teilhabe ihrer Versicherten an Anwendungen der TI nutzen, ist ihre Einbeziehung in das Clearing-Verfahren erforderlich. Jedoch fehlt es auch hierfür an einer eindeutigen Rechtsgrundlage. Diese Einschätzung teilt das BMG und hat mir zugesichert, eine entsprechende Befugnisnorm in das nächste geeignete Gesetzgebungsverfahren einzubringen. Ein Diskussionsentwurf liegt mir bereits vor, der nunmehr der Abstimmung zwischen BMG, BMJ und mir bedarf.

Querverweise:

5.10 Entwicklungen bei Gesundheitsregistern, 6.1 Elektronische Patientenakte

6.6 Modellvorhaben Genomsequenzierung

Im „Hau-Ruck-Verfahren“ wird der Forschung eine zusätzliche Datenquelle erschlossen, fachliche und datenschutzrechtliche Belange blieben zugunsten einer schnellen Festlegung unberücksichtigt.

Der von der Bundesregierung vorgelegte Entwurf eines Gesetzes zur Weiterentwicklung der Gesundheitsversorgung (Gesundheitsversorgungsweiterentwicklungsgesetz, GVWG) vom 1. Januar 2021 – noch ohne eine Regelung zur Genomsequenzierung – umfasste auf etwa 170 Seiten in 15 Artikeln Änderungen in verschiedensten Gesetzen; allein in Artikel 1 für das SGB V immerhin 72 Nummern mit Änderungsvorschlägen zu unterschiedlichen Paragrafen. Hierzu gab es im März 2021 bereits im parlamentarischen Beratungsverfahren ergänzende Änderungsanträge mit einem Umfang von 88 Seiten. Hierunter befand sich in Änderungsantrag 3 der Entwurf eines neuen § 64 d SGB V zum „Modellvorhaben Genomsequenzierung“. Die Regelung sollte den Versicherten in der gesetzlichen Krankenversicherung bei seltenen und bei onkologischen Erkrankungen einen Anspruch auf personalisierte Medizin geben. Das bedeutet, es soll mittels Genomsequenzierung Diagnostik und Therapiefindung vorgenommen werden. Wesentlicher Regelungsinhalt war weiter das Errichten einer sog. „gemeinsamen Dateninfrastruktur“, in der Genomdaten gespeichert und genutzt werden können. Leider fehlte es der Formulierung in vielerlei Hinsicht an Gehalt und Konkretisierung, worauf ich mit Stellungnahme vom 29. März 2021 hinwies. Wesentliche Punkte waren nicht Gegenstand der Regelung: es fehlte an Vorgaben zu Trägerschaft und Aufbau der Dateninfrastruktur, zur datenschutzrechtlichen Verantwortung, zur Ausgestaltung der Verfahren u. a. zur Datennutzung und zu Zuständigkeiten. Ebenso fehlten Regelungen zur Datensicherheit und zum Verhältnis zum Gendiagnostikgesetz.

Aufgrund der zeitlichen Enge – die Sitzung des Gesundheitsausschusses stand an, ohne dass auf die eklatanten Mängel reagiert und nachjustiert worden wäre – adressierte ich am 9. April 2021 ein Schreiben unmittelbar an den Ausschuss für Gesundheit des Bundestages. Es zählte im Einzelnen die fehlenden Regelungen auf und endete mit der Empfehlung, das Vorhaben zurückzustellen, um eine fachlich und rechtlich vollständige Regelung zu ermöglichen.

Entgegen meiner Empfehlung wurde die Regelung des Modellvorhabens nicht zurückgestellt. Eine kurzzeitig vorgelegte überarbeitete Fassung enthielt dann Vorgaben zu Datenflüssen, einer Vertrauensstelle und einem Antragsverfahren für den Datenzugang, die sich an den Regelungen der §§ 303a ff SGB V für das Forschung

sdatenzentrum beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) anlehnten. Eine weitere Überarbeitung vom 19. Mai 2021 berücksichtigte weitere von mir geltend gemachte relevante Punkte und traf Festlegungen zu den Verantwortlichen für die Vertrauensstelle – das Robert Koch-Institut (RKI) – und für die Dateninfrastruktur – das BfArM.

Der ursprüngliche zielführende Ansatz einer verteilten Dateninfrastruktur blieb bei diesem gedrängten Verfahren auf der Strecke. Dabei ist eine dezentrale Struktur „state of the art". Ein jeweils anlassbezogener, partieller Austausch oder Datenzugang reicht für die Zwecke des Modellvorhabens aus und vermeidet eine durchgehend doppelte Datenhaltung – wie nun beim BfArM. Eine dezentrale Datenhaltung hat weitere Vorteile: Sie entspricht dem Prinzip der Datenminimierung und erleichtert auch in technischer Hinsicht die Erfüllung der Anforderungen an die Datensicherheit.

Es besteht also weiterhin viel Potential für Verbesserungen und ich hoffe, dass diese in der neu angelaufenen Legislaturperiode aufgegriffen werden.

Ich empfehle, beim Modellvorhaben Genomsequenzierung den Aufbau der „gemeinsamen Dateninfrastruktur" dezentral zu strukturieren und statt einer doppelten Datenhaltung jeweils anlassbezogene Datenzugänge vorzusehen.

Querverweise:

5.11 Datenerhebungsbefugnisse der Krankenkassen im Krankengeldfallmanagement

6.7 Pränataltests in Hongkong

Die Durchführung von Pränataltests darf nicht aus Kostengründen an Labore in Drittstaaten ausgelagert werden, bei denen erhebliche Risiken im Hinblick auf die Einhaltung datenschutzrechtlicher Vorgaben bestehen.

Im Berichtszeitraum ging aus internationalen Presseberichten (https://www.reuters.com/investigates/special-report/health-china-bgi-dna) hervor, dass eine chinesische Unternehmensgruppe Labore u. a. in Hongkong betreibt, die genetisches Probenmaterial untersuchen. Beauftragt werden sie in einem nicht unerheblichen Maße – ausschlaggebend ist dafür vor allem der Kostenfaktor – auch von deutschen Leistungserbringern mit der Auswertung von nicht invasiven pränatalen Bluttest (NIPT), die von Schwangeren in Anspruch genommen werden. So ist mir bekannt, dass ein solcher Pränataltest in Deutschland durch ein Unternehmen mit Sitz in Hessen angeboten wird, welches das gewonnene Probenmaterial an die chinesischen Labore weiterleitet. Den Presseberichten folgend bestehen konkrete Anhaltspunkte dafür, dass das chinesische Unternehmen die Proben auch für eigene Forschungsprojekte verwendet, die unter Umständen auch in Kooperation mit dem chinesischen Militär betrieben werden.

Abgesehen von der im Raum stehenden zweckwidrigen Nutzung der Daten, die per se unzulässig wäre, ist auch eine Übermittlung personenbezogener Daten in Drittstaaten, für die keine Angemessenheitsentscheidung der Europäischen Kommission vorliegt und ein ausreichender Schutz der personenbezogenen Daten auch nicht auf andere Weise sichergestellt ist, unzulässig, gerade wenn es um solche sensiblen Daten geht.

Der Hessische Datenschutzbeauftragte, der die datenschutzrechtliche Aufsicht über das o. a. Labor führt, prüft derzeit die Datenschutzkonformität. Dabei wurde mit dem Unternehmen vereinbart, bis zum Abschluss der Prüfung keine weiteren Proben an das in Hongkong ansässige Labor zu übersenden.

In der Zwischenzeit sind die NIPTs für die Anwendung bei Schwangerschaften mit besonderen Risiken auf Grundlage des Beschlusses des Gemeinsamen Bundesausschusses vom 19. September 2019 zur Änderung der Mutterschafts-Richtlinien (BAnz AT 20. Dezember 2019 B6) als Kassenleistung zugelassen worden.

Ich habe mich sowohl an den Gemeinsamen Bundesausschuss als auch an den Spitzenverband Bund der Krankenkassen (GKV-SV) gewandt und diese auf die bestehende Problematik hingewiesen. Gleichzeitig habe ich sie aufgefordert, Maßnahmen zu ergreifen, um hinsichtlich des Angebotes von NIPTs die Sicherheit der nach Art. 9 DSGVO besonders schützenswerten genetischen Daten der Versicherten zu gewährleisten.

Ich konnte zunächst erreichen, dass die Mutterschafts-Richtlinie um den Hinweis auf die Einhaltung der datenschutzrechtlichen Vorgaben bei der Beauftragung von Laboren durch die Ärztinnen und Ärzte ergänzt wurde. Im Übrigen bleibt das Prüfergebnis des Hessischen Datenschutzbeauftragten abzuwarten, aus dem sich möglicherweise weiterer Handlungsbedarf auch für mich ergeben wird.

6.8 Umsetzung des Diagnose-Korrektur-Anspruch § 305 SGB V

Nach anfänglichen Schwierigkeiten ist die Umsetzung des neugeregelten Diagnose-Korrekturanspruchs bei den gesetzlichen Krankenkassen gelungen.

In meinem 29. Tätigkeitsbericht (Nr. 7.14) hatte ich über die Ergänzung des § 305 Abs. 1 SGB V berichtet, die den Versicherten auch auf nationaler Ebene zur Durchsetzung ihres durch Art. 16 DSGVO garantierten Rechts auf Berichtigung mittels eines Diagnose-Korrektur-Anspruchs gegenüber ihrer Krankenkasse verhelfen sollte. Zu Beginn dieses Berichtszeitraums erreichten mich noch Beschwerden von Versicherten, deren Krankenkassen ihren Anspruch auf Korrektur der Diagnosedaten trotz Vorliegens der formalen Voraussetzungen (Beleg der Unrichtigkeit durch einen ärztlichen Nachweis) nicht innerhalb der gesetzlich vorgesehenen Frist von vier Wochen beschieden haben. Nach Darstellung einzelner Krankenkassen lag die Verzögerung an der komplexen technischen Umsetzung der gesetzlichen Vorgaben, die einer gewissen Vorlaufzeit bedurften, die aber das Gesetz nicht einräumte.

Die Argumentation der Krankenkassen war für mich nachvollziehbar, so dass ich zunächst von datenschutzaufsichtsrechtlichen Maßnahmen bei nicht fristgerechter Diagnosekorrektur abgesehen und Übergangslösungen – etwa als Hinweis an die Versicherten, dass die ärztliche Bestätigung der unrichtigen Diagnose bis zur vollständigen technischen Umsetzung des Korrekturanspruchs der schon abgerufenen (fehlerhaften) Patientenquittung hinzugefügt werden kann und beide Dokumente vorerst als Gesamtdokumentation an Dritte (z. B. Versicherungen) übermittelt werden können – akzeptiert habe.

Im dritten Quartal dieses Berichtsjahres haben mich keine weiteren Beschwerden erreicht. Ich gehe deshalb davon aus, dass die technische Umsetzung des Diagnose-Korrektur-Anspruchs erfolgreich abgeschlossen wurde. Im Rahmen kommender Vor-Ort-Kontrollen bei Krankenkassen werde ich dies überprüfen.

6.9 Erstattungsfähige Digitale Gesundheitsanwendungen

Für erstattungsfähige digitale Gesundheitsanwendungen ist es zukünftig nicht mehr ausreichend, lediglich eine Selbsterklärung der Hersteller zur Datenschutzkonformität vorzulegen, sondern dieses muss durch ein Zertifikat nachgewiesen werden.

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) führt gemäß § 139e Abs. 1 SGB V ein Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen (DiGA) nach § 33a SGB V und entscheidet über die Anträge der DiGA-Hersteller zur Aufnahme in das Verzeichnis. Die Hersteller digitaler Gesundheitsanwendungen weisen derzeit die Erfüllung der datenschutzrechtlichen Anforderungen gemäß § 139e Abs. 2 S. 2 Nr. 2 SGB V unter Verwendung einer Selbsterklärung nach Anlage 1 zur Digitale Gesundheitsanwendungen-Verordnung (DiGAV) nach.

Dieses Verfahren ist jedoch aus datenschutzrechtlicher Sicht unzureichend, da allein aufgrund einer Herstellererklärung die Einhaltung der datenschutzrechtlichen Vorgaben nicht sicher anzunehmen ist. Diesbezüglich habe ich mich im Rahmen des Gesetzgebungsverfahrens zum Digitale–Versorgung–und–Pflege–Modernisierungs–Gesetz (DVPMG) erfolgreich dafür eingesetzt, eine Änderung hinsichtlich des Nachweises zu erreichen.

Zum 1. April 2023 erfolgt eine Ablösung der bisherigen Praxis der Selbsterklärung und wird fortan durch eine Nachweisführung mittels eines Datenschutzzertifikats nach § 42 DSGVO ersetzt.

Mit der im Rahmen des DVPMG novellierten Regelung des § 139e Abs. 11 SGB V ist das BfArM im Hinblick auf das Datenschutzzertifikat beauftragt, im Einvernehmen mit mir sowie im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) Prüfkriterien zu erarbeiten. Diese sollen die geltenden und abstrakten datenschutzrechtlichen Anforderungen der DSGVO und des § 4 DiGA-Verordnung in anwendungsgerechte Prüfungspunkte übersetzen. Die Festlegung der Prüfkriterien erfolgt dabei erstmalig bis zum 31. März 2022.

Ich gehe davon aus, das Einvernehmen mit dem BfArM im ersten Quartal 2022 herstellen zu können.

6.10 Digitalisierung der öffentlichen Verwaltung

Die Digitalisierung der öffentlichen Verwaltung bleibt weiterhin ein vorrangiges Anliegen der Regierungsverantwortlichen in Bund und Ländern. Den selbst gesetzten Umsetzungstermin bis zum 31. Dezember 2022 vor Augen forcieren sie ihre Aktivitäten, um Verwaltungsleistungen auch elektronisch über ihre Portale den Bürgerinnen und Bürgern anbieten zu können.

Bundesportal und Nutzerkonto Bund

Über das Verwaltungsportal des Bundes – kurz Bundesportal – sind Verwaltungsleistungen insbesondere des Bundes, aber auch der Länder und Kommunen, sowohl durch die Bürgerinnen und Bürger als auch durch Organisationen (z. B. Unternehmen) zu erreichen. Das noch im Aufbau befindliche Bundesportal stand 2021 in einer Basis-Version zur Verfügung, die sukzessive durch die zuständige Stelle, das vormalige Bundesministerium des Innern, für Bau und Heimat (BMI), ausgebaut und verbessert wurde.

Um sich für digitale Verwaltungsleistungen identifizieren und authentifizieren zu können, wird ein Nutzerkonto benötigt. Dieses wird vom Betreiber BMI auf Bundesebene seit April 2021 nur noch in der Ausprägung als Bürgerkonto (Nutzerkonto Bund für natürliche Personen) bereitgestellt. Gleichzeitig wurde die bisherige Komponente „Unternehmenskonto“ des Nutzerkontos Bund abgeschaltet sowie bereits angelegte Unternehmenskonten gelöscht. Für juristische Personen, rechtsfähige Vereinigungen, natürliche Personen in ihrer Funktion als Gewerbetreibende oder beruflich Selbständige oder für Behörden soll ein sog. einheitliches Organisationskonto als Nutzerkonto eingeführt werden.

Im Verlauf der bisherigen Entwicklung der Projekte Bundesportal und Nutzerkonto Bund einschließlich der geplanten Weiterentwicklungen und Optimierungen hat sich zwischen dem BMI und mir ein regelmäßiger und kontinuierlicher Austausch zu den damit verbundenen datenschutzrechtlichen Fragestellungen etabliert. Dies ist ein gutes Beispiel für eine „gelebte“ und wirkungsvolle Beratung der Bundesregierung mit Vorbildcharakter für andere Projekte.

E-Gesetzgebung und E-Scannen

Das Projekt „Elektronisches Gesetzgebungsverfahren des Bundes“ (E-Gesetzgebung) ist Teil der Dienstekonsolidierung der Bundesregierung. Hier sollen Rechtsetzungsverfahren des Bundes auf einer einheitlichen IT-Basis so gestaltet werden, dass Abstimmungsprozesse medienbruchfrei verlaufen können. Dazu wird eine gemeinsame Plattform entwickelt, auf der die mit Rechtsetzung befassten Organisationseinheiten der Bundesministerien Rechtstexte in einer einheitlichen und dem Handbuch der Rechtsförmlichkeit entsprechenden Struktur anlegen. Diese Dokumente sollen dann auf der Plattform vom jeweils federführenden Ressort der Bundesregierung in die Ressortabstimmungsprozesse gegeben werden, an denen auch ich beteiligt werde.

Beim Betrieb dieser Plattform werden auch personenbezogene Daten von Beschäftigten der beteiligten Behörden verarbeitet. Die Projektverantwortlichen haben einen iterativen Ansatz gewählt, bei dem bereits zu einem frühen Entwicklungszeitpunkt eine Version des Produkts mit eingeschränkten Funktionen zur Verfügung stand. In mehreren Veröffentlichungen pro Jahr wurden und werden die Funktionen erweitert. Dieses Vorgehen machte eine engmaschige Datenschutzberatung notwendig. Geplante Änderungen an den Verarbeitungsprozessen personenbezogener Daten mussten und müssen kurzfristig geprüft und bewertet werden, so dass sich auch hier ein kontinuierlicher, konstruktiver Austausch mit dem in diesem Projekt ebenfalls federführenden BMI etabliert hat. Schwerpunkte der Beratung waren hinsichtlich der ersten Produktveröffentlichung im April 2021 die Frage der datenschutzrechtlichen Verantwortlichkeit und für die Veröffentlichung der fortgeschriebenen Version im Oktober 2021 der Datenschutz durch Voreinstellung (privacy by design) sowie eine Prüfung auf Verarbeitung besonderer Kategorien personenbezogener Daten. Meine diesbezüglichen Hinweise wurden jeweils vom BMI aufgenommen und umgesetzt.

Ebenfalls Teil der Dienstekonsolidierung ist die Maßnahme E-Scannen, bei der es um die Digitalisierung von Eingangsdokumenten und Bestandsakten geht. Hier berate ich den vom BMI im Juni 2021 etablierten Lenkungsausschuss. Obwohl dieses Projekt noch am Anfang steht, kann ich bereits jetzt feststellen, dass sich auch hier ein konstruktiver Beratungsprozess anbahnt.

6.11 Brexit – Datentransfer mit dem Vereinigten Königreich

Am 28. Juni 2021 nahm die Europäische Kommission die Angemessenheitsbeschlüsse für die Übermittlung personenbezogener Daten an das Vereinigte Königreich gemäß der Datenschutz-Grundverordnung (DSGVO) und der Strafverfolgungsrichtlinie (JI-RL) an. Mit der Anerkennung des angemessenen Datenschutzniveaus bedürfen Datenübermittlungen aus dem Europäischen Wirtschaftsraum (EWR) in das Vereinigte Königreich, im Rahmen des Anwendungsbereichs der Beschlüsse, keiner besonderen Genehmigung durch die Datenschutz-Aufsichtsbehörden und müssen von keinen

weiteren Schutzmaßnahmen aus Kapitel V der DSGVO bzw. Kapitel V der JI-RL begleitet werden.

Am 31. Dezember 2020 endete der Übergangszeitraum, in dem das Vereinigte Königreich zwar bereits schon nicht mehr Mitglied der Europäischen Union (EU) war, jedoch noch das Recht der EU und somit auch die DSGVO Anwendung fand. Zum 1. Mai 2021 trat das Handels- und Kooperationsabkommen zwischen der EU und dem Vereinigten Königreich in Kraft, das bereits seit Jahresbeginn 2021 vorläufig angewendet wurde, um den Zeitraum zwischen Auslaufen des Übergangszeitraums zum 31. Dezember 2020 und dem Inkrafttreten zum 1. Mai 2021 zu überbrücken. Auf dieser Grundlage konnten personenbezogene Daten bis zum 30. April 2021 bzw. verlängert bis zum 30. Juni 2021 weiterhin ohne besondere Schutzmaßnahmen in das Vereinigte Königreich übermittelt werden, obwohl das Vereinigte Königreich mit dem Brexit seit dem 1. Januar 2021 als ein Drittland im Sinne der DSGVO anzusehen war.

Parallel zur Übergangsfrist startete die Europäische Kommission am 19. Februar 2021 das Annahmeverfahren für die Angemessenheitsbeschlüsse für das Vereinigte Königreich. Zu deren Entwürfen hat der Europäische Datenschutzausschuss (EDSA) in seiner Sitzung am 13. April 2021 zwei Stellungnahmen verabschiedet[21]. Am 28. Juni 2021 nahm die Europäische Kommission beide Angemessenheitsbeschlüsse für die Übermittlung personenbezogener Daten an das Vereinigte Königreich gemäß der DSGVO und der JI-RL an[22]. Mit dieser Anerkennung des angemessenen Datenschutzniveaus bedürfen Datenübermittlungen aus dem EWR an das Vereinigte Königreich, im Rahmen des Anwendungsbereichs der Beschlüsse, keiner besonderen Genehmigung durch die Datenschutz-Aufsichtsbehörden und muss von keinen weiteren Schutzmaßnahmen aus Kapitel V der DSGVO bzw. Kapitel V der JI-RL begleitet werden. Beide Angemessenheitsbeschlüsse haben eine Geltungsdauer bis zum 27. Juni 2025, sofern sie nicht vorher verlängert werden (vgl. oben 3.2.2.2).

Die Prüfung, ob die allgemeinen datenschutzrechtlichen Voraussetzungen für die entsprechende Datenverarbeitung erfüllt sind, bleibt davon unabhängig erforderlich.

Querverweise:

3.2.2.2 Schwerpunkt Drittlandübermittlung

6.12 Outing von Asylbewerbern

Bei Daten zur sexuellen Orientierung handelt es sich um besondere Kategorien personenbezogener Daten, deren Verarbeitung auch im asylrechtlichen Kontext problematisch ist.

Ein Petent wandte sich in mehreren Fällen an mich und schilderte ein aus seiner Sicht erfolgtes Outing homosexueller Asylbewerber bzw. unterstützender Personen im Rahmen der Befragung von Zeugen durch sog. Vertrauensanwälte in den Herkunftsländern der Asylbewerber. Im Rahmen des Asylverfahrens hat das Bundesamt für Migration und Flüchtlinge (BAMF) von Amts wegen den durch einen Asylbewerber vorgetragenen Sachverhalt zu klären. Sofern keine eigenen Erkenntnisse über konkret geschilderte Sachverhalte im Herkunftsland des Asylbewerbers vorliegen und auch das Auswärtige Amt (AA) hierzu keine Erkenntnisse hat, können sog. Vertrauensanwälte mit Ermittlungen beauftragt werden. Hierzu übermittelt das BAMF dem AA auf entsprechenden Vordrucken den konkreten Sachverhalt und zu klärende Fragestellungen. Im weiteren Verlauf beauftragt das AA einen bei ihm unter Vertrag stehenden Anwalt im Herkunftsland. Hierzu muss es den Sachverhalt und die zu klärenden Fragen an diesen übermitteln. Insbesondere im Zusammenhang mit der sexuellen Orientierung von Asylbewerbern ist hierbei besondere Vorsicht geboten. Eine Übermittlung von Daten an das AA und von diesem an den Vertrauensanwalt darf nur im notwendigen Umfang erfolgen. Auch bei der Auswahl der Vertrauensanwälte und deren Instruierung ist besondere Sorgfalt geboten, um zu verhindern, dass eine Gefährdung der Asylbewerber durch ein (unbeabsichtigtes) Outing oder sie unterstützender Personen im Rahmen deren Ermittlungen erfolgt.

21 Stellungnahme des EDSA zum Entwurf Angemessenheitsbeschluss DSGVO: https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf
Stellungnahme des EDSA zum Entwurf Angemessenheitsbeschluss JI-RL: https://edpb.europa.eu/system/files/2021-04/edpb_opinion152021_ukadequacy_led_en.pdf

22 Angemessenheitsbeschluss DSGVO: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf
Angemessenheitsbeschluss JI-RL: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf

6.13 Handydatenauswertung durch Bundesamt für Migration und Flüchtlinge rechtswidrig?

Das Verwaltungsgericht (VG) Berlin hat am 2. Juni 2021 in erster Instanz über eine Klage gegen die Auswertung der Handydaten einer Asylsuchenden entschieden und dieser stattgegeben.

§ 15a Asylgesetz (AsylG) räumt dem Bundesamt für Migration und Flüchtlinge (BAMF) grundsätzlich die Befugnis ein, die Datenträger von Ausländern auszuwerten. Voraussetzung ist jedoch, dass dies zur Feststellung der Identität und Staatsangehörigkeit des Asylsuchenden erforderlich sein muss und das Ziel nicht durch mildere Mittel erreicht werden kann.

Das BAMF liest die Handydaten von Asylsuchenden bereits zu einem sehr frühen Zeitpunkt aus. Bestimmte Daten werden in einem sog. Ergebnisreport ausgewertet. Dieser wird anschließend in einem Daten-Tresor gespeichert. Erst nach Begründung der Erforderlichkeit wird dieser Report nach entsprechender Prüfung durch einen Volljuristen zur weiteren Verwendung im Asylverfahren freigegeben. Diese Praxis stellt das VG mit seiner Entscheidung in Frage. Vorliegend hätte das BAMF nach Auffassung des Gerichts statt der Auswertung des Handys mildere Mittel, wie etwa die frühzeitig vorgelegten Dokumente der Asylsuchenden, heranziehen können. Ein Auslesen des Handys und das Speichern der Daten auf Vorrat sei dagegen unzulässig, entschied das VG. Da die Erhebung der Daten rechtswidrig gewesen sei, hätte nach Auffassung des VG auch der Ergebnisreport nicht verwertet werden dürfen. Die Auffassung des VG deckt sich damit mit meiner Position.

Das BAMF hat gegen das Urteil des VG Berlin Sprungrevision beim Bundesverwaltungsgericht eingelegt. Die höchstrichterliche Entscheidung wird ggf. weitreichende Konsequenzen für die künftige Praxis des BAMF haben und wird daher nicht nur dort mit Spannung erwartet.

In einem ähnlich gelagerten Fall hat eine betroffene Person bei mir Datenschutzbeschwerde gegen die Auswertung seines Handys eingereicht. Über diese ist noch nicht entschieden.

6.14 P 20 – Polizei 20/20: Der Weg zu einem gemeinsamen Datenhaus

Bis zu einem gemeinsamen „Datenhaus“ der Polizeibehörden des Bundes und der Länder ist es noch ein weiter Weg. Um dieses Ziel zu erreichen, müssen nicht nur technische und strukturelle Hürden genommen, sondern auch die datenschutzrechtlichen Leitplanken von Anfang an programmübergreifend und innerhalb der rund 30 Teilprojekte beachtet werden.

In den letzten Jahren habe ich immer wieder über das Projekt, das nunmehr in „P20 – Polizei 20/20“ umbenannt wurde, berichtet (vgl. 29. TB Nr. 6.1) und gegenüber dem Bundesministerium des Innern, für Bau und Heimat (BMI) deutlich gemacht, wie wichtig meine regelmäßige Beteiligung bei der Entwicklung dieses IT-Großprojekts ist. Zudem habe ich mehrfach um eine Auflistung sämtlicher Teilprojekte von P20 – Polizei20/20 nebst Projektbeschreibungen gebeten, um mir überhaupt einen Überblick über den Umfang des Projekts verschaffen zu können.

Beteiligung durch das BMI an P20 – Polizei 20/20 und den Teilprojekten

Die Information meiner Behörde zu dem Projekt P20 – Polizei 20/20 hat sich verbessert. Das BMI hat mir im April 2021 eine Auflistung zur Verfügung gestellt, aus der hervorgeht, dass das Projekt derzeit ca. 30 Teilprojekte beinhaltet, die in unterschiedlichen Bundesländern und in unterschiedlicher Teilnehmerstärke teilweise schon pilotiert werden. Darüber hinaus wurde ich im Vorfeld mit kurzer Frist zu den Vergabeverfahren zu einem einheitlichen Asservatenmanagementsystem (eAMS) und der elektronischen Akte in Strafsachen (EAS) beteiligt. Zu beiden Verfahren habe ich erste Stellungnahmen abgegeben.

Das BMI hat im Laufe des Jahres den Beratungsbedarf offensichtlich erkannt und informiert mich seither quartalsweise über den aktuellen Sachstand des Gesamtprojekts. Zudem wurde ich zu einem Termin mit dem Competence Center Fachlichkeit (CCF) eingeladen. Darüber hinaus haben Termine mit der Kerngruppe Datenschutz, die im BMI angesiedelt ist und der AG INPOL (einer Arbeitsgruppe des Arbeitskreises Sicherheit der DSK) zu ausgewählten Themen stattgefunden. Es wurden bereits Workshops zur „hypothetischen Datenneuerhebung“ und zu dem Teilprojekt „Proof of Concept (PoC) Datenkonsolidierung“ durchgeführt. Weitere Workshops zu Themen der Zweckbindung, KI-Anwendungen, Identity & Access Management und WiPras (Wiederholungsprognoseassistent) wurden mir in Aussicht gestellt. Ich begrüße ausdrücklich, dass mich das BMI nun stärker beteiligt.

Teilprojekt Proof of Concept (PoC) Datenkonsolidierung

Mit dem Teilprojekt PoC Datenkonsolidierung soll ein weiteres Verbundsystem außerhalb des polizeilichen Informationsverbundes nach dem Bundeskriminalamtgesetz (BKAG) entstehen (dazu bereits 29. TB Nr. 6.1). Im Unterschied zu dem polizeilichen Informationsverbund sollen mit dem PoC Daten im niedrigschwelligen Bereich zwischen den Polizeibehörden der Länder abgeglichen und recherchiert werden können. Faktisch handelt es sich um einen zweiten – neben dem in § 29 BKAG vorgesehenen – Informationsverbund, der aber die im Gesetz vorgesehenen Speicherschwellen unterschreitet. Das Bundeskriminalamt (BKA) soll dabei als technischer Dienstleister fungieren und die Länder als „Auftragsverarbeiter" unterstützen.

Ende des Jahres hat mir das BMI die Software vorgestellt. Obgleich sich das BMI im letzten Jahr für dieses Teilprojekt noch nicht verantwortlich sah, hat es mir zwischenzeitlich mitgeteilt, der PoC sei in das Gesamtprojekt P20 – Polizei 20/20 integriert worden. Meine datenschutzrechtlichen Einwände habe ich von Anfang an (seit Anfang 2019) geltend gemacht und halte diese auch weiterhin aufrecht. Weil ich die mit dem PoC beabsichtigte Datenverarbeitung für datenschutzrechtlich unzulässig halte, habe ich im März 2021 gegenüber dem BKA formell eine Warnung nach § 16 Abs. 2 S. 4 BDSG ausgesprochen. Für die mit dem PoC geplante unterstützende Tätigkeit des BKA als Auftragsverarbeiter der Länder fehlt es an einer rechtlichen Grundlage. Außerdem steht die mit dem PoC angestrebte Datenverarbeitung im Widerspruch zu den abschließenden Regelungen des BKAG. Das BKA darf rechtlich nicht als Auftragsdatenverarbeiter tätig werden, insbesondere wenn der „Auftrag" eigentlich in seinen ureigenen Aufgabenbereich als Zentralstelle gehört, nämlich hier einen bundesweiten Verbund bereitzustellen. Die Konstruktion der Auftragsverarbeitung kommt erst recht nicht in Betracht, wenn damit im Ergebnis die gesetzlichen Grenzen der Zentralstellentätigkeit unterlaufen werden. Das BKA hat zu der Warnung Stellung genommen, teilt meine Rechtsauffassung jedoch nicht. Meine Einwände habe ich in dem Workshop gegenüber dem BMI noch einmal verdeutlicht. Die weitere Entwicklung bleibt abzuwarten. Ich werde über den Fortgang berichten.

Entwicklung des Gesamtprojekts

Ein Entwicklungsschwerpunkt des letzten Jahres lag noch deutlich im organisatorischen und koordinierenden Bereich der unterschiedlichen Gremien.

Inhaltlich hat das BMI deutlich gemacht, die Vereinheitlichung der Fallbearbeitungssysteme (FBS) und der Vorgangsbearbeitungssysteme (VBS), Verbundsysteme (INPOL und PIAV) sowie eines eAMSe vorrangig voranzutreiben. Dazu würden derzeit entsprechende Interimslösungen entwickelt. Der Datenumfang bei den Polizeien des Bundes und der Länder ist äußerst umfangreich. Mit Blick darauf und aufgrund der technischen Komplexität können die IT-Systeme nur schrittweise umgestellt werden, bevor die Daten perspektivisch im Datenhaus gespeichert werden können. Bis Ende des Jahres soll die Konzeptionierungsphase für das „gemeinsame Datenhaus" vorangetrieben werden. Dreh- und Angelpunkt des Datenhauses wird nach meiner Einschätzung in der präzisen Verteilung von Zugriffsrechten liegen, damit der Grundsatz der Zweckbindung gewahrt und zwischen den einzelnen polizeilichen Zwecken getrennt werden kann (vgl. unter Nr.11.5). Das BMI hat mir zum Teilprojekt Datenhaus eine frühzeitige Beteiligung zugesagt.

In meinem letzten Tätigkeitsbericht (vgl. 29. TB Nr. 6.1) habe ich mich zu der strategischen Komponente des polizeilichen Informations- und Analyseverbundes (PIAV-S) geäußert. PIAV-S soll den Informations- und Nachrichtenaustausch zwischen den Polizeien des Bundes und der Länder erweitern. Zu dem Projekt sind meine datenschutzrechtlichen Bedenken noch nicht ausgeräumt. Bislang konnte noch nicht abschließend geklärt werden, ob die mit PIAV-S verarbeiteten Daten anonymisiert oder pseudonymisiert und damit personenbezogene Daten sind. Ich befinde mich mit dem BMI hierzu noch in einem Austausch.

Der Gesamtprogrammleiter machte deutlich, P20 – Polizei 20/20 sei von einer agilen Programmierung geprägt. In einem mit der AG INPOL abgestimmten Grundsatzschreiben habe ich mich zuletzt u. a. dazu geäußert, in welcher Form datenschutzrechtliche Anforderungen innerhalb agiler Programmierungsprozesse umgesetzt werden müssen. Insbesondere müssen datenschutzrechtliche Vorgaben vor Beginn der agilen Entwicklung vollständig festgelegt und belastbar dokumentiert werden.

Querverweise:

6.25 Agile Projektentwicklung

6.15 GETZ: Unzureichende Evaluation

Das 2012 gegründete Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ) dient der Bekämpfung der politisch motivierten Kriminalität und des Terrorismus sowie von Spionage und Proliferation. Eine ernsthafte Evaluation dieser Einrichtung scheint jedoch nicht gewollt zu sein.

Im GETZ treffen sich regelmäßig alle großen Bundes- und Landesbehörden (insgesamt 40) aus den Bereichen Polizei, Nachrichtendienste und Strafverfolgung. Dort tauschen sie sich informell zu Entwicklungen und Trends in den verschiedenen „Phänomenbereichen" aus. Ich bewerte die datenschutzrechtliche Ausgestaltung der Arbeit im GETZ generell kritisch, da es das im Nachkriegsdeutschland eingeführte Trennungsgebot zwischen Polizei und Nachrichtendiensten betrifft und der Informationsaustausch dort zudem sehr intransparent ist.

Im Frühjahr des Jahres 2020 wurde mir durch das Bundesinnenministerium (BMI) auf mehrmalige Bitte hin ein Evaluationsbericht zum GETZ aus dem Jahr 2017 übersandt. Aufgrund einer Einstufung als Verschlusssache kann ich auf Inhalte des Berichts hier nicht eingehen.

Schildern kann ich jedoch, dass ich die Evaluation für methodisch unzureichend sowie lückenhaft und daher im Ergebnis nicht hilfreich halte. Dies beginnt damit, dass keine unabhängige Stelle, sondern eine der beteiligten Behörden, mit der Evaluation beauftragt wurde. Der Gegenstand der Evaluation, das GETZ und seine Arbeitsprozesse, wird in dem Bericht nicht näher beschrieben. Das Thema Datenschutz wurde vollständig aus der Evaluation ausgeklammert – und das bei einem Gesprächszirkel aus Polizeibehörden und Nachrichtendiensten, dessen Inhalte unbekannt bleiben. Wie viele Straftaten durch den konkreten Informationsaustausch verhindert oder aufgeklärt wurden, ist ebenfalls nicht Thema. Auch eine Dokumentation der Evaluation ist faktisch nicht vorhanden, so dass eine eigene Einschätzung der Ergebnisse des Berichts nicht möglich ist.

Insgesamt drängte sich mir der Eindruck auf, dass das Hauptziel der Evaluation die Legitimation der politischen Entscheidung zur Einrichtung des GETZ war. Eine unabhängige und objektive Evaluation im Sinne einer kritischen Erfolgsanalyse war offensichtlich nicht gewollt. Meine Kritik habe ich dem BMI im Mai 2020 mitgeteilt und eine neue Evaluation dringend angeregt, ohne dass eine Reaktion erfolgte. Im Jahr 2021 habe ich nochmals nachgehakt, jedoch ebenfalls keine Antwort erhalten. Erst auf meine Information hin, dass ich diesen Beitrag in den Tätigkeitsbericht aufnehmen werde, teilte das BMI mir mit, dass mir augenscheinlich unvollständige Unterlagen zur Verfügung gestellt worden waren. Diese werde ich nun anfordern und gegebenenfalls weiter berichten.

6.16 Datenverarbeitung beim BND

Die Herstellung datenschutzkonformer Zustände beim Bundesnachrichtendienst (BND) braucht zuweilen einen langen Atem. Schon im Jahr 2009 hatte ich datenschutzrechtliche Verstöße im Rahmen des Betriebes einer zentralen Großdatei beim BND festgestellt. Diese wurden bis heute nicht vollständig behoben.

Bereits in meinem 23. Tätigkeitsbericht habe ich über datenschutzrechtliche Verstöße in einer beim BND geführten Großdatei berichtet. Unter anderem hatte der BND in dieser Großdatei keine den gesetzlichen Vorgaben entsprechende Wiedervorlage- und Löschungsüberprüfungen implementiert und durchgeführt. Dies hatte zur Konsequenz, dass sich in dieser Datei personenbezogene Daten befanden, deren Verarbeitung nicht mehr erforderlich und damit unzulässig war. Gleichwohl ist eine Löschung dieser Daten nicht erfolgt.

Ende 2015 implementierte der BND eine systemseitige Wiedervorlage zur Überprüfung der Erforderlichkeit einer weiteren Verarbeitung oder ggf. Löschung personenbezogener Daten in der Großdatei. Dies hatte zur Folge, dass sich der Datenbestand in der Großdatei insbesondere in zwei Datenarten aufspaltete. Zum einen in solche Daten, für die eine gesetzeskonforme Löschwiedervorlage implementiert wurde, und zum anderen in solche Daten, die vor der Implementierung der Wiedervorlagefunktion in der Großdatei enthalten waren. Für letztere wurde die Wiedervorlagefunktion nicht in Funktion gesetzt, so dass diese nach zehn Jahren im aktiven Bestand ohne eine Erforderlichkeitsprüfung in den Datenschutzarchivbereich der Großdatei überführt werden.

Dieses Vorgehen halte ich auch weiterhin für datenschutzrechtlich bedenklich.

Eine nichttechnische Lösung zur Herstellung eines gesetzeskonformen Zustandes mittels Durchsicht der in der Datei enthaltenen Dokumente nach löschpflichtigen personenbezogenen Daten hat der BND bis zum heutigen Tag mit dem Verweis auf den nicht leistbaren Aufwand abgelehnt. Eine Löschung des überwiegenden Archivbestandes wurde seitens BND und Bundeskanzleramt (BKAmt) mit dem Verweis auf die Notwendigkeit des Vorhaltens der Informationen für den politischen Raum (z. B. Untersuchungsausschüsse) lange verweigert.

Im Jahr 2018 erfolgte eine Wendung dahingehend, dass das BKAmt nunmehr eine Löschung des Archiv

bestandes ohne Nennung eines Termins in Aussicht stellte. Zu klären seien jedoch zunächst archivrechtliche Fragestellungen mit dem Bundesarchiv. Ich habe diesen Klärungsprozess aktiv unterstützt und weiter darauf hingewiesen, dass die gesetzwidrig gespeicherten personenbezogenen Daten zu löschen sind. Sofern eine Trennung der personenbezogenen von den nicht-personenbezogene Daten realisierbar wäre, könnten letztere natürlich auch weiterhin archiviert werden. Ist dies jedoch nicht möglich, müsste das gesamte Archiv gelöscht werden.

Eine Klärung der genannten Fragestellung zwischen BND, BKAmt und Bundesarchiv konnte bis zum Redaktionsschluss dieses Tätigkeitsberichts nicht herbeigeführt werden.

Wenngleich der Datenschutzarchivbereich nicht aktiv genutzt wird, sondern nur in eng umgrenzten Ausnahmefällen zugänglich ist, wächst er bis heute stetig an.

Ich werde die weitere Entwicklung beobachten und auch zukünftig auf einen datenschutzkonformen Zustand der Datei drängen.

6.17 Überführung der Stasi-Akten ins Bundesarchiv

Seit dem 17. Juni 2021 gehört das Stasi-Unterlagen-Archiv zum Bundesarchiv. An den gesetzlichen Regelungen für den Umgang mit den Stasi-Unterlagen ändert sich zunächst nichts.

Mit dem Inkrafttreten des Gesetzes zur Änderung des Bundesarchivgesetzes, des Stasi-Unterlagen-Gesetzes (StUG) und zur Einrichtung einer SED-Opferbeauftragten wurde die Behörde des Bundesbeauftragten für die Stasi-Unterlagen aufgelöst. Seit dem 17. Juni 2021 gehört diese als Stasi-Unterlagen-Archiv zum Bundesarchiv. Eine Veränderung der rechtlichen Grundlagen in Bezug auf die Stasi-Unterlagen ist hiermit nicht verbunden. Es gelten somit die bisherigen Regelungen des StUG für die Arbeit mit den Unterlagen, aber auch hinsichtlich des Zugangs zu diesen, fort.

Dies begrüße ich, da es sich auch weiterhin um kein allgemeines Archivgut handelt, wie es durch das Bundesarchiv im Übrigen verwaltet wird. Die Stasi-Unterlagen enthalten höchstpersönliche Daten, die in der Regel mit unrechtmäßigen Mitteln beschafft oder sogar konstruiert wurden und somit eines besonderen Schutzes und speziellen Zugangsregelungen bedürfen. Ich werde mich daher auch bei künftigen Kontrollen davon überzeugen, dass diese Standards wie bisher eingehalten werden. Ein besonderes Augenmerk wird dann geboten sein, wenn die beabsichtigte Zusammenlegung der Unterlagen von mehreren bisherigen Außenstellen erfolgt.

6.18 Anwendungen auf der elektronischen Gesundheitskarte

Mit dem Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG), das zum 9. Juni 2021 in Kraft getreten ist, wurden einige Anwendungen der Telematikinfrastruktur (TI) neu eingeführt und existierende neu geregelt. In meiner Beratung zur technischen Umsetzung der neuen Anforderungen achte ich darauf, dass eine Trennung der Datenverarbeitung der verschiedenen Anwendungen gewährleistet bleibt.

Bisher waren die Anwendungen Notfalldatensatz und elektronischer Medikationsplan auf der elektronischen Gesundheitskarte (eGK) vorgesehen. Der Notfalldatensatz wird nun in die neue elektronische Patientenkurzakte (ePKA) aufgenommen. Der Medikationsplan wird in eine eigene Anwendung in der TI, ohne Speicherung auf der eGK, überführt. Versicherte haben für einen Übergangszeitraum eine Wahlmöglichkeit, welches System sie nutzen wollen.

Auch wenn die ePKA ähnlich benannt ist wie die elektronische Patientenakte (ePA), erfüllt sie einen anderen Zweck. Hier sollen fest definierte, strukturierte Notfalldaten hinterlegt werden können. Diese Daten dienen dazu, dass beispielsweise Rettungssanitäter auch ohne technische Freigabe des Versicherten einen Überblick über relevante Vorerkrankungen und den Gesundheitsstand erhalten können. Außerdem bilden sie die Grundlage für den Datenaustausch zu Ärztinnen und Ärzten im EU-Ausland. Hierzu müssen Versicherte eine Einwilligung abgeben, um überhaupt am europäischen System teilzunehmen, und zum Zeitpunkt der Behandlung im Ausland die Übermittlung durch eine eindeutige, bestätigende Handlung konkret technisch freigeben.

In meiner Beratung der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) zur technischen Konzeption von ePKA und elektronischem Medikationsplan setze ich mich dafür ein, dass die jeweiligen Datenverarbeitungen in der ePA, der ePKA und dem elektronischen Medikationsplans getrennt bleiben. Die Versicherten müssen die drei Anwendungen jeweils unabhängig voneinander wählen und darauf vertrauen können, dass in der jeweiligen Anwendung verarbeiteten Daten nicht gleichzeitig und ohne ihre aktive Mitwirkung in anderen Anwendungen zur Verfügung stehen. Eine Vermischung dieser Verarbeitungen, die z. B. dazu führen könnte, dass der Notfallzugriff der ePKA auch bei der ePA möglich ist, muss somit ausgeschlossen sein.

Da das DVPMG kein eindeutiges Einrichtungsverfahren für die ePKA vorsieht, habe ich außerdem angeregt, ein Vorgehen ähnlich zur Einrichtung der ePA zu nutzen, das eine Beantragung bei der Krankenkasse und dann die Ersteinrichtung beim Leistungserbringer vorsieht.

Das DVPMG führt ferner zu Änderungen beim E-Rezept, dessen aktuelle Testphase im Dezember 2021 verlängert wurde. So soll es für Privatrezepte möglich sein, die Rechnungsdaten auch im zentralen E-Rezept-Speicher abzulegen. Ein Schwerpunkt meiner Beratung der gematik liegt darauf, die Zugriffsmöglichkeiten auf diese Rechnungsdaten durch Dritte zu beschränken. Die App für das E-Rezept, die die gematik nicht nur spezifiziert, sondern auch selbst entwickelt, bietet als Zusatzfunktion Push-Benachrichtigungen an. Da diese Funktion über die Plattformen der mobilen Betriebssystemanbieter abgewickelt wird, war hier eine intensive Beratung notwendig. In technischer Hinsicht konnte ich die gematik davon überzeugen, die Inhalte zu verschlüsseln und auch die Meta-Daten durch das Verschicken von Leernachrichten zu verschleiern. Gleichzeitig habe ich eine umfangreiche datenschutzrechtliche Beratung im Hinblick auf mögliche Übermittlungen personenbezogener Daten an Drittländer geleistet, die Folgen aus dem Schrems-II-Urteil des Europäischen Gerichtshofs (s. Nr. 3.2.2.2) dargelegt und um deren Beachtung gebeten.

Ebenfalls aus dem DVPMG ergibt sich der Auftrag an die gematik, einen Sofortnachrichtendienst für die TI (TI-Messenger) zu entwickeln. Diesbezüglich habe ich die gematik bei der Konzeption und Spezifikation dieses Dienstes beraten und ein besonderes Augenmerk darauf gelegt, dass die Anforderungen, die die Datenschutzkonferenz (DSK) für Krankenhaus-Messenger in einem Whitepaper veröffentlicht hat, auch für den TI-Messenger berücksichtigt werden. Der Ende-zu-Ende-verschlüsselte TI-Messenger beruht auf dem Matrix-Protokoll und steht zunächst nur Leistungserbringern zur Verfügung. Im weiteren Verlauf des Jahres 2022 sollen ihn auch die Versicherten für die Kommunikation mit Krankenhäusern und Praxen nutzen können. Aus Sicht des Datenschutzes wäre das ein großer Fortschritt und gleichzeitig eine Beschleunigung in der medizinischen Versorgung.

6.19 Digitale Identitäten

Um digitale Verwaltungsprozesse zu nutzen, brauchen Bürgerinnen und Bürger eine sichere und einfach nutzbare Möglichkeit, sich online auszuweisen. Ich berate die Bundesregierung zu mehreren Projekten mit Bezug zu digitalen Identitäten und setze mich für eine Lösung ein, die auf sicherer Technologie basiert und Nutzende durch klare Regeln schützt.

Die Bundesregierung betreibt mehrere Teilprojekte (z. B. Smart-eID, ID-Wallet), die sich mit digitalen Identitäten beschäftigen. Gemeinsames Ziel dieser Teilprojekte ist es, den Bürgerinnen und Bürgern zu ermöglichen, sich online „ausweisen“ zu können. Die Bundesregierung hat die Teilprojekte im Projekt Digitale Identitäten des Bundesministeriums des Innern, für Bau und Heimat (BMI) gebündelt.

Onlineausweisfunktion des Ausweises

In Deutschland existiert mit dem eID-System bereits eine technische Infrastruktur für digitale Identitäten. 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 ausgestattete Dokumente).

Mit einem geeigneten Smartphone oder einem Kartenleser können die mit einem Chip ausgestatteten Ausweise genutzt werden, um Identitäten online rechtssicher nachzuweisen. Das System gilt als datenschutzfreundlich und sicher. So liegt die digitale Identität physisch getrennt vom Internet im Chip des Ausweises. Außerdem benutzt das System keine einheitliche Nummer für jeden Ausweis. Der Chip generiert vielmehr für jede Stelle, bei der der Ausweis „vorgelegt“ wird, eine eigene Nummer. Damit wird eine unerwünschte Profilbildung der Nutzenden über mehrere Dienste hinweg erschwert.

Da die Stellen, die Daten aus dem Ausweis online verarbeiten wollen, sich registrieren lassen müssen und ein Zertifikat ausgestellt bekommen, können Bürgerinnen und Bürger beim Einsatz des Ausweises sicher sein, ihre Identifikationsdaten nur gegenüber seriösen Anbietern offenzulegen.

Smart-eID

Kritisiert wird das eID-System aufgrund bisher geringer Einsatzmöglichkeiten sowie vermeintlich hoher Nutzungshürden durch die Kopplung an den physischen Ausweis.

Um die Nutzung des eID-Systems zu vereinfachen, wurden das Personalausweisgesetz (PAuswG), das

eID-Karte-Gesetz (eIDKG) und das Aufenthaltsgesetz (AufenthG) zum 1. September 2021 jeweils so erweitert, dass die Ausweisdaten auch auf ein mobiles Endgerät, z. B. ein Smartphone, mittels eines sicheren Verfahrens übertragen werden dürfen und dann ohne Einsatz der physischen Karte als elektronischer Identitätsnachweis dienen. Das hierzu als Erweiterung des eID-Systems entwickelte Verfahren wird als „Smart-eID" bezeichnet. Außerhalb des Smartphones wird die bereits bestehende eID-Infrastruktur für die Onlinefunktion des Personalausweises komplett wiederverwendet, so dass die aufgezeigten datenschutzfreundlichen Elemente dieser Infrastruktur auch hier greifen.

ID-Wallet

Gleichzeitig betreibt die Bundesregierung in Zusammenarbeit mit mehreren Unternehmen ein weiteres Teilprojekt, in dem eine ID-Wallet („elektronische Brieftasche") entwickelt wird. Dabei handelt es sich um eine App für das Smartphone, in der Bürgerinnen und Bürger alle Arten von Nachweis-Dokumenten speichern können sollen. Denkbar sind neben Daten aus Personalausweis oder Führerschein, z. B. auch Leistungsnachweise oder Mitgliedschaftsbescheinigungen.

Den technischen Hintergrund bildet eine Infrastruktur, die auf der Blockchain-Technologie basiert. Dazu wurde im Frühjahr 2021 mit der Anwendung „Hotel-Check-in" ein Pilotprojekt im nicht-öffentlichen Bereich gestartet. Hier wurde auf der Grundlage einer entsprechenden Erprobungsklausel in § 29 Bundesmeldegesetz (BMG) die ID-Wallet als weiteres elektronisches Verfahren zur Erfüllung des Melderechts erprobt.

Ziel der Bundesregierung ist es, die ID-Wallet darüber hinaus für alle Lebensbereiche zu öffnen und so zusammen mit der Blockchain-Infrastruktur ein sog. „Ökosystem" für selbstverwaltete Nachweise aller Art aus dem öffentlichen und nicht öffentlichen Bereich zu schaffen.

Aufgrund der aufsichtsbehördlichen Zuständigkeit der Landesdatenschutzbehörden für den nicht öffentlichen Bereich (z. B. Hotel-Betreiber) erfolgte meine Beratung mit Blick auf diese geplante Verwendung der ID-Wallet ausschließlich bezogen auf die seitens der Bundesregierung konzipierte Grundstruktur der App. Insoweit konnte ich aber bereits Fragen und Hinweise u. a. zur fraglichen Zweckmäßigkeit der Blockchain-Technologie und zur Sicherheit der ID-Wallet-App adressieren, die sowohl das Pilotprojekt als auch die spätere breitere Verwendung betreffen werden.

Gerade beim Einsatz der Blockchain-Technologie ergeben sich komplexe datenschutzrechtliche Fragen, die bislang noch nicht hinreichend geklärt werden konnten. Wenn personenbezogene Daten auf der Blockchain verarbeitet werden, muss es einen hierfür Verantwortlichen geben, an den sich Betroffene wenden können. Dieser muss unter anderem in der Lage sein, insbesondere auch das Recht auf Löschung oder Korrektur wahrzunehmen, was in einer auf Unveränderlichkeit ausgelegten Struktur wie der Blockchain-Technologie eine Herausforderung ist.

Verknüpfung der Smart-eID mit der ID-Wallet

Ein weiteres Ziel der Bundesregierung ist es, mit Hilfe einer sog. Basis-ID aus dem elektronischen Personalausweis abgeleitete Identifikationsdaten in der ID-Wallet bereitzustellen. Im August 2021 gab es hierzu eine Veranstaltungsreihe unter Hinzuziehung von Experten unterschiedlicher Disziplinen mit der Zielsetzung, Lösungen für eine Verknüpfung der Smart-eID und des Ökosystems der ID-Wallet zu entwickeln.

In Anbetracht einer Prüf- und Bewertungsfrist von lediglich zwei Wochen und in Ermangelung prüffähiger Dokumente habe ich meine erste Einschätzung anhand der Gewährleistungsziele des Standard-Datenschutzmodells vorgenommen. Dabei habe ich eine Präferenz für die Nutzung der (Smart-)eID-Infrastruktur zur Identifikation und zum dauerhaften Speichern der Identifikationsdaten ausgearbeitet, bei dem Verantwortlichkeiten bereits etabliert sind das Sicherheitsniveau bekannt und eine Rechtsgrundlage vorhanden ist.

ID-Wallet-App mit Führerschein-Nachweis

Am 23. September 2021 veröffentlichte die Bundesregierung überraschend die ID-Wallet-App. Die Veröffentlichung erfolgte aber nicht in der Smart-eID-verknüpften Form des Pilotprojektes („Hotel-Check-in"), zu der meine Beratung erfolgte, sondern mit dem Führerschein-Nachweis als erstem Anwendungsfall. Weder über diesen Veröffentlichungszeitpunkt noch über die Planungen zur Einbindung des Führerschein-Nachweises war ich im Vorfeld informiert.

Diese App-Variante musste bereits nach einer Woche wieder zurückgezogen werden, um Datenmissbrauch zu vermeiden. Sicherheitsforscherinnen und -forscher hatten Möglichkeiten aufgezeigt, das System anzugreifen und die Nutzenden über die wahren Empfänger ihrer Daten zu täuschen.

Zusammenfassende Bewertung der Aktivitäten der Bundesregierung

Die Bestrebungen der Bundesregierung zur Ermöglichung einer besseren Nutzbarkeit digitaler Identitäten sind – wie oben dargestellt – in mehreren parallel betriebenen Teilprojekten verteilt. Um digitale Verwaltungsprozesse im öffentlichen und nicht-öffentlichen Bereich medienbruchfrei zu nutzen, brauchen Bürge

rinnen und Bürger eine sichere und einfach nutzbare Möglichkeit, sich online auszuweisen. Die Vorgaben zur Umsetzung solcher Prozesse sollten in erster Linie durch den Staat gestaltet werden, um sich nicht den Regeln großer Technologiekonzerne unterwerfen zu müssen. Die Grundvoraussetzung für ein Identifikationssystem ist mit der eID-Infrastruktur, basierend auf etablierter Technik, vorhanden. Durch den Ausbau der bisher eher überschaubaren Einsatzmöglichkeiten elektronischer Identitäten könnte auch aus meiner Sicht ein größerer Nutzungsanreiz gesetzt werden. Auch Erweiterungen und Vereinfachungen der Nutzungsoberfläche sind sinnvoll, wenn sie sicherstellen, dass die mit der eID erreichbare Verbesserung der Datenhoheit der Bürgerinnen und Bürger im digitalen Bereich auch effektiv zum Tragen kommt.

Ein digitales Nutzungssystem, das Bürgerinnen und Bürgern ihre Identifikationsdaten und weitere Attribute wie Zeugnisse in ihrer eigenen Verwendungshoheit belässt, begrüße ich daher prinzipiell. Allerdings führt der Ansatz, dass Betroffene selbst ihre Daten verwalten, allein noch nicht zur Datensouveränität. Es muss auch sichergestellt sein, dass sie informiert und ohne Nachteile entscheiden können, wem sie welche Daten offenbaren. Zudem wird ein klares Regelwerk benötigt, das Verantwortliche und deren Pflichten benennt und Bürgerinnen und Bürger systematisch schützt. Technisch muss die Lösung so ausgereift sein, dass sie in der Lage ist, Betrug und Datenabfluss zu verhindern. Hierfür werde ich mich auch weiterhin bei der Beratung zum Gesamtprojekt „Digitale Identitäten“ einsetzen.

6.20 Das Sicherheitsüberprüfungsgesetz – Ein Gesetz mit vielen Fragezeichen

Das Sicherheitsüberprüfungsgesetz (SÜG) regelt einen Teilbereich der nationalen Sicherheit und enthält hierzu auch spezielle datenschutzrechtliche Regelungen. In der Praxis hat sich gezeigt, dass an einigen Stellen noch nachgebessert werden muss. Die aktuell anstehende Evaluierung des SÜG ist hierfür eine gute Gelegenheit.

Das Sicherheitsüberprüfungsrecht unterliegt der besonderen Herausforderung, die unterschiedlichen Interessen des Staates und des Einzelnen möglichst ins Gleichgewicht zu bringen. Den Sicherheitsinteressen des Staates steht hierbei das Recht auf informationelle Selbstbestimmung des Einzelnen gegenüber, der im Rahmen der Sicherheitsüberprüfung einige auch höchstpersönliche Daten preisgeben muss. Um vertrauliche Informationen zu bewahren und lebenswichtige Einrichtungen für den Staat sowie seine Bürgerinnen und Bürger vor Sabotage zu schützen, überprüfen staatliche Stellen vorab alle Personen, die Zugang zu solchen Informationen und Einrichtungen erhalten sollen, in einer sog. Sicherheitsüberprüfung. Hierbei erheben verschiedene Behörden umfangreiche Daten bei der betroffenen Person sowie in deren Umfeld und verarbeiten diese. Jede Datenverarbeitung ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Solche Eingriffe erfordern klare Grenzen und eine Rechtsgrundlage. Das SÜG regelt deshalb die Voraussetzungen und das Verfahren der Sicherheitsüberprüfungen und beinhaltet besondere Regelungen zum Datenschutz.

In der Praxis hat sich in der Vergangenheit jedoch gezeigt, dass es im Gesetz einige Regelungslücken gibt, die die Anwender des Rechtes vor zum Teil große Probleme stellen. Mit diesem Artikel möchte ich daher exemplarisch einige Lücken oder Unstimmigkeiten im SÜG aufzeigen.

Folgende Fragen müssen mittels gesetzlicher Regelungen beantwortet werden:

1. Haben Datenschutzbeauftragte eines Unternehmens das Recht, die dort geführten Sicherheitsakten einzusehen?

   Nach der aktuellen Gesetzeslage ergibt sich für Datenschutzbeauftragte in Behörden ein Einsichtsrecht gem. § 36 SÜG i. V. m. §§ 5 ff. BDSG. Diese Regelung gilt zumindest ihrem Wortlaut nach nicht unmittelbar auch für Datenschutzbeauftragte in Unternehmen. Ein Grund dafür, das Einsichtsrecht hier unterschiedlich zu regeln, liegt meines Erachtens nicht vor.

   Die Letztverantwortung für den Inhalt der Sicherheitsakten und die dazu gespeicherten und verarbeiteten personenbezogenen Daten liegt bei der Unternehmensleitung/Geschäftsführung des betroffenen Unternehmens. Zur ordnungsgemäßen Erfüllung der datenschutzrechtlichen Vorgaben auch im Bereich des SÜG kann (oder muss) diese einen betrieblichen Datenschutzbeauftragten bestellen. Es kann nicht im Sinne des Gesetzgebers sein, dass meine Behörde hier der einzige Ansprechpartner für Unternehmen und Betroffene ist. Die Verpflichtung, eine ordnungsgemäße Datenverarbeitung zu gewährleisten, wird den Unternehmen erschwert, wenn sie sich im Bereich des SÜG nicht eines betrieblichen Datenschutzbeauftragten bedienen können.

   Ich vertrete daher die Auffassung, dass auch in Unternehmen Datenschutzbeauftragten ein Einsichtsrecht in dort geführten Sicherheitsakten zustehen muss. Die Gesetzeslage ist hier nicht eindeutig. Deshalb sollte der Gesetzgeber im SÜG selbst eine

Regelung zum Einsichtsrecht der Datenschutzbeauftragten in nichtöffentlichen Stellen treffen. Zwecks Klarstellung der Gleichbehandlung der Datenschutzbeauftragten im öffentlichen und nichtöffentlichen Bereich empfehle ich das Einsichtsrecht beider Datenschutzbeauftragten gemeinsam im SÜG zu regeln.

2. Wer ist der richtige Adressat einer Beanstandung im nichtöffentlichen Bereich?

   In § 36 a Abs. 2 SÜG ist meine Zuständigkeit für datenschutzrechtliche Kontrollen sowohl bei öffentlichen als auch nichtöffentlichen Stellen geregelt, soweit sie Aufgaben dieses Gesetzes erfüllen. Jedoch fehlt im nichtöffentlichen Bereich eine klare Regelung dahingehend, wem gegenüber ich meine Kontrollergebnisse – insbesondere Beanstandungen – adressiere. Eine Ergänzung des § 36a SÜG, die den Adressaten der jeweiligen Kontrollergebnisse regelt, wäre hier wünschenswert.

3. Welche Maßnahmen sind durch das Bundesamt für Verfassungsschutz (BfV) bei einer Sicherheitsüberprüfung auf Antrag ausländischer Dienststellen nach § 33 SÜG durchzuführen?

   Welche Maßnahmen bei den unterschiedlichen Arten der Sicherheitsüberprüfungen durchzuführen sind, regelt § 12 SÜG. Nicht geregelt ist hingegen, welche Maßnahmen erfolgen sollen, wenn eine Überprüfung auf Antrag einer ausländischen Stelle durchgeführt wird. Darüber hinaus bedarf es hier auch weiterer Regelungen zum Umgang mit den erhobenen personenbezogenen Daten, wie etwa Bestimmungen zur Vernichtung und Löschung.

4. Auf welcher Grundlage kann die Datenübermittlung im Rahmen des in der Wirtschaft häufig auftretenden Besuchskontrollverfahrens erfolgen?

   Ist hier eine Einwilligung seitens der Betroffenen zur Datenweitergabe möglich?

   Nach der geltenden Rechtslage ist die Weitergabe von personenbezogenen Daten im Rahmen des sog. „Besuchskontrollverfahrens“ nicht gesetzlich geregelt. Das Besuchskontrollverfahren kommt zum Einsatz, wenn sicherheitsüberprüftes Personal ein anderes als das Beschäftigungsunternehmen oder eine staatliche Stelle besuchen soll und dabei der Zugang zu Verschlusssachen erforderlich oder möglich ist.

   Weder das SÜG noch das BDSG enthalten Regelungen dazu, unter welchen Voraussetzungen oder gar welche personenbezogenen Daten an die besuchte Stelle zu übermitteln sind. Ebenfalls bleibt der Umgang mit den Daten bei der aufnehmenden Stelle ungeregelt.

   Die Datenweitergabe erfolgt derzeit aufgrund einer von den Betroffenen abgegebenen Einwilligung (Anlage 19h zum Geheimschutzhandbuch des Bundesministeriums für Wirtschaft und Energie).

   Problematisch ist hier, dass § 36 SÜG den § 51 Abs. 1 BDSG für entsprechend anwendbar erklärt. Dieser regelt Anforderungen an die Qualität der Einwilligung und deren Nachweis, soweit eine Datenverarbeitung auf der Grundlage einer Einwilligung per Rechtsvorschrift zugelassen ist. Im SÜG findet sich, wie vorstehend bereits erwähnt, aber eben keine derartige Regelung. Der Verweis auf § 51 BDSG scheint zu kurz gegriffen für den Bereich des SÜG. Es erscheint mehr als fraglich, ob das Erfordernis einer durch Rechtsvorschrift zugelassenen Einwilligung tatsächlich im Interesse des Gesetzgebers gewesen ist. Soweit hier allein auf die Anforderungen an die Einwilligung und die Nachweispflicht verwiesen werden sollte, ist dies jedenfalls nicht eindeutig.

   Sinnvoll wäre es auch hier, für das Besuchskontrollverfahren eine passende Regelung im SÜG selbst aufzunehmen. Alternativ könnte man den Verweis auf § 51 Abs. 1 BDSG auf Modalitäten und Nachweis der Einwilligung beschränken, sodass eine Einwilligung seitens der Betroffenen nicht mangels bestehender Regelung im SÜG gesperrt würde.

Ich werde die aus meiner Sicht notwendigen Ergänzungen und Änderungen im SÜG der neuen Bundesregierung erläutern und diese um Prüfung sowie mögliche Umsetzung meiner Anregungen bitten.

Nun ist der Gesetzgeber gefragt!

Ich empfehle, das Einsichtsrecht der betrieblichen Datenschutzbeauftragten in die im Unternehmen geführten Sicherheitsakten, den Adressaten einer Beanstandung im nichtöffentlichen Bereich, den Umfang der Maßnahmen bei Sicherheitsüberprüfungen gem. § 33 SÜG sowie die Datenübermittlung im sogenannten Besuchskontrollverfahren im SÜG zu regeln.

6.21 Pilotprojekt zur „intelligenten“ Videoüberwachung am Bahnhof Berlin Südkreuz, 2. Teil

Der Abschlussbericht des 2. Teils des Projektes weist allenfalls erste Ansätze für die geplante Nutzung aus, die Software genügt den Anforderungen eines Einsatzes im komplexen Umfeld eines Bahnhofes bei weitem nicht. Das Projekt wird bis Ende 2021 fortgeführt.

In der Vergangenheit habe ich in meinem 27. Tätigkeitsbericht (Nr. 9.3.3) und in meinem 28. Tätigkeitsbericht (Nr. 6.2) schon von dem Pilotprojekt zur intelligenten Videoüberwachung am Bahnhof Südkreuz in Berlin berichtet. Dort testete die Deutsche Bahn AG zusammen mit der Bundespolizei im ersten Teil Software zur biometrischen Gesichtserkennung (s. o. g. Tätigkeitsberichte). Im zweiten Teil wurde im Herbst 2019 Software von drei verschiedenen Herstellern zur Erkennung von verschiedenen Gefahrensituationen, sowie zur Nachverfolgung der Positionen von Personen oder Gegenständen und zur retrograden Auswertung von Videodaten getestet. Mitte Mai 2021 wurde mir der Testbericht (Stand 23. November 2020) zur Kenntnis gegeben. Im Ergebnis wird dort festgestellt, dass keine Software den Anforderungen genügte, lediglich vielversprechende Ansätze zur Lösung konnte in vielen Fällen konstatiert werden. Zur Erinnerung: getestet wurde die Situation „liegende Person“, z. B. eine gestürzte Person die Hilfe benötigt, die Situation „Betreten definierter Bereiche“, z. B. Personen, die sich zu nahe an der Bahnsteigkante befinden, die Situation „Personenströme/Ansammlungen“, z. B. Ansammlungen vor Fahrtreppen, die Situation „Personenzählung“, d. h. zählen von Personen in einem festgelegten Bereich, sowie die Situation „abgestellte Gegenstände“, das sind Gepäckstücke die eine längere Zeit unbeaufsichtigt abgestellt werden. Diese Situationen wurden federführend von der Deutschen Bahn AG getestet, die o. g. Situationen „Nachverfolgung von Positionen“ und „retrograde Auswertung von Videodaten“ wurden unter Federführung der Bundespolizei getestet.

In den Situationen unter der Federführung der DB-AG war durchgehend die Fehlalarmierungsquote zu hoch, teilweise wurden Situationen nicht vom System erkannt. Einzig die Visualisierung von Personenströmen und Ansammlungen gelang allen Systemen. Die Situation „Nachvollziehen von Positionen“ konnte von einem Hersteller gar nicht umgesetzt werden, der zweite Hersteller konnte die Positionen nicht kameraübergreifend nachvollziehen und der dritte Hersteller benötigte zur Umsetzung der Anforderungen umfangreiche Nachkonfigurationen der Software, die als zu umfangreich erkannt wurden. Zur retrograden Auswertung der Videodaten erwies sich keines der Systeme als geeignet für den bundespolizeilichen Einsatz.

Zu den Rahmenbedingungen des Tests gehörte, dass die Erkennung von Personen nicht aufgrund biometrischer Merkmale erfolgen durfte. Die Hersteller sicherten daher zu, dass mögliche biometrische Module der Software vorab deaktiviert wurden. Es wurde ein Teil der bereits vorhandenen Videokameras am Bahnhof Südkreuz genutzt, die Szenen wurden von Darstellern gespielt und jeweils in einem deutlich markierten Bereich aufgenommen. Damit war sichergestellt, dass Passanten die Bereiche meiden konnten und nicht unfreiwillig gefilmt wurden. Die Öffentlichkeit wurde durch Hinweisschilder und Informationen in der Presse informiert, die wissenschaftliche Begleitung des Projektteils erfolgte durch die ITIS GmbH der Universität der Bundeswehr in München. Der Bericht endet mit der Empfehlung, die Videoanalysetechnik weiterzuentwickeln und zu erproben. Der Test solle dabei auch auf weitere Softwareanbieter ausgedehnt werden.

Dieses schlechte Testergebnis sollte nach meinem Dafürhalten nicht die Grundlage weiterer, ähnlich aufwendiger Tests sein, sondern – wenigstens zum jetzigen Zeitpunkt – das Ende derartige Tests bedeuten. Vielmehr sollte die Gelegenheit ergriffen werden, die Steigerung der Sicherheit der Bahnhöfe durch andere Maßnahmen zu erreichen.

Der Innenminister hat in einer Pressemitteilung vom Dezember 2020 jedoch schon angedeutet, dass die Tests fortgeführt werden sollen. Letzten Informationen zufolge werden die Tests des zweiten Projektteils bis zum Ende des Jahres 2021 fortgeführt. Weitere Details liegen mir noch nicht vor.

6.22 Eurojust, Europäische Staatsanwaltschaft: Neue Zuständigkeiten

Die strafjustizielle Zusammenarbeit auf europäischer Ebene gewinnt zunehmend an Bedeutung. Hierfür stehen insbesondere neuere Rechtsakte für Eurojust und die Europäische Staatsanwaltschaft. Um den Datenschutz in diesem Bereich sicherzustellen, arbeite ich auf nationaler und europäischer Ebene in verschiedenen Gremien mit.

Eurojust

Bei Eurojust handelt es sich um eine Einrichtung der Europäischen Union, welche die Justizbehörden der Mitgliedstaaten bei der grenzüberschreitenden Zusammenarbeit unterstützt. Dies betrifft beispielsweise die

Bekämpfung von Terrorismus, Drogen- oder Waffenhandel. Da es sich bei Eurojust selbst um eine europäische Einrichtung handelt, liegt die Aufsicht bei dem Europäischen Datenschutzbeauftragten (EDSB). Meine Aufgabe ist es, gemeinsam mit den Datenschutzbeauftragten der Länder die Übermittlungen von personenbezogenen Daten durch die deutschen Strafverfolgungsbehörden an Eurojust zu beaufsichtigen. Dementsprechend habe ich z. B. geprüft, ob sichere Kommunikationskanäle zwischen Eurojust und den nationalen Stellen vorhanden sind. Auch habe ich ein Informationsgespräch mit dem deutschen Mitglied bei Eurojust geführt, in dem insbesondere Fragen zur konkreten Arbeitsweise von Eurojust im europäischen Mehrebenensystem geklärt werden konnten.

Europäische Staatsanwaltschaft

Bei der Europäischen Staatsanwaltschaft (EUStA) handelt es sich um eine neue Einrichtung auf europäischer Ebene, die ihre Arbeit am 1. Juni 2021 aufgenommen hat. Die EUStA ist für Straftaten gegen die finanziellen Interessen der Union zuständig und verfolgt Straftaten zu Lasten des EU-Haushalts. Dazu kann sie Ermittlungen durchführen, Strafverfolgungsmaßnahmen ergreifen und vor den zuständigen Gerichten der Mitgliedstaaten die Aufgaben der Staatsanwaltschaft wahrnehmen. Deutschland ist einer der 22 Mitgliedstaaten, die im Rahmen der verstärkten Zusammenarbeit an der EUStA teilnehmen. Bei ihrer Ermittlungsarbeit ist die EUStA befugt, auf nationale Strafverfolgungsbehörden zurückzugreifen, so dass sich meine Aufsichtstätigkeit primär auf die Einhaltung datenschutzrechtlicher Vorgaben bei den betroffenen Strafverfolgungsbehörden des Bundes bezieht. Aufgrund der erst kürzlich erfolgten Arbeitsaufnahme der europäischen Einrichtung setze ich mich ferner mit den Datenschutzaufsichtsbehörden der teilnehmenden Mitgliedstaaten sowie dem primär zuständigen EDSB über die organisatorische Ausgestaltung der EUStA in den Mitgliedstaaten sowie die Klärung offener Zuständigkeitsfragen auseinander. Insgesamt handelt es sich hierbei um eine neue Aufgabe im Rahmen meiner aufsichtsrechtlichen Zuständigkeit.

Koordinierte Aufsicht von Eurojust und Europäischer Staatsanwaltschaft (Coordinated Supervision Committee, CSC)

Um eine koordinierte Aufsicht von Eurojust und EUStA in der EU sicherzustellen, kommen die Mitglieder der europäischen Aufsichtsbehörden und der EDSB im sog. Ausschuss für koordinierte Aufsicht (CSC) zusammen. In diesem Gremium werden gemeinsame Vorgehensweisen zu grenzüberschreitenden Aufsichtsthemen festgelegt. Die Repräsentanz der deutschen Aufsichtsbehörden übe ich gemeinsam mit zwei Vertretungen der Landesdatenschutzbehörden aus.

6.23 Zusammenarbeit mit anderen Kontrollorganen im Bereich der Nachrichtendienste des Bundes

In diesem Jahr habe ich die Zusammenarbeit mit der G10-Kommission und dem Parlamentarischen Kontrollgremium im Rahmen mehrerer Gespräche auf unterschiedlichen Ebenen intensiviert und wichtige Weichen für unsere künftige Zusammenarbeit gestellt.

Die in den letzten Jahren begonnene Zusammenarbeit mit der G 10-Kommission und dem Parlamentarischen Kontrollgremium (PKGr) habe ich in diesem Jahr weiter fortgesetzt. Dazu fand ein gemeinsamer Jour Fixe mit der G 10-Kommission auf Arbeitsebene statt.

Auch die Zusammenarbeit mit dem PKGr konnte nach dem Antrittsbesuch von Herrn Kiesewetter, dem Vorsitzenden des Gremiums in der 19. Legislaturperiode, in meiner Bonner Dienststelle weiter ausgebaut werden. Das kollegiale und vertrauensvolle Gespräch mit Herrn Kiesewetter führte zu einem Austausch mit dem Ständigen Bevollmächtigten, Herrn Schlatmann, und einem weiteren Termin auf Arbeitsebene. Dies wollen wir mit den Verantwortlichen der 20. Legislaturperiode fortsetzen. Mit der Intensivierung dieser Kontakte sollen bereits im Vorfeld aktiv die Weichen für eine konstruktive künftige Zusammenarbeit gestellt werden, die für mich von besonderer Bedeutung ist. Damit möchte ich auch den Änderungen des PKGr-Gesetzes Rechnung tragen, die am 1. Januar 2022 in Kraft treten. Das Gesetz sieht zukünftig einen engeren Austausch mit den Kontrollorganen über die Nachrichtendienste des Bundes vor (G 10-Kommission, BfDI sowie der neu geschaffene Unabhängige Kontrollrat) und mit dem PKGr als dem verbindenden Element. Ich verstehe die Gesetzesänderung nicht nur als gesetzlichen Auftrag, sondern auch als Chance, die gemeinsame Zusammenarbeit weiter auszubauen und positiv zu prägen, um so dem Datenschutz mit seiner stetig wachsenden Bedeutung auch auf dieser Ebene gerecht zu werden.

6.24 Passenger Name Records (PNR) – Zentrale Fragen sind weiterhin ungeklärt

Beim Europäischen Gerichtshof (EuGH) und auch bei deutschen Gerichten sind weiterhin Verfahren anhängig, mit denen die Rechtmäßigkeit der Verarbeitung von Fluggastdaten zur Bekämpfung von Terrorismus und anderen schweren Straftaten geklärt werden soll. Zudem liegen nun erste Zahlen zum Einsatz von abstrakten Gefährdungsmustern in Deutschland vor, die meine Zweifel an der Vereinbarkeit mit den Grundrechten bestärken.

Den Umfang der Verarbeitung von Fluggastdaten durch Polizeibehörden halte ich für unverhältnismäßig. Hierauf habe ich bereits in vergangenen Berichtsjahren wiederholt hingewiesen (vgl. 22. TB Nr. 13.5.4; 26. TB Nr. 2.3.2; 27. TB Nr. 1.3; 28. TB Nr. 6.4; 29. TB Nr. 6.6). Die Richtlinie (EU) 2016/681 vom 27. April 2016 über die Verwendung von Fluggastdatensätzen zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (PNR-RL) verpflichtet die Mitgliedstaaten, anlasslos und permanent Fluggastdaten von Luftfahrtunternehmen zu erheben, abzugleichen und über fünf Jahre zu speichern, um auch eine rückwirkende Auswertung zu ermöglichen. Deutschland hat die PNR-RL mit dem Fluggastdatengesetz (FlugDaG) umgesetzt.

Die Datenbestände können insbesondere automatisiert mit Fahndungsdatenbanken abgeglichen werden, aber auch mit vorher erstellten Mustern. Erfüllt eine Person die Kriterien eines solchen Musters (z. B. Art der Buchung, gewählte Flugroute etc.), ist dies vergleichbar mit einem Treffer beim Abgleich mit einer polizeilichen Datenbank. Es entsteht eine Art Verdacht, dass die betroffene Person eine der im FlugDaG genannten terroristischen und weiteren schweren Straftaten begangen hat oder innerhalb eines übersehbaren Zeitraumes begehen wird. Personen können so in den Fokus von Bundeskriminalamt (BKA) und Landeskriminalämtern, Zoll und Bundespolizei, aber auch des Bundesamts und der Landesämter für Verfassungsschutz, des militärischen Abschirmdienstes oder des Bundesnachrichtendienstes, geraten.

Dass ich, ebenso wie meine Kolleginnen und Kollegen in Europa, das positive Fazit der EU-Kommission in der Evaluierung zur Umsetzung der PNR-RL anzweifle, habe ich bereits zum letzten Berichtsjahr deutlich gemacht (vgl. 29. TB Nr. 6.6). Auch die nunmehr vorliegenden Zahlen zu den ersten zwei Jahren der Nutzung von Mustern in Deutschland lassen erhebliche Zweifel an der Verhältnismäßigkeit der Musterabgleiche aufkommen.

Zudem konnte die Musterfunktionalität das gesetzliche Ziel, Personen zu identifizieren, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie eine Terrorismus-bezogene Straftat im Sinne des FlugDaG begangen haben oder innerhalb eines übersehbaren Zeitraumes begehen werden, in den ersten zwei Jahren nicht fördern. Hinzu kommt, dass die Anwendung von Musterabgleichen auf Flügen innerhalb der Europäischen Union (EU) keineswegs zur Umsetzung der sog. PNR-Richtlinie ((EU) 2016/681) erforderlich ist. Hierdurch wird die Zahl der Grundrechtseingriffe noch einmal erheblich vergrößert, ohne dass eine entsprechende Erforderlichkeit erkennbar ist.

Spätestens seit dem **Gutachten** vom 26. Juli 2017 zum geplanten Fluggastdaten-Abkommen zwischen Kanada und der EU des EuGH ist deutlich geworden, dass es dringend nötig ist, die Erkenntnisse auch mit Blick auf die PNR-RL und das FlugDaG umzusetzen (vgl. 28. TB Nr. 6.4). Die laufenden Vorabentscheidungsersuchen vor dem EuGH von Gerichten aus verschiedenen Mitgliedstaaten und Klagen gegen Luftfahrtunternehmen und die Fluggastdatenzentrale beim BKA werden weitere Klärung zur Vereinbarkeit der PNR-RL und auch des FlugDaG mit den Grundrechten bringen.

6.25 Agile Projektentwicklung

Große IT-Projekte im Bereich der Sicherheitsbehörden weisen immer höhere Komplexität und Dynamik auf und die Entwicklungsmethoden werden stets angepasst. Erste Projekte werden heute mit agilem Projektmanagement durchgeführt. Ziel ist es, Flexibilität, Transparenz und Sicherheit für alle Beteiligten zu erzielen. Um beim Entwicklungsprozess so früh wie möglich zu ausführbarer Software zu gelangen, wird die Entwurfsphase auf ein Mindestmaß reduziert und auf agile Projekt- und Softwareentwicklung gesetzt. Diese muss kein Widerspruch zum Datenschutz sein.

Bei der Entwicklung von IT-Systemen müssen datenschutzrechtliche Leitplanken beachtet werden. Die Ziele und Meilensteine müssen so genau festgelegt und dokumentiert sein, dass eine fundierte datenschutzrechtliche Beratung und Kontrolle möglich ist. Andernfalls besteht bei Sicherheitsbehörden die Gefahr, dass aufgrund von Beanstandungen nach § 16 BDSG oder Anordnungen nach § 69 Abs. 2 BKAG Teile des IT-Systems in einem kostenintensiven Prozess überarbeitet oder gar neu programmiert werden müssen.

Bei den Sicherheitsbehörden bewegt man sich im Bereich der grundrechtssensitiven staatlichen Eingriffsverwaltung mit entsprechenden Gesetzesvorbehalten. Datenschutzrechtliche Vorgaben müssen vor Beginn der

agilen Entwicklung vollständig festgelegt und belastbar dokumentiert werden. In Bezug darauf gibt es keinen Verhandlungsspielraum wie beispielsweise bei Zeit oder Budget. So ist bereits mit dem Projektauftrag zu klären, innerhalb welcher konkreten und detaillierten rechtlichen Vorgaben sich das Projekt bewegen kann bzw. muss. Auch technische Entwicklungsziele sind innerhalb der datenschutzrechtlichen Leitplanken zu formulieren und zu dokumentieren.

Datenschutzrechtliche Anforderungen durchziehen die gesamte Projektentwicklung, von der Zielsetzung des Projekts über die Entwicklung eines geeigneten Datenmodells und die zweckgebundene Datenverarbeitung bis hin zur Datenspeicherung, Löschung und Protokollierung. Im Entwicklungsprozess ist zu dokumentieren, auf welche Weise die Entwicklungsvorgaben eingehalten und wie die fachlichen Anforderungen innerhalb der rechtlichen Leitplanken umgesetzt werden. Dazu gehört auch der Nachweis, dass die Rückverfolgbarkeit bzw. Nachvollziehbarkeit der Software gewährleistet ist.

Zeitpunkte, an denen Berichte über den Entwicklungsfortschritt erstellt werden, müssen vorab festgelegt werden. Diese können wieder Gegenstand der datenschutzrechtlichen Beratung sein.

Am Ende sollte eine technische Beschreibung und Dokumentation des betriebsfertigen Systems stehen, die es ermöglicht, das Produkt vor seinem Einsatz vollständig auf seine datenschutzrechtliche Zulässigkeit zu prüfen.

6.26 Personalverwaltungssystem PVSplus: Noch nicht gelöste datenschutzrechtliche Herausforderungen

Die Einführung des einheitlichen Personalverwaltungssystems PVSplus in der Bundesverwaltung ist mit einigen bisher ungelösten datenschutzrechtlichen Herausforderungen verbunden. Ich werde künftig meine Beratungs- und Kontrolltätigkeiten in diesem Bereich weiter verstärken.

Seit einigen Jahren hat die Bundesverwaltung mit dem Projekt „Personalverwaltungssystem PVSplus“ ein informationstechnisches Großvorhaben in Angriff genommen. Hierbei sollen die unterschiedlichen Personalverwaltungssysteme in der Bundesverwaltung durch eine einheitliche informationstechnische Lösung großflächig konsolidiert und künftig ausschließlich in den zentralen Rechenzentren des Informationstechnikzentrums Bund (ITZBund) betrieben werden. Die eingesetzte Lösung basiert auf dem Verfahren eines großen Enterprise-Resource-Planning (ERP) Anbieters.

Bislang habe ich im Rahmen meiner aufsichtsbehördlichen Tätigkeit schwerpunktmäßig beratende Unterstützung angeboten, die insbesondere seitens des ITZBund, wo PVSplus für den zentralen Einsatz in der Bundesverwaltung weiterentwickelt wird, rege beansprucht worden ist. Positive Ergebnisse meiner Beratungen im Bereich des Beschäftigtendatenschutzes waren z. B. Anpassungen bei der Bezügemitteilung. Auch bei der Vereinbarung zur Auftragsverarbeitung hat meine Beratung Verbesserungen ermöglicht.

Dennoch sind die im Laufe der Jahre auf diese Weise erreichten datenschutzrechtlichen Ergebnisse noch keineswegs zufriedenstellend. Insbesondere verfügt die eingesetzte Softwareanwendung aktuell über keine ausreichend automatisierten Löschroutinen, um die gesetzlichen Lösch- und Aufbewahrungsvorgaben der durchaus sensiblen personenbezogenen Daten zu gewährleisten.

Neben der beratenden Begleitung des Projektes bzw. Produktes werde ich zukünftig den Fokus auch auf gezielte Kontrollen der Datenverarbeitung über PVSplus bei den Bundesbehörden legen, die PVSplus für ihre Personalverwaltung nutzen.

Für diese „Kundenbehörden“ gilt: Solange PVSplus keine verlässliche automatisierte Löschung der personenbezogenen Daten zur Verfügung stellt, ist die Wahrung der gesetzlichen Lösch- und Aufbewahrungsvorgaben durch organisatorische Maßnahmen zu gewährleisten.

7 Informationsfreiheit

7.1 Gremien

7.1.1 Konferenz der Informationsfreiheitsbeauftragten in Deutschland

Die Konferenz der Informationsfreiheitsbeauftragten aus Bund und Ländern (IFK) gab auch 2021 wichtige Anstöße zu aktuellen Themen der Transparenz staatlichen Handelns.

Die Konferenz hat das Ziel, das Recht auf Zugang zu amtlichen Informationen zu fördern und für die Weiterentwicklung der Informationsfreiheit einzutreten. Hierzu werden durch die IFK beispielsweise Entschließungen verabschiedet, die Forderungen zu informationsfreiheitsrechtlichen Themen an die Gesetzgeber und Regierungen in Bund und Ländern enthalten. Den jährlich wechselnden Vorsitz hatte im Jahr 2021 der Landesbeauftragte für die Informationsfreiheit Sachsen-Anhalt inne. Pandemiebedingt fanden die Konferenzen als Videokonferenzen statt.

Auf der 40. Konferenz wurden drei Entschließungen verabschiedet. Die IFK forderte mehr Transparenz im Verfassungsschutz, die Einführung behördlicher Informationsfreiheitsbeauftragter bei allen öffentlichen Stellen und im Rahmen eines Forderungspapiers an den neu gewählten Bundestag die Schaffung eines Transparenzgesetzes auf Bundesebene.

Auch die 41. Konferenz verfolgte das Ziel, der Informationsfreiheit noch mehr Geltung zu verschaffen. Es wurden drei Entschließungen gefasst. Die IFK forderte den Bundesgesetzgeber zur Zustimmung zur Tromsø-Konvention des Europarats auf; diese Konvention ist 2009 in Kraft getreten und beinhaltet ein allgemeines Recht auf Zugang zu amtlichen Dokumenten der öffentlichen Verwaltung und Mindeststandards bei der Bearbeitung von Informationszugangsanträgen. Zudem wurde gefordert, die Beratungs- und Kontrollkompetenzen im Umweltinformationsrecht in den Ländern auch auf die Landesbeauftragten für Informationsfreiheit zu übertragen. Die IFK forderte den Bundesgesetzgeber darüber hinaus auf, die EU-Richtlinie zum Schutz von Whistleblowern so schnell wie möglich umzusetzen und den Schutz auch auf Hinweisgeberinnen und -geber zu erstrecken, die Verstöße gegen nationales Recht melden.

Im nächsten Jahr wird Schleswig-Holstein den Vorsitz der IFK übernehmen.

7.1.2 Internationale Konferenz der Informationsfreiheitsbeauftragten

Die Internationale Konferenz der Informationsfreiheitsbeauftragten (ICIC) hat ein neues Exekutivkomitee für drei Jahre gewählt.

Zur ersten Vorsitzenden des ICIC-Exekutivkomitees wurde Comisionada Presidente Blanca Lilia Ibarra at the National Institute for Transparency, Access to Information and Personal Data Protection of Mexico gewählt. Darüber hinaus waren die Kandidaten aus Albanien, Bermuda, Brasilien, Chile, Kenia, Südafrika und den Vereinigten Staaten erfolgreich. Das neu konstituierte Exekutivkommitee hat die Geschäfte am 24. Juni 2021 übernommen.

Nachdem die zunächst für 2020 in Brasilien geplante 12. Internationalen Konferenz der Informationsfreiheitsbeauftragten pandemiebedingt verschoben worden war, wurde sie ab Mai 2021 in Form verschiedener Online-Veranstaltungen (Webinare, Workshops und Sitzungen) durchgeführt. Die diesjährige Sitzung der Beauftragten fand am 23. und 24. Juni 2021 in Form einer Videokonferenz statt. Neben den Berichten über den Stand der Informationsfreiheit in den Regionen waren eine Resolution über die strategischen Prioritäten der ICIC [23] in den nächsten Jahren sowie zur proaktiven Veröffentlichung von Informationen im Zusammenhang mit der Covid-19-Pandemie Gegenstand der Tagesordnung. Die Weiterentwicklung und Ausrichtung der ICIC wird nach dem Strategieplan eine Aufgabe für die nächsten Jahre sein.

23 Weitere Infos zum Strategieplan der ICIC: https://www.informationcommissioners.org/icic-signs-resolution-on-its-strategic-plan-for-the-next-three-years

7.2 „Glyphosat“-Urteil – Zur Veröffentlichung einer behördlich erstellten Stellungnahme nach Informationszugang

Das Urheberrecht steht der Weiterverbreitung einer behördlich erstellten Stellungnahme zum Herbizit Glyphosat nicht entgegen, wenn die Behörde diese bereits als amtliches Werk veröffentlicht hat. Auch die Weiterverbreitung im Rahmen einer Berichterstattung über Tagesereignisse war im konkreten Fall zulässig.

Der Streit um die Veröffentlichung einer durch das Bundesinstitut für Risikobewertung (BfR) erstellten Stellungnahme zu den Krebsrisiken des Herbizids Glyphosat wurde vom Oberlandesgericht Köln (OLG Köln) am 12. Mai 2021 entschieden (Az.: 6 U 146/20).

Der Verein Open Knowledge Foundation (OKF) hatte das Dokument ohne Zustimmung des BfR in einem redaktionellen Artikel auf seiner Internetseite „Frag den Staat“ veröffentlicht. Dagegen war das BfR gerichtlich vorgegangen. Das OLG Köln lehnte einen dahingehenden Unterlassungsanspruch der Behörde jedoch ab. Damit bestätigte das OLG Köln im Ergebnis die Entscheidung der Vorinstanz (vgl. 29. TB, Nr. 8.2.1).

Dass die Stellungnahme des BfR grundsätzlich Urheberrechtsschutz genießen kann, war vor dem OLG nicht mehr streitig. Nach Auffassung des Gerichts ist eine Veröffentlichung dennoch aus verschiedenen Gründen zulässig:

Als „amtliches Werk“ nach § 5 Abs. 2 Urheberrechtsgesetz (UrhG) ist die Stellungnahme vom Urheberrechtsschutz ausgenommen. Das BfR hatte über 45.000 IFG-Anträge erhalten und daraufhin selbst durch eine im Bundesanzeiger veröffentliche Allgemeinverfügung entschieden, jeder antragstellenden Person das Dokument über die Internetseite des BfR zur Verfügung zu stellen. Das OLG ging davon aus, dass die Behörde das Werk damit im amtlichen Interesse zur allgemeinen Kenntnisnahme veröffentlicht und ein amtliches Werk geschaffen hat. Einschränkende Erklärungen und Restriktionen des Zugriffs sollen daran nichts ändern. Auch ein – nach Urteil des Bundesgerichtshofs vom 20. Juli 2006 (Az.: I ZR 185/03) dafür erforderliches – spezifisches Verbreitungsinteresse bejaht das OLG vor dem Hintergrund der hohen gesellschaftspolitischen Bedeutung der Information, welche die Auswirkungen des Pflanzenschutzmittels auf Umwelt und Gesundheit betrifft. Ob bereits die erste Gewährung des Informationszugangs nach dem IFG für die Annahme eines öffentlichen Werkes nach § 5 Abs. 2 UrhG ausreicht, lässt das Gericht hingegen ausdrücklich offen.

Der Verein kann sich zudem auf § 50 UrhG berufen. Danach ist eine öffentliche Wiedergabe von Werken zur „Berichterstattung über Tagesereignisse“ in einem durch den Zweck gebotenen Umfang gestattet. Das Gericht würdigt dafür die redaktionelle Berichterstattung. Es kommt zu dem Ergebnis, dass die Stellungnahme nicht um ihrer selbst willen präsentiert wird, sondern in einem größeren Kontext redaktionell eingebettet in eine kritische Berichterstattung über die Behörde erscheint. Als Gegenstand der Berichterstattung sieht das Gericht nicht die Stellungnahme als solche oder die Nichtherausgabe des Dokuments an, sondern letztlich die Rolle des BfR im Zusammenhang mit der (Neu-) Zulassung des Pflanzenschutzmittels Glyphosat. Dem beklagten Verein gehe es sowohl um den erschwerten Informationszugang mit Mitteln des Urheberrechts, was er als „Zensururheberrecht“ bezeichnet, als auch um die Gefährlichkeit des Unkrautvernichtungsmittels Glyphosat. Der Inhalt des Textes ermöglicht den Lesern der Website eine eigene Beurteilung, ob – und wenn ja – inwieweit die im Rahmen der Berichterstattung erhobenen Vorwürfe berechtigt sind.

Das Gericht sah die Veröffentlichung auch als verhältnismäßig an. Bei der zugrundeliegenden Abwägung hatte es einbezogen, dass die Berichterstattung ein das öffentliche Interesse besonders berührendes Thema zum Inhalt hat und eine wirtschaftliche Verwertung der Zusammenfassung nicht in Betracht kommt.

Die Entscheidung des OLG Köln beruht damit auf den geschilderten Umständen des konkreten Falles, bei denen die Behörde eine „amtliche Information“ selbst durch Veröffentlichung zu einem „amtlichen Werk“ im Sinne des § 5 UrhG gemacht hat und eine Berichterstattung zu Tagesereignissen unter Offenlegung des Dokuments zulässig war. Über den Einzelfall hinaus macht das Urteil des OLG Köln deutlich, dass Behörden sich zumindest nicht pauschal und schrankenlos auf das Urheberrecht berufen können, um die weitere Veröffentlichung und Verwertung amtlicher Informationen zu beschränken.

Die Revision gegen die Entscheidung wurde nicht zugelassen. Die Entscheidung ist allerdings noch nicht rechtskräftig, da Nichtzulassungsbeschwerde beim Bundesgerichtshof eingelegt wurde.

7.3 Open Government Partnership

Der 3. Nationale Aktionsplan Deutschlands als Mitglied der Open Government Partnership (OGP) wurde beschlossen. Er enthält insbesondere auf Bundesebene zahlreiche Selbstverpflichtungen für offenes Regierungs- und Verwaltungshandeln.

Die OGP ist eine internationale Initiative zur Förderung des offenen Regierungs- und Verwaltungshandelns. Die Mitgliedsstaaten verpflichten sich u. a. Transparenz, Teilhabe, Zusammenarbeit und Innovation in den jeweiligen Ländern zu fördern. Um dieser Verpflichtung nachzukommen, werden in sog. „Nationalen Aktionsplänen" (NAP) Projekte und Vorhaben als „Selbstverpflichtung" beschrieben und niedergelegt. An der Entwicklung der NAP sind neben Bund und Ländern auch zivilgesellschaftliche Akteure beteiligt. Die NAP und die Umsetzung der enthaltenen Selbstverpflichtungen werden von einer unabhängigen Stelle evaluiert.

Im Berichtsjahr wurde der Abschlussbericht über die Umsetzung des 2. NAP für die Jahre 2019 bis 2021 von der Bundesregierung beschlossen. Zudem wurde bereits der 3. NAP für die Jahre 2021 bis 2023 beschlossen, der insgesamt vierzehn Selbstverpflichtungen enthält. Neben der Selbstverpflichtung, eine Web-basierte Plattform zu errichten, die Informationen über Planungs- und Genehmigungsverfahren großer Infrastrukturvorhaben des Bundes im Verkehrssektor öffentlich zugänglich machen soll, ist beispielsweise auch die Intensivierung der Aktivitäten des Kompetenzzentrums Open Data (CCOD) im Bundesverwaltungsamt als eigener Punkt enthalten. Das CCOD unterstützt und berät die Bundesbehörden bei der Bereitstellung von offenen Daten. Der NAP sieht die langfristige Etablierung von Fachkonferenzen und den verstärkten Wissensaustausch zwischen den Behörden, der Wissenschaft, der Wirtschaft, den Ländern und der Zivilgesellschaft, vor. In der Verantwortung des Bundesministeriums der Justiz und für Verbraucherschutz wird ein Konzept für ein Rechtsinformationsportal des Bundes erarbeitet, auf dem digitale Rechtsinformationen zur Verfügung gestellt werden sollen.

Drei Projekte des NAP werden von Bundesländern in eigener Verantwortung betreut. Hamburg hat sich zur Entwicklung von Softwareprodukten für die Bearbeitung von digitalen Beteiligungsverfahren im Bereich der räumlichen Planung und Planfeststellung verpflichtet. Nordrhein-Westfalen will Rahmenbedingungen für die Bereitstellung von offenen Daten von Unternehmen der Daseinsvorsorge und von Wahldaten schaffen und – als drittes Länderprojekt – zusammen mit Sachsen ein landesweites Beteiligungsportal entwickeln. Zwei Vorhaben entstehen in Kooperation des Bundes mit einzelnen Bundesländern. Das Bundesministerium des Innern, für Bau und Heimat (BMI) und die Länder Baden-Württemberg und Nordrhein-Westfalen entwickeln eine Plattform, auf der Open-Source-Projekte verzeichnet und zur öffentlichen Bearbeitung und Weiterentwicklung bereitgestellt werden können. Zusammen mit der Hansestadt Bremen beabsichtigt das BMI ferner, einen zentralen nationalen Bekanntmachungsservice für öffentliche Auftragsvergaben einzurichten.

Ich unterstütze die Leitgedanken und die Ziele der OGP ausdrücklich. Auch künftig sollten neben der Weiterentwicklung der Digitalisierung besonders die Aspekte Transparenz und Open-Data gefördert werden.

7.4 Formatwahlrecht: Ja oder Nein?

Ein Recht auf die Wahl des Formats der Bereitstellung amtlicher Informationen besteht dann nicht mehr, wenn die Informationen bereits in einem anderen Format (vollständig) zugänglich sind.

Ein Petent bat mich um Vermittlung, weil er sein Recht auf Informationszugang durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) als verletzt ansah.

Gegenstand des Informationszugangsantrages war die Herausgabe des IT-Grundschutz-Kompendiums 2021 in einem maschinenlesbaren Format. Im Rahmen des Vermittlungsverfahrens präzisierte der Petent den Antragsgegenstand dahingehend, dass er die Bereitstellung des Dokuments in einer XML-Version wünschte. Das BSI lehnte den Informationszugang unter Verweis auf § 9 Abs. 3 IFG ab, da auf der Internetseite des BSI eine PDF-Version des Grundschutzkompendiums zur Verfügung stehe. Der Petent bat mich um Prüfung, ob ihm nicht doch eine XML-Version zur Verfügung zu stellen sei.

Die Frage, ob man als Antragsteller in einem IFG-Verfahren ein Recht auf Bestimmung des (Datei-)Formats hat in dem die begehrten Informationen zur Verfügung gestellt werden, ist immer wieder Gegenstand von Eingaben. Das Recht zur Bestimmung der „Art des Informationszugangs" nach § 1 Abs. 2 Satz 2 IFG umfasst grundsätzlich auch das Wahlrecht hinsichtlich des Dateiformates (vgl. 2. TB zur Informationsfreiheit, Nr. 4.14.3), wonach dem Petenten die beantragte XML-Version herauszugeben gewesen wäre.

Im vorliegenden Fall war die Ablehnung des Antrags durch das BSI aber dennoch nicht zu beanstanden, da die Informationen in der XML-Version nicht über die der PDF-Version hinausgingen. Soweit meinem Haus eine

Prüfung möglich war, bestanden Unterschiede lediglich hinsichtlich der in der XML-Version zusätzlich enthaltenen Metadaten.

Ein Formatwahlrecht bestand daher nicht (mehr), soweit die begehrten Informationen bereits in einem anderen Format in zumutbarer Weise aus allgemein zugänglichen Quellen beschafft werden konnten. Anders dürfte indes zu entscheiden sein, wenn die Dateiformate inhaltliche Unterschiede aufweisen würden.

Ungeachtet dessen würde ich es begrüßen, wenn die Bereitstellung von amtlichen Informationen – auch unter Open-Data Gesichtspunkten – in unterschiedlichen Formaten erfolgen würde.

7.5 Transparenz im Gesetzgebungsverfahren

Die Erhöhung der Transparenz in Gesetzgebungsverfahren ist weiterhin erklärtes Ziel der Bundesregierung.

Im November 2018 wurde die Vereinbarung zur Erhöhung der Transparenz in Gesetzgebungsverfahren durch die Bundesregierung beschlossen. Das Bundeskanzleramt hat im Herbst 2020 alle Ressorts zum Umsetzungsstand befragt. Das Ergebnis dieser Umfrage im Ressortkreis zeigt vielversprechende Ansätze. Viele Ressorts arbeiten schon jetzt früh und aktiv mit den zu beteiligenden Akteuren zusammen. Die Einleitung der Länder- und Verbändebeteiligung bei Referentenentwürfen wird immer öfter (auch) online bekannt gegeben. Die Erfahrungen dabei sind regelmäßig positiv.

Auf ihrem Internetauftritt unter www.bundesregierung.de hat die Bundesregierung Unterseiten zu Gesetzesvorhaben und zur Beteiligung eingerichtet. Unter „Gesetzesvorhaben der Bundesregierung“ sind Links und Hinweise zu geplanten „Rechtsakten“ der Bundesministerien und der EU-Kommission eingestellt. Unter „Beteiligung auf Bundesebene“ können laufende und abgeschlossene Beteiligungen auf Bundesebene eingestellt werden, so dass die Öffentlichkeit oder Fachöffentlichkeit anlassbezogen die Möglichkeit hat, ihre Ideen, Meinungen oder Reaktionen einzubringen. Die einzelnen Gesetzgebungs- und Beteiligungsverfahren seien auf diese Weise schnell und einfach auffindbar. Gesetzgebungsprozesse würden transparent und die Beteiligung der Zivilgesellschaft gestärkt.

Ich begrüße diese Bemühungen zur Stärkung der Transparenz im Gesetzgebungsverfahren und ermuntere ausdrücklich zu weiteren Schritten. Leider leidet das Gesetzgebungsverfahren gegenüber den Beteiligten außerhalb des Ressortskreises, also auch dem BfDI und insbesondere NGOs gegenüber – wie bereits erwähnt – unter völlig unnötigen kurzen Fristsetzungen, die die Transparenz konterkarieren, weil nur noch theoretische eine Beteiligung möglich ist. Hier muss es eine Rückkehr zu den vorgesehen Fristen geben.

7.6 Beanstandung des BMVI wegen der Verweigerung des Informationszugangs ohne Grund

Das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) verweigerte die Herausgabe der E-Mail Kommunikation zwischen Bundesminister Scheuer und dem Leiter für Strategisches Medienmanagement ohne tragfähige rechtliche Begründung. Dieses Vorgehen habe ich förmlich beanstandet.

Ein Petent bat das BMVI um Informationszugang zum kompletten E-Mail-Verlauf zwischen dem Leiter für Strategisches Medienmanagement des BMVI und Bundesminister Scheuer hinsichtlich der Veröffentlichung eines Presseartikels zur sog. Maut-Affäre. Den Antrag lehnte das BMVI unter Verweis auf den Versagungsgrund des § 3 Nr. 1 lit. g) IFG ab. Nach Auffassung des BMVI stand dem Informationszugang das laufende Verfahren eines parlamentarischen Untersuchungsausschusses entgegen. Im Bescheid führte das BMVI aus, dass der Begriff des Verfahrens beim o. g. Ausnahmetatbestand umfassend sei. Diese Norm bezwecke, die Tätigkeiten der Institutionen der Rechtspflege zu schützen. Parlamentarische Untersuchungsverfahren fielen nach Artikel 44 GG unter die dritte Fallgruppe des § 3 Nr. 1 lit g) IFG. Der Untersuchungsausschuss habe ein klares Aufklärungsziel. Aufgabe des Ausschusses sei es laut Beschluss des Bundestages, die Vorgänge rund um die Infrastrukturabgabe für Personenkraftwagen „unter vertraglichen, rechtlichen, insbesondere verfassungsrechtlichen, haushälterischen und politischen Gesichtspunkten“ zu untersuchen. Dabei erhebe er Beweise, die für die Sachverhaltsaufklärung und Wahrheitsfindung für erforderlich erachtet werden. Gemäß § 17 Untersuchungsausschussgesetz komme der Untersuchungsausschuss auf der Grundlage seiner Beweiserhebung zu Schlussfolgerungen. Die erbetenen E-Mails seien insofern Beweismittel des laufenden Untersuchungsausschuss-Verfahrens und in Erfüllung entsprechender Beweisbeschlüsse an den Ausschuss übersandt worden.

Der E-Mail-Verlauf sei dabei nur ein kleiner Teil aller Beweismaterialien. Eine Veröffentlichung ohne Bezug zur großen Menge der weiteren Beweismaterialien – insgesamt seien dem Untersuchungsausschuss bislang rund eine Millionen Seiten Dokumente übermittelt

worden – könne zu einer „verzerrten Wahrnehmung in der Öffentlichkeit führen und dadurch die Sachverhaltsaufklärung und Wahrheitsfindung der Ermittelnden nachteilig beeinträchtigen bzw. beeinflussen".

Nach meiner Auffassung lag ein Versagungsgrund für den Informationszugang entgegen der Ansicht des BMVI nicht vor. Insbesondere war ein Versagungsgrund nach § 3 Nr. 1 lit. g) IFG nicht gegeben. Dieser Ausschlusstatbestand erlaubt die Verweigerung des Informationszuganges, wenn das Bekanntwerden der Information nachteilige Auswirkungen auf die Durchführung eines laufenden Gerichtsverfahrens, den Anspruch einer Person auf ein faires Verfahren oder die Durchführung strafrechtlicher, ordnungswidrigkeitsrechtlicher oder disziplinarischer Ermittlungen haben kann.

Entgegen der Auffassung des BMVI fallen Parlamentarische Untersuchungsverfahren nach Art. 44 GG grundsätzlich nicht unter § 3 Nr. 1 lit. g) IFG.

Während im Strafverfahren die Verwirklichung eines bestimmten, fest umrissenen Tatbestandes im Hinblick auf die individuelle Schuld einer Person durch das Gericht geprüft wird, geht es in dem Verfahren eines Untersuchungsausschusses um die Aufklärung eines Sachverhalts zu politischen Zwecken in Wahrnehmung der Kontrollfunktion des Parlaments. Als Instrument und essentielles Organ parlamentarischer Kontrolle übt ein Untersuchungsausschuss keine rechtsprechende Gewalt aus, auch wenn das Verfahrensrecht des Ausschusses Befugnisse des Strafverfahrensrechts entlehnt. Ein Parlamentarischer Untersuchungsausschuss führt ferner keine strafrechtlichen, ordnungswidrigkeitsrechtlichen oder disziplinarischen Ermittlungen und unterfällt auch daher nicht der dritten Fallgruppe des § 3 Nr. 1 lit. g) IFG.

Der Hinweis des BMVI, dass einem Ausschuss, ähnlich einem Strafgericht, ein Auftrag zur retrospektiven sachlichen wie wahrheitsgemäßen Aufklärung eines Sachverhalts mit Mitteln des Strafprozesses obliege, kann darüber nicht hinweghelfen. Auch bei diesem Argumentationsversuch wird verkannt, dass der Untersuchungsausschuss weder von seiner verfassungsrechtlichen Organisation noch seiner verfassungsrechtlichen Aufgabenstellung und Kontrollfunktion ein strafverfahrensrechtliches Organ darstellt.

Eine Rechtfertigung der Versagung des Informationszuganges war damit im Ergebnis nicht ersichtlich, so dass ich die Versagung des Informationszugangs beanstandet habe.

Das BMVI wies meine Beanstandung mit Nachdruck zurück, weil nach dortiger Ansicht die Voraussetzung für eine Beanstandung – nämlich ein objektiver Rechtsverstoß gegen das IFG – nicht vorgelegen habe. Die wiederholt vorgetragene und wenig überzeugende Argumentation des BMVI teile ich weiterhin nicht.

7.7 IFG – „Konkurrenz" für den Buchhandel?

Die Ablehnung eines IFG-Antrags, der auf elektronische Übermittlung eines frei im Handel erhältlichen Buches gerichtet war, war zulässig.

Der Petent wandte sich mit seinem Antrag auf Informationszugang an die Deutsche Nationalbibliothek. Er beantragte elektronischen Zugang zu einem Buch, das zu diesem Zeitpunkt sowohl direkt über den Verlag als auch frei im Handel zu erwerben war. Zudem bestand die Möglichkeit, es in den Lesesälen der Deutschen Nationalbibliothek einzusehen.

Die Deutsche Nationalbibliothek lehnte den IFG-Antrag ab und berief sich dafür auf § 9 Abs. 3 IFG. Nach dieser Regelung kann der Informationszugang abgelehnt werden, wenn die begehrte Information in zumutbarer Weise aus allgemein zugänglichen Quellen beschafft werden kann. Vor dem Hintergrund der verschiedenen Möglichkeiten, das Buch zu kaufen oder sich von seinem Inhalt Kenntnis zu verschaffen, konnte ich die Argumentation der Deutschen Nationalbibliothek nachvollziehen.

Nach § 4 Abs. 2 des Gesetzes über die Deutsche Nationalbibliothek (DNBG) stehen die Bestände der Bibliothek der Allgemeinheit gemäß einer Benutzungsordnung zur Verfügung. Die Benutzung der Bestände sowie die Inanspruchnahme von Dienstleistungen der Bibliothek sind nach § 4 Abs. 2 S. 1 DNBG allerdings grundsätzlich kostenpflichtig. Ob es sich hierbei um eine spezielle und deshalb gegenüber dem IFG vorrangige „Regelung in anderen Rechtsvorschriften über den Zugang zu amtlichen Informationen" im Sinne des § 1 Abs. 3 IFG handelt, konnte in diesem Fall offen bleiben. Denn im Ergebnis würde auch dies dazu führen, dass ein Informationszugangsanspruch nach dem IFG verneint werden müsste. Auch der Umstand, dass es sich offenbar um ein urheberrechtlich geschütztes – allerdings bereits veröffentlichtes – Werk handelte, brauchte nicht näher betrachtet zu werden, da die Ablehnung bereits auf Grundlage von § 9 Abs. 3 IFG nicht zu beanstanden war.

Der Fall zeigt exemplarisch: Der Buchhandel braucht eine „Konkurrenz" durch das IFG nicht zu befürchten, sofern es um nicht vergriffene Werke geht.

7.8 Stiftungsrat Bauakademie

Die Argumente für die Ablehnung eines Antrags auf Zugang zu Dokumenten zur Gründung der Bundesstiftung Bauakademie waren nicht überzeugend.

Dokumente zum Gründungsprozess der Bundesstiftung Bauakademie waren Gegenstand eines Vermittlungsverfahrens. Ein Petent begehrte von dem Bundesministerium des Innern, für Bau und Heimat (BMI) u. a. Zugang zu Dokumenten zur Erstellung der Satzung der Bundesstiftung Bauakademie. Ferner begehrte der Petent auch Zugang zu dem Gutachten einer Wirtschaftsprüfungsgesellschaft hinsichtlich der rechtlichen Konzeption der Stiftung und zu Dokumenten zur Organisation und zu den Aufgaben der Geschäftsstelle der Stiftungsratsvorsitzenden.

Das BMI lehnte den Antrag zunächst u. a. unter Hinweis auf § 3 Nr. 1 lit. g IFG ab, da ein arbeitsrechtliches Verfahren in Zusammenhang mit dem Besetzungsverfahren des Direktorenpostens zwar erstinstanzlich abgeschlossen war, jedoch noch Berufung in der Sache eingelegt werden konnte. Nach meinem Hinweis im Vermittlungsverfahren wurde dieser Ausschlussgrund nicht mehr angeführt, da § 3 Nr. 1 lit. g IFG zutreffend nur dem Schutz eines laufenden Gerichtsverfahrens und nicht eines (nur möglichen) Rechtsmittels dient.

Die Ablehnung des Informationszugangs wurde jedoch auch auf § 4 Abs. 1 IFG gestützt. Schutzgegenstand des § 4 Abs. 1 IFG ist der behördliche Entscheidungsprozess. Das BMI begründete die Ablehnung mit dem zu diesem Zeitpunkt noch nicht abgeschlossenem Entscheidungsprozess in dem (neuen) Stellenbesetzungsverfahren für den Gründungsdirektor oder die Gründungsdirektorin der Stiftung, da sämtliche Dokumente Einfluss auf das Stellenbesetzungsverfahren haben könnten. Eine Bekanntgabe der Informationen würde eine objektive Personalauswahl erschweren bzw. vereiteln.

In dem pauschalen Umfang, der alle antragsgegenständlichen Informationen umfasste, waren die Gründe für die vollständige Ablehnung des Informationszugangs für mich nicht nachvollziehbar. Insbesondere richtete sich der IFG-Antrag des Petenten auf Informationen zur Erstellung des Satzungsentwurfes und der rechtlichen Konzeption der Stiftung. Es überzeugte mich nicht, dass solche Erörterungen rechtlicher Fragen das Ergebnis des Personalauswahlverfahrens gefährden könnten.

Hinsichtlich des Gutachtens der Wirtschaftsprüfungsgesellschaft lehnte das BMI den Zugang ebenfalls unter Verweis auf den Ausschlussgrund des § 4 Abs. 1 IFG ab. Da es sich bei dem Gutachten um keine vom Entscheidungsprozess unabhängige Vorarbeit handle, liege kein Fall des § 4 Abs. 1 S. 2 IFG vor. Die Begründung ist in meinen Augen nicht stichhaltig. Gutachten fließen regelmäßig in den Entscheidungsprozess ein und sind diesem vorgelagert. Sofern ausnahmsweise eine so enge Verknüpfung des Gutachtens mit dem Entscheidungsprozess gegeben ist, bedarf dies einer eingehenden Begründung, die das BMI hier nicht nachvollziehbar geben konnte. Es wurde nicht hinreichend dargetan, dass eine so enge Verknüpfung mit der Entscheidungsvorbereitung gegeben wäre, welche die Anwendung des § 4 Abs. 1 S. 2 IFG ausschließen könnte. Es war somit nicht ersichtlich, dass das Gutachten Teil des behördlichen Entscheidungsprozesses geworden war und unmittelbar der Entscheidungsvorbereitung diente. Dies hätte insbesondere gegolten soweit Gegenstand des Gutachtens, wie von dem Petenten vorgetragen, (größtenteils) Einschätzungen zu der praktischen rechtlichen Ausgestaltung des bereits abgeschlossenen Verfahrens der Errichtung der Stiftung Bauakademie gewesen wären.

Der Antrag des Petenten wurde auch im Widerspruchsverfahren abgelehnt. In der Sache ist nunmehr eine Klage aus (auch) presserechtlichem Anspruch anhängig. Jedenfalls das antragsgegenständliche Gutachten wurde dem Petenten nach Abschluss des nochmaligen Bewerbungsverfahrens und der Auswahl eines Gründungsdirektors zugänglich gemacht.

7.9 Umweltinformationsgesetz

7.9.1 Ombudsfunktion im Umweltinformationsrecht

Meine Behörde kann die Kontroll- und Ombudsfunktion nun auch beim Zugang zu Umweltinformationen ausüben.

Im März 2021 wurde mir die Zuständigkeit für die Beratung und die Kontrolle rund um das Umweltinformationsgesetz (UIG) des Bundes übertragen. Insbesondere wurde meine bisher lediglich für das IFG bestehende Ombudsfunktion auf den wichtigen Bereich des Umweltinformationsrechts ausgedehnt. Nun kann jede Person den Bundesbeauftragten für die Informationsfreiheit anrufen, wenn sie ihr Recht auf Informationszugang nach dem Informationsfreiheitsgesetz oder dem Umweltinformationsgesetz des Bundes als verletzt ansieht. Flankiert wird dies durch eine erweiterte Kontrollzuständigkeiten für mein Haus. Die neue Zuständigkeit ergibt sich aus einer Novelle des UIG, die am 4. März 2021 in Kraft getreten ist.

Mit der Beratungs- und Kontrollzuständigkeit für den Zugang zu Umweltinformationen bei den öffentlichen Stellen des Bundes wird meine langjährige Forderung erfüllt. Die Bedeutung des Umweltinformationsgesetzes als Anspruchsgrundlage für den Informationszugang ist

nicht nur vor dem Hintergrund des in den vergangenen Jahren vermehrt spürbar werdenden Klimawandels gewachsen. Bislang blieb den Antragstellenden bei einer Weigerung der angefragten Behörde, die Information zugänglich zu machen, nur der zeit- und kostenaufwändige Rechtsweg vor die Verwaltungsgerichte.

7.9.2 UIG oder IFG? Eine manchmal nicht einfache Abgrenzungsfrage

Eine informationspflichtige Behörde muss einen auf der Grundlage des IFG gestellten Antrag auch unter dem Aspekt des UIG betrachten und umdeuten, wenn Umweltinformationen Gegenstand des Antrags sind.

Ein Petent bat mich um Vermittlung bei einem Antrag nach dem Informationsfreiheitsgesetz (IFG) an die Physikalisch-Technische Bundesanstalt (PTB). Auf dem Gelände der PTB in Braunschweig war es zu einem Austritt des radioaktiven Stoffes Krypton-85 gekommen. Der Vorfall stellte ein bedeutsames Vorkommnis im Sinne der Strahlenschutzverordnung (StrlSchV) dar. Um die Ursache des Vorfalls zu ermitteln, wurde eine externe Sachverständigenorganisation beauftragt. Der Antrag des Petenten richtete sich auf Herausgabe des erstellten Berichts. Die PTB lehnte den Informationszugang ab. Sie sei gemäß § 109 Abs. 3 StrlSchV verpflichtet, die Ergebnisse der Untersuchung des Vorkommnisses vor dem Zugriff Unbefugter zu schützen. § 109 Abs. 3 StrlSchV stelle eine durch Rechtsvorschrift geregelte Geheimhaltungsvorschrift i.S.d. § 3 Nr. 4 IFG dar. Damit bestehe kein Anspruch auf Informationszugang zu dem Bericht.

Hier sehe ich noch Klärungsbedarf. Der Begriff des Unbefugten ist im Strahlenschutzrecht nicht definiert. Der Begriff findet sich allerdings in verschiedenen Normen des Strahlenschutzrechts. In § 109 StrlSchV wird er in Abgrenzung zu Personen verwendet, die eine Berechtigung oder Genehmigung im Anwendungsbereich des Strahlenschutzrechts besitzen. Es könnte sich dabei also auch um eine (bloße) Regelung der internen Abläufe und Verpflichtungen des Strahlenschutzverantwortlichen handeln, organisatorisch im eigenen Verantwortungsbereich dafür Sorge zu tragen, dass Unbefugte auf die genannten Aufzeichnungen keinen Zugriff nehmen können. Die Regelung würde einen Anspruch auf Zugang zu amtlichen Informationen nach dem IFG dann nicht ausschließen. Sie würde keine Geheimhaltungspflicht statuieren, sondern lediglich den Personenkreis beschränken, dem der Zugang zu den Dokumenten gestattet ist.

Ferner begründete die PTB die Ablehnung des Antrages mit Betriebs- und Geschäftsgeheimnissen nach § 6 IFG, die in dem Sachverständigenbericht enthalten seien. Eine erfolgte Drittbeteiligung des Betroffenen habe nicht zu dessen Einwilligung geführt.

In der vorliegenden Konstellation scheint es aber naheliegend, dass das Begehren des Petenten als Antrag auf Zugang zu Umweltinformationen auszulegen ist. Die PTB hat dies bestritten und darauf abgestellt, dass der Prüfbericht sich ausschließlich mit technischen Aspekten eines defekten Bauteils beschäftigt, das den Austritt des Krypton-85 verursachte. Umweltinformationen seien in diesen rein technischen Fragestellungen nicht zu sehen. Diese Begründung stand im Widerspruch zur Argumentation hinsichtlich § 109 StrlSchV. Während dort der Bericht mit dem Vorkommnis in Verbindung gebracht und ihm eine strahlenschutzrechtliche Relevanz beigemessen wird, die in der Emission von Strahlung begründet liegt, wird der Bericht im Hinblick auf die Eigenschaft als Umweltinformation völlig getrennt vom Emissionsereignis betrachtet. Der weit gefasst Anwendungsbereich des UIG könnte hier aber dazu führen, dass der Bericht als Umweltinformation anzusehen ist.

Folgte man dieser Auffassung, würde der nach § 6 IFG bestehenden Ausschlussgrund des Vorliegens eines Geschäfts- oder Betriebsgeheimnisses bei der Anwendung des UIG nicht greifen. Gemäß § 9 Abs. 1 S. 2 UIG kann der Zugang zu Umweltinformationen über Emissionen nämlich nicht deshalb verweigert werden, weil durch die Bekanntgabe Betriebs- oder Geschäftsgeheimnisse zugänglich gemacht würden (§ 9 Abs. 1 S. 1 Nr. 3 UIG). Der Petent kann gegen den Widerspruchsbescheid der PTB noch Klage erheben. Ich werde den Fortgang des Verfahrens beobachten.

8 Kontrollen und Beratung

8.1 Pflichtkontrollen

Die Pandemie hat die Durchführung der gesetzlich vorgeschriebenen Kontrollen im Sicherheitsbereich teilweise sehr erschwert und die Bearbeitung verzögert. Aufgrund der vielfach hohen Geheimhaltungsgrade der kontrollierten Inhalte war eine Kontrolle im schriftlichen Verfahren oder auch als Remote-Veranstaltung oft nicht möglich. Trotzdem konnte ich meiner Kontrollfunktion nachkommen.

8.1.1 Kontrollen und Beanstandungen bei Anti-Terror-Datei (ATD) und Rechtsextremismus-Datei (RED)

Kontrolle im Bundesnachrichtendienst

Die Nutzung der ATD im Bundesnachrichtendienst (BND) war Gegenstand meiner Kontrolle im Berichtsjahr 2018 (s. 27. TB, Nr. 9.3.11), die im Jahr 2021 abgeschlossen werden konnte. Im Ergebnis wurden mehrere Beanstandungen ausgesprochen, die ich aufgrund des Geheimhaltungsgrades des Kontrollgegenstands hier nicht alle ausführen kann. Ein Teil der Beanstandungen bezog sich dabei auf die Art und Weise der automatisierten Einspeicherung, die nach meiner Bewertung meine Kontrolle der Datenhistorie erheblich erschwert, wenn nicht gar in Einzelfällen unmöglich macht. Diese Kritik spielt auch bei anderen Beanstandungen (z. B. bei den Kontrollen im Bundesamt für Verfassungsschutz) eine wesentliche Rolle. In der Vergangenheit hatte ich nur deswegen von Beanstandungen in diesem Zusammenhang abgesehen, weil durch das Bundesministerium des Innern, für Bau und Heimat (BMI) Abhilfe durch Neugestaltung der Datei in Aussicht gestellt wurde. Dies ist bis heute nicht geschehen.

Zum Jahresende 2020 habe ich die regelmäßige Pflichtkontrolle der ATD im BND begonnen. Dies geschah unter den pandemiebedingten Beschränkungen mit dem Versuch, die Einsichtnahme in Datensätze des BND und deren Speicherungsbegründung ausschließlich in einem schriftlichen Verfahren durchzuführen. Die vergleichsweise hohen Verschlusssacheneinstufungen des Kontrollgegenstands sowie die sehr vertraulich zu behandelnde speicherungsbegründende Dokumentation erschweren diese Kontrolle im Vergleich zu einer Kontrolle in Präsenz beim BND erheblich. Dies führt zu großen Verzögerungen im Ablauf. Ich beabsichtige meine im Jahr 2022 wieder anstehende Kontrolle der ATD beim BND, sofern es die Pandemiesituation zulässt, wieder vor Ort wahrzunehmen

Kontrolle im Bundesamt für Verfassungsschutz

Sowohl die Antiterrordatei (ATD) als auch die Rechtsextremismusdatei (RED) wurden von mir bereits im Jahr 2019 im Bundesamt für Verfassungsschutz (BfV) kontrolliert und 2021 mit jeweils einem Kontrollbericht von mir bewertet. Inhaltlich gab es in beiden Kontrollen mehrere Beanstandungen, die durch das Bundesministerium des Innern (BMI) in einer ersten Antwort zu den Kontrollberichten bis auf eine nicht akzeptiert werden. Das BMI vertritt dabei unterschiedliche Auffassungen sowohl in den festgestellten Sachverhalten als auch in der rechtlichen Bewertung. Dieser Meinung kann ich mich nur in im Fall einer konkreten Beanstandung anschließen, bei der im Kontrolltermin vor Ort ein falscher Eindruck entstanden war. Von den insgesamt ursprünglich fünf Beanstandungen bei der ATD und den drei bei der RED wird daher jeweils eine Beanstandung von mir nicht mehr aufrecht gehalten. Diese Kontrollen sind damit abgeschlossen. Allerdings habe ich zum Ende des Jahres 2021 bereits die nächste Pflichtkontrolle der ATD und der RED im BfV aufgenommen. Ich konnte natürlich nicht davon ausgehen, dass alle Differenzen in der Bewertung der Kontrollsituation aus dem Jahr 2019 ausgeräumt werden konnten oder genug Zeit blieb, kritisierte Zustände vollumfänglich zu verbessern. Aus meiner Sicht bleibt bei beiden Dateien die von mir wiederholt auch schon vor der Kontrolle 2019 öffentlich vorgebrachte Kritik bestehen, die letztlich die Forderung nach einer grundlegenden Umgestaltung bzw. Abschaffung zur Konsequenz hat.

Kontrolle im Bundesamt für den Militärischen Abschirmdienst

Beim Bundesamt für den Militärischen Abschirmdienst (BAMAD) stand im Berichtsjahr 2021 die regelmäßige Kontrolle der Nutzung der RED an. Diese ausschließlich im schriftlichen Verfahren ausgeübte Kontrolle konnte noch im selben Jahr ohne Beanstandung beendet werden.

Kontrolle im Bundeskriminalamt

Im November 2020 habe ich die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in der RED durch das Bundeskriminalamt (BKA) kontrolliert. Aus technischen Gründen befand sich in der RED zum Zeitpunkt der Kontrolle ein Doppelbestand an Einspeicherungen. Das BKA teilte im Nachgang zur Kontrolle mit, dass dieser Doppelbestand inzwischen bereinigt werden konnte. Von einer Beanstandung habe ich deshalb abgesehen (vgl. § 16 Abs. 2 Satz 2 BDSG). Auch im Übrigen ergab die Anfang 2021 abgeschlossene Bewertung keinen Grund für eine Beanstandung. Die Kontrolle der Speicherungen in der ATD und deren Nutzung durch das BKA konnte bis zum Redaktionsschluss nicht abgeschlossen werden.

Kontrolle im Zollkriminalamt

Die Pflichtkontrolle der ATD beim Zollkriminalamt (ZKA) habe ich im Juli 2021 durchgeführt. Prüfgegenstand waren die vom ZKA veranlassten Speicherungen personenbezogener Daten. Erfreulicherweise konnte ich feststellen, dass das ZKA meine Empfehlungen aus den letzten beiden Kontrollbesuchen aufgegriffen hat. Die Speichervoraussetzungen waren in allen geprüften Fällen nachvollziehbar dokumentiert. Daher bot auch die diesjährige Kontrolle erneut keinen Anlass für eine Beanstandung.

Kontrolle in der Bundespolizei

Die Ende 2019 begonnene Kontrolle der RED bei einer ausgewählten Direktion im Bereich der Bundespolizei (BPol) konnte 2021 abgeschlossen werden. Notwendige Nachforderungen von Unterlagen begründeten den längeren Prüfzeitraum. Wegen des Verschlussgrades der Datei kann über Einzelheiten nicht berichtet werden. Es wurden eine Beanstandung sowie mehrere Empfehlungen zur Behebung von Dokumentationsdefiziten ausgesprochen. Wie schon in vergangenen Prüfungen hat sich erneut gezeigt, dass aufgrund meiner Kontrollankündigung eine gründliche Prüfung der Datei bei der verantwortlichen Stelle stattgefunden hat. Dabei wurde ein nicht unerheblicher Prozentsatz an löschreifen Datensätzen identifiziert.

Die Ende 2019 begonnene ATD-Kontrolle bei der BPol konnte im Laufe des Berichtsjahres 2020 beendet werden. Es wurden Empfehlungen ausgesprochen, die auch hier vorhandene Dokumentationsdefizite abstellen sollten.

Die regelmäßigen Pflichtkontrollen der ATD und der RED bei der BPol für das Jahr 2021 konnten bis zum Redaktionsschluss nicht abgeschlossen werden.

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

8.1.2 Eurodac

Im Berichtsjahr 2020 habe ich – pandemiebedingt im rein schriftlichen Verfahren – eine Kontrolle im Bereich der polizeilichen Nutzung der Datenbank European Dactyloscopy (Eurodac) durch das Bundeskriminalamt (BKA) eingeleitet. Diese Kontrolle wurde im Jahr 2021 zum Abschluss gebracht.

Über frühere Pflichtkontrollen zur Datenverarbeitung im Schengener Informationssystem (SIS), im europäischen Visa-Informationssystem (VIS) sowie dem europäischen Asylsystem Eurodac habe ich bereits in meinen letzten Tätigkeitberichten informiert (vergleiche 27. TB Nr. 9.3.5 und 28. TB Nr. 6.7.1).

Informationen aus der Asyldatei Eurodac zum Zweck der Gefahrenabwehr und Strafverfolgung dürfen ausschließlich von bestimmten Strafverfolgungsbehörden abgefragt werden. Die Abfragen müssen zudem im konkreten Einzelfall zur Aufdeckung, Verhütung oder Verfolgung terroristischer und sonstiger schwerer Straftaten erforderlich sein. Hierbei gelten strenge Voraussetzungen. Danach darf eine Eurodac-Abfrage nur erfolgen, wenn vorherige Abfragen in den nationalen Fingerabdrucksystemen und im VIS nicht zu einer Identifikation der betroffenen Person geführt haben (sogenannte Abfragekaskade).

Bei einem der geprüften Vorgänge wurde gegen Art. 20 Abs. 1 Eurodac-Verordnung verstoßen, jedenfalls weil die vorzuschaltende VIS-Abfrage unterlassen wurde. Die ausdrückliche Regelung in der Eurodac-Verordnung lässt das derzeit nicht zu.

Der gewählte Ermittlungsansatz mag aus Sicht der Strafverfolgungsbehörden durchaus nachvollziehbar gewesen sein. Er entsprach aber nicht den strengen rechtlichen Vorgaben einer Eurodac-Abfrage durch den Gesetzgeber, an die ich als Aufsichtsbehörde gebunden bin. Ich habe daher eine Beanstandung nach § 16 Abs. 2 S. 1 BDSG gegenüber dem Bundeskriminalamt (BKA) ausgesprochen.

Bezüglich der unterlassenen VIS-Abfrage wurde eine Sensibilisierung des entsprechenden Fachbereiches durch das BKA zugesagt.

Da ich im Rahmen meiner Prüfung auch festgestellt habe, dass die Dokumentation der VIS-Abfragen nicht hinreichend erfolgt ist, habe ich zudem auch noch einmal meine bereits in der Vergangenheit ausgesprochene Empfehlung zu diesem Thema in Erinnerung gerufen (vgl. 28. TB Nr. 6.7.1).

8.1.3 VIS

Im Berichtsjahr 2020 habe ich – pandemiebedingt im rein schriftlichen Verfahren – eine Kontrolle im Bereich der polizeilichen Nutzung des Visa-Informationssystems (VIS) bei der Financial Intelligence Unit (FIU) eingeleitet. Diese Kontrolle wurde im Jahr 2021 zum Abschluss gebracht.

Über frühere Pflichtkontrollen zur Datenverarbeitung im europäischen VIS habe ich bereits in meinen letzten Tätigkeitberichten informiert (vergleiche 27. TB Nr. 9.3.5 und 28. TB Nr. 6.7.1).

Polizeibehörden und Nachrichtendienste dürfen Daten aus dem VIS abrufen, wenn dies in konkreten Einzelfällen erforderlich ist, um bestimmte terroristische oder andere schwere Straftaten zu verhüten, aufzudecken oder zu verfolgen.

Bis zum 31. März 2021 war die FIU innerhalb des Zollkriminalamtes eingerichtet und damit entsprechend der Notifizierung als zugangsberechtigte Stelle benannt. Allerdings war die FIU auf der nationalen Liste nicht gemäß Art. 3 Abs. 5 VIS-Beschluss in Verbindung mit § 2 Abs. 3 VISZG als ermächtigte Organisationseinheit innerhalb der zugangsberechtigten Behörde ausgewiesen.

Seit dem 1. April 2021 ist die FIU aufgrund einer zu diesem Zeitpunkt in Kraft getretenen Gesetzesänderung neben dem Zollkriminalamt eine eigene Direktion. Da sie durch diese Statusänderung nominell nicht mehr unter die trotzdem erforderliche Notifizierung fällt, habe ich zwar eine Nachnotifizierung angemahnt, jedoch auf eine weitere Beanstandung verzichtet, da im Ergebnis von einer Abrufberechtigung der FIU ausgegangen werden konnte.

Meine Kontrolle bei der FIU führte im Ergebnis zu zwei Beanstandungen.

Es wurden VIS-Recherchen durchgeführt, obwohl die sie betreffenden Personen kein Schengen-Visum benötigten. Dabei wurde nicht hinreichend geprüft und dokumentiert, weshalb davon ausgegangen wurde, dass die Vorgaben des VIS-Zugangsbeschlusses vorlagen.

Des Weiteren wurden VIS-Daten an Drittstaaten übermittelt, ohne dass die Voraussetzungen des VIS-Zugangsbeschlusses erfüllt waren. Zudem wurden nicht alle nationalen Übermittlungsvoraussetzungen geprüft, festgestellt und dokumentiert.

In seiner Reaktion hat mir das Bundesministerium für Finanzen (BMF), als Rechts- und Fachaufsicht der FIU, die künftige Beachtung der von mir beanstandeten Punkte und in diesem Zusammenhang eine Überarbeitung der entsprechenden Handlungsanweisung zugesagt. Auch die Aufnahme in die Liste der abrufberechtigten Stellen soll veranlasst werden.

8.1.4 Kontrolle der getätigten Abfragen im Zollfahndungsinformationssystem INZOLL

Polizeiliche Datenbanken ermöglichen mit wenig Aufwand einen großen Einblick in sensible personenbezogene Daten. Umso wichtiger ist es, dass Abfragen dieser Systeme nur im Rahmen der dienstlichen Notwendigkeit erfolgen. Dies habe ich unlängst beim Zollfahndungsdienst kontrolliert.

Mit Inkrafttreten des neuen Zollfahndungsdienstgesetzes (ZFdG) im April 2021 erhielt ich den Auftrag, im Rahmen meiner Tätigkeit umfangreiche Pflichtkontrollen zur Datenverarbeitung im Zollfahndungsdienst durchzuführen. Diesem Auftrag bin ich im August mit einer Kontrolle im Zollkriminalamt (ZKA) in Köln gefolgt. Gegenstand meiner Kontrolle waren die von Beschäftigten des ZKA erfolgten Zugriffe auf Daten im Informationssystem des Zollfahndungsdienstes (INZOLL). Ich konzentrierte mich auf die über eine Suchmaske erfolgten Zugriffe auf personenbezogene Daten.

Mit einer sorgfältig ausgewählten Stichprobe war es mir möglich, einen referats- und arbeitsgruppenübergreifenden Einblick in die getätigten Abfragen mit der dafür angegebenen Begründung zu erhalten und den notwendigen Zusammenhang zwischen dem jeweiligen Bearbeitungsvorgang und der Suche in der Datenbank herzustellen.

Insgesamt war ich mit dem Kontrollergebnis im ZKA zufrieden und konnte keine unberechtigten Abfragen feststellen. Lediglich zu einer Abfrage fehlte der Aktenrückhalt, weshalb ich die Prüfung dieses Vorgangs nicht abschließen konnte. Trotz des guten Kontrollergebnisses habe ich dem ZKA Empfehlungen ausgesprochen, um sowohl den Arbeitsablauf der Beschäftigten bei Abfragen als auch das INZOLL-Benutzermanagement zu verbessern. So sollten Zugänge zum System zukünftig restriktiver vergeben und ein optimaler Prozess etabliert werden, der Arbeitsabläufe bei Personalveränderun

gen im Umgang mit INZOLL-Zugängen regelt. Darüber hinaus halte ich es für unerlässlich, die Beschäftigten des Zollfahndungsdienstes mit detaillierten Handlungsanweisungen und Schulungen verstärkt in der Handhabung von Abfragen auszubilden, um Unsicherheiten im Umgang mit Begründungen für Suchanfragen, aber auch in der Dokumentation und Aktenführung zu beseitigen.

An dieser Stelle möchte ich nicht unerwähnt lassen, dass der erfolgreiche Kontrollablauf trotz der pandemiebedingten Einschränkungen auch der guten Vorbereitung und Kooperation des ZKA zu verdanken ist.

8.1.5 Schengener Informationssystem

Im Berichtsjahr 2020 habe ich eine Kontrolle im Bereich der polizeilichen Nutzung des Schengener Informationssystems (SIS) beim Zollkriminalamt (ZKA) eingeleitet. Diese Kontrolle wurde aufgrund der pandemischen Lage im rein schriftlichen Verfahren durchgeführt und 2021 zum Abschluss gebracht.

Über frühere Pflichtkontrollen zur Datenverarbeitung im SIS habe ich bereits in meinen letzten drei Tätigkeitberichten informiert (vgl. 27. TB Nr. 9.3.5, 28. TB Nr. 6.7.1, 29. TB Nr. 9.5.1) Im SIS erfassen die Polizei- und Justizbehörden der Mitgliedstaaten des Schengen-Raums Personen- und Sachfahndungen sowie Einreise- und Aufenthaltsverbote (zu weiteren Kontrollen und Informationen rund um das SIS II vgl. auch Nr. 8.2.7).

Meine Kontrolle beim ZKA hat keine wesentlichen datenschutzrechtlichen Defizite aufgezeigt, so dass von mir keine Beanstandung ausgesprochen werden musste. Jedoch beinhaltet mein Kontrollbericht zwei Empfehlungen, die u. a. Sachverhalte im Zusammenhang mit Ausschreibungsverfahren (Dokumentation und Erforderlichkeit bestimmter Maßnahmen) betreffen.

Querverweise:

8.2.7 Datenschutzaufsicht und Beratung beim Bundesamt für Verfassungsschutz (BfV)

8.2 Sonstige Kontrollen

8.2.1 Fragebogenkontrolle Datenschutzbeauftragte in Jobcentern

Ich habe eine Fragebogenkontrolle bei 22 Jobcentern zur organisatorischen Stellung der Datenschutzbeauftragten durchgeführt.

Nach Art. 37 Abs. 1 DSGVO sind Jobcenter als öffentliche Stellen dazu verpflichtet, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen. Die oder der Datenschutzbeauftragte hat eine entscheidende Position innerhalb der Behörde, um die Einhaltung datenschutzrechtlicher Vorschriften zu gewährleisten. Die Stellung und Aufgaben sind in DSGVO und Bundesdatenschutzgesetz (BDSG) geregelt.

Ziel der Überprüfung war die Organisation der Jobcenter hinsichtlich der Stellung und Aufgabenerfüllung der Datenschutzbeauftragten. Von besonderem Interesse war dabei, in welchem Umfang die Datenschutzbeauftragten zur ordnungsgemäßen Aufgabenerfüllung freigestellt sind, ob sie weisungsunabhängig handeln können, ob Interessenkonflikte bestehen und wie die Zusammenarbeit sowie Unterstützung durch die Dienststelle erfolgt. Bezüglich ihrer Aufgabenerfüllung wurde u. a. erfragt, ob die Datenschutzbeauftragten strukturierte Prüfungen der verschiedenen Tätigkeitsbereiche durchführen oder in welcher Art und Weise die Kontrolltätigkeit anderweitig durchgeführt und der Beratungsauftrag wahrgenommen wird.

Meine Kontrolle ergab, dass in vielen Fällen die Datenschutzbeauftragten nicht in ausreichendem Umfang von sonstigen Aufgaben freigestellt worden sind. So habe ich in zwanzig Fällen die Empfehlung ausgesprochen, die Freistellungsquote zu erhöhen. Ich halte bei einer Beschäftigtenanzahl von 500 eine vollständige Freistellung für geboten, da ansonsten eine ordnungsgemäße Aufgabenerfüllung nicht möglich ist.

Defizite bestanden auch im Bereich der Abwesenheitsvertretung. Nach meiner Auffassung gehört es zur ordnungsgemäßen Aufgabenerfüllung und zur Unterstützungspflicht durch die Dienststelle, eine Abwesenheitsvertretung sicherzustellen. Wie die Dienststelle jedoch die Vertretung sicherstellt, ist grundsätzlich ihrer Organisationshoheit überlassen. Ich empfehle eine feste Abwesenheitsvertretung, die zumindest über grundsätzliche datenschutzrechtliche Kenntnisse verfügt, da nur in diesem Fall die kontinuierliche Aufgabenerfüllung auch bei längerer Abwesenheit sichergestellt ist. Um eine durchgehende Vertretung sicherzustellen, wurde acht kontrollierten Jobcentern empfohlen, die Regelung

der Abwesenheitsvertretung der oder des Datenschutzbeauftragten zu ändern.

Weitere Beanstandungen gab es im Bereich der Kontrolltätigkeiten der Datenschutzbeauftragten. Diese sind verpflichtet, die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen. Nur durch eine umfassende strukturierte Kontrolltätigkeit, die jeden Geschäftsbereich des Jobcenters in regelmäßigen Abständen umfasst, ist die Einhaltung eines hohen Datenschutzniveaus möglich. In acht Fällen habe ich die Empfehlung ausgesprochen, einen Jahreskontrollplan und entsprechende Kontrollberichte zu erstellen. So soll sichergestellt werden, dass auch tatsächlich regelmäßige Kontrollen jobcenterintern vorgenommen werden und die Ergebnisse der Kontrolle dem Verantwortlichen zugänglich sind. So können Beanstandungen zeitnah durch den Verantwortlichen abgestellt werden.

Im Nachgang zur schriftlichen Kontrolle sind mir mehrere Fälle bekannt geworden, in denen es zu Differenzen über die Stellung und Aufgabenwahrnehmung zwischen Geschäftsführungen von Jobcentern und Datenschutzbeauftragten gekommen ist. Auch aus diesem Grund werde ich diese Punkte weiterhin kontrollieren.

8.2.2 Vorgangsbearbeitungssystem des Bundeskriminalamts

In seinem Vorgangsbearbeitungssystem (VBS) verarbeitet das Bundeskriminalamt (BKA) tagtäglich sehr viele personenbezogene Daten. Dieses Informationssystem entspricht nach wie vor nicht den datenschutzrechtlichen Vorgaben. Die Beseitigung der von mir festgestellten Datenschutzprobleme gestaltet sich zäh.

Im Berichtsjahr 2019 habe ich das VBS des BKA aufgrund mehrerer schwerwiegender Datenschutzverstöße beanstandet (vgl. 28. TB Nr. 6.7.3). Die langwierige Beseitigung der von mir festgestellten Datenschutzverstöße habe ich in meinem letzten Tätigkeitsbericht kritisiert (vgl. 29. TB Nr. 9.5.3). Mehrfach habe ich das Bundesministerium des Innern, für Bau und Heimat (BMI) darum gebeten, mir einen Zeit- und Maßnahmenplan zukommen zu lassen, wie und wann das BKA die von mir festgestellten Datenschutzverstöße beseitigen wird. Meinem Anliegen ist bislang nicht entsprochen worden. Das BMI verweist darauf, dass es sich bei der angekündigten Neuausrichtung der Dokumentation und Aktenführung im BKA aufgrund der Überschneidungen und Kompatibilitätsanforderungen mit der elektronischen Akte nach E-Government-Gesetz (EGovG) und der elektronischen Akte in Strafsachen um ein sehr komplexes Vorhaben handle. Das künftige System der Dokumentation und Aktenführung müsse die rechtlichen Vorgaben erfüllen sowie den unterschiedlichen fachlichen Anforderungen im BKA gerecht werden. Bis zur Umsetzung der erforderlichen Maßnahmen würden im Bereich der Dokumentation und Aktenführung die dienstkundlichen Fähigkeiten im BKA weiter gestärkt und Verfahrensabläufe, etwa in Bezug auf die Aussonderungsprüfung, weiter optimiert. Ein Konzept zur Weiterentwicklung des VBS sei in Erarbeitung.

Ich erkenne durchaus die Komplexität des Vorhabens. Vor diesem Hintergrund habe ich dem BKA angeboten, bei der Aufbereitung der datenschutzrechtlichen Problemlagen im Zusammenhang mit dem VBS in Form eines gemeinsamen Workshops zu beraten. Angesichts der erheblichen Datenschutzprobleme erwarte ich allerdings, dass die Neuausrichtung des VBS beim BKA Priorität hat. Den ersten gemeinsamen Workshop, der Anfang Dezember 2021 stattfand, habe ich als konstruktiv und zielführend empfunden.

8.2.3 Erste Anordnung gegenüber dem BKA

Im Fall einer überlangen Speicherung habe ich das erste Mal von meiner Anordnungskompetenz nach § 69 Abs. 2 Bundeskriminalamtgesetz (BKAG) Gebrauch gemacht. Das BKA klagt dagegen.

Bereits vor mehreren Jahren hatte der Petent sich an mich gewandt, da eine Sicherheitsüberprüfung bei ihm nicht erfolgreich verlaufen war. Das Bundeskriminalamt (BKA) erteilte ihm keine Auskunft. Meine Überprüfung hatte ergeben, dass er polizeilich seit mehreren Jahrzehnten und beim BKA seit 1998 als sogenannte Kontakt- und Begleitperson in einer Datei gespeichert ist. Rechtsgrundlage für die Speicherung ist § 483 Abs. 1 Satz 1 der Strafprozessordnung (StPO). Demnach darf die Strafverfolgungsbehörde personenbezogene Daten in einer Strafverfahrensdatei führen, „soweit dies für Zwecke des Strafverfahrens erforderlich ist“. Leider hat der Gesetzgeber diese Formulierung sehr weit gefasst. Das Bundesverfassungsgericht hat diesbezüglich entschieden, dass die Speicherung von Daten zu Dritten in Strafverfahren eine spezifische individuelle Nähe der betroffenen Person zu der aufzuklärenden Gefahr oder Straftat voraussetzt (vgl. BVerfG, Urteil vom 20. April 2016, BVerfGE 141, 220 (274 f. Rn. 116)). Sehr ähnlich ist dies seit 2018 im BKAG (§19 Abs. 1 Nr. 3) formuliert. Auch in Dateien nach der StPO ist daher aus Gründen der Verhältnismäßigkeit in verfassungskonformer Auslegung auf solche eingrenzenden Merkmale zu achten, vor allem über einen derart langen Zeitraum. Eine solche Nähe oder ein vergleichbarer Gesichtspunkt konnten vom BKA über einen langen Zeitraum nicht mehr dokumentiert werden, sodass die Speicherung der betroffenen Kontakt- und Begleitperson meines Erachtens unverhältnismäßig ist.

Die Auskunftsanfrage des Petenten beim BKA wurde mit Hinweis auf die Auskunftsverweigerungsgründe gem. § 57 Abs. 4 i.V.m. § 56 Abs. 2 BDSG abgewiesen. Bei meiner Prüfung kam ich jedoch zu dem Schluss, dass dem Petenten ein Auskunftsrecht zusteht. Das BKA hatte mir keine tragfähigen Gründe benannt, nach denen die Aufgabenerfüllung und die öffentliche Sicherheit durch die Erteilung der Auskunft gefährdet wären.

Vor diesem Hintergrund habe ich die Speicherung des Petenten als Kontakt- und Begleitperson sowie die unterlassene Beauskunftung gemäß § 16 Abs. 2 BDSG beanstandet. Schon zuvor hatte der Petent selbst gegen das BKA Klage auf Auskunft und Löschung seiner Daten erhoben. Meine Beanstandung wurde vom Bundesministerium des Innern, für Bau und Heimat (BMI) als Aufsichtsbehörde des BKA zurückgewiesen. Daher habe ich nunmehr gegenüber dem BKA gemäß § 69 Abs. 2 BKAG angeordnet, den Datensatz des Petenten zu sperren, ihm eine Auskunft zu erteilen und nach Abschluss seines Klageverfahrens die Daten zu löschen. Das BMI bestreitet meine Kompetenz, eine Löschung anzuordnen und beruft sich insofern auf die Gesetzesbegründung zum BKAG. Meiner Ansicht nach ist das BKAG an dieser Stelle jedoch europarechtskonform auszulegen. Die JI-Richtlinie sieht in Art. 47 Abs. 2 Buchstabe b) eine entsprechende Kompetenz für die nationalen Aufsichtsbehörden explizit vor („insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten"). Das BKA hat gegen meine Anordnung Klage erhoben. Eine Entscheidung liegt noch nicht vor.

8.2.4 Funkzellendatenbank des Bundeskriminalamts

Nach ständiger Rechtsprechung des Bundesverfassungsgerichts (BVerfG) dürfen bestimmte intensive Grundrechtseingriffe nur zum Schutz bestimmter Rechtsgüter bzw. erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden. Entsprechende Eingriffsschwellen sind durch eine gesetzliche Regelung zu gewährleisten (BVerfGE 120, 274 [326 f.]). Dieses verfassungsrechtliche Postulat wurde vom Bundeskriminalamt (BKA) wiederholt unterlaufen. Für den Betrieb einer Datenbank zum Abgleich von Funkzellendaten fehlt es an einer tauglichen Rechtsgrundlage.

Im Berichtszeitraum des 27. Tätigkeitsberichts habe ich eine Datei beanstandet, in der das BKA Daten aus Funkzellenabfragen aus einer Vielzahl von Verfahren aus verschiedenen Bundesländern speicherte (vgl. 27. TB Nr. 9.3.6.2). In dieser Datei glich das BKA personenbezogene Daten ab, die die Strafverfolgungsbehörden in Bund und Ländern durch Funkzellenabfragen erhoben hatten. Gestützt wurde die Datei auf die Generalklausel in § 7 BKAG a.F. (Zentralstellenaufgabe). Besonders eingriffsintensive Datenverarbeitungen bedürfen jedoch einer spezifischen Rechtsgrundlage. Das BVerfG fordert für eingriffsintensive Maßnahmen normenklare und verhältnismäßige Regelungen. Je größer der Grundrechtseingriff, desto genauer muss der Gesetzgeber die Voraussetzungen und Eingriffsschwellen regeln. Welche verfassungsrechtlichen Anforderungen an die tatbestandliche Eingrenzung der jeweiligen Eingriffsbefugnis zu stellen sind, richtet sich vor allem nach Art und Schwere des Grundrechtseingriffs. Dafür sind insbesondere Eingriffsintensität und Streubreite maßgeblich, die im Verhältnis dazu an bestimmte Einschreitschwellen geknüpft sein müssen. Es kommt insbesondere darauf an, ob die Betroffenen selbst einen Anlass für den Eingriff gegeben haben (vgl. BVerfGE 100, 313, 376; 115, 320, 347; 109, 279, 353).

Der Zentralstellengeneralklausel des § 7 BKAG a.F. kommt insofern nur die Funktion einer informationellen Verzahnung und Koordinierung zu. Die Vorschrift kann schwerer wiegende Grundrechtseingriffe aufgrund ihrer zu weiten und zu pauschalen Fassung nicht rechtfertigen (so auch Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 22). Diese Sichtweise sehe ich nun in dem Beschluss des Bundesverfassungsgerichts vom 27. Mai 2020 (BVerfGE 155, 119) bestätigt. Dort hat das Gericht festgehalten, dass das Bundeskriminalamt als Zentralstelle im Wesentlichen auf die Wahrnehmung von Koordinationsaufgaben beschränkt ist (Rn. 209).

Auch § 16 Abs. 1 und Abs. 4 BKAG können hier nicht herangezogen werden. § 16 Abs. 1 BKA befugt das BKA, Daten, die es im Zusammenhang mit der Erfüllung einer bestimmten gesetzlichen Aufgabe erhoben hat, auch für die Erfüllung einer anderen Aufgabe weiter zu verarbeiten. Vorliegend entbehrt jedoch schon die (erstmalige) Erhebung der Funkzellendaten durch das BKA einer gesetzlichen Rechtsgrundlage. Vor allem aber handelt es sich bei § 16 Abs. 1 BKAG um eine Grundnorm, die das BKA in die Lage versetzen soll, personenbezogene Daten zur Erfüllung seiner Aufgaben zu verarbeiten. Insofern ist die Norm im vorliegenden Zusammenhang denselben Einwänden ausgesetzt wie § 7 Abs. 1 BKAG (a.F.).

Daher war ich sehr verwundert, dass das BKA bereits seit 2019 eine Datenbank für die Speicherung und den Abgleich von Funkzellendaten betreibt; eine Information die ich übrigens erst nach mehrfachen Nachfragen erhalten habe. Dies habe ich zum Anlass für eine Kontrolle genommen. Zum Stichtag 6. September 2021 enthielt die Datendank 99.880.125 Datensätze. Solch intensive Eingriffe in die Grundrechte der betroffenen Personen können im Einklang mit der oben zitierten Rechtsprechung weder auf § 7 Abs. 1 i.V.m. § 2 Abs. 1 und 2 BKAG a.F. noch auf § 483 Abs. 1 Strafprozessord

nung gestützt werden. Mangels ausreichender Rechtsgrundlage verstoßen die Datenspeicherung und der Datenabgleich in der betriebenen Datenbank gegen den Gesetzesvorbehalt und sind damit nicht rechtmäßig. Ich habe sie als solche beanstandet. Das Bundesministerium des Innern und für Heimat und das Bundeskriminalamt sind meiner Auffassung entgegengetreten.

8.2.5 Verarbeitung erkennungsdienstlicher Daten durch das Bundeskriminalamt in INPOL-Z

Im Jahr 2011 hatte ich die Speicherung erkennungsdienstlicher Daten (ED-Daten) durch das Bundeskriminalamt (BKA) im bundesweiten zentralen polizeilichen Informationssystem (INPOL-Z) kontrolliert und Nachbesserungen empfohlen (vgl. 24. TB Nr. 7.4.3). Den aktuellen Stand des Bereinigungsprozesses habe ich in einem Beratungs- und Kontrollbesuch geprüft.

Das BKA betreibt das bundesweite zentrale polizeiliche Informationssystem INPOL-Z. In der sogenannten „E-Gruppe“ sind darin erkennungsdienstliche Daten, beispielsweise Fingerabdrücke, gespeichert. Die datenschutzrechtliche Verantwortung für diese Daten tragen die Landespolizeibehörden, die sie in das System einspeichern.

Ursprünglich hatte das BKA diese Daten der Länderpolizeien auch dann weitergespeichert, wenn das verantwortliche Land sie bereits gelöscht hatte. Später wurde diese Verfahrensweise vom BKA geändert und ED-Daten nur dann weitergespeichert, wenn eigene Erkenntnisse vorlagen, die eine eigene Weiterspeicherung rechtfertigten. Bei meiner Prüfung dieser weiteren Speicherung im Jahr 2011 war ich zu dem Ergebnis gekommen, dass eine solche nur dann rechtmäßig ist, wenn ihr eine schriftlich dokumentierte Prognoseentscheidungen über eine weitere Speicherung getroffen wurden (sog. Negativprognosen) zu Grunde liegt (vgl. 24. TB Nr. 7.4.3).

Negativprognosen

Bei einer aktuellen Überprüfung der Umsetzung meiner diesbezüglichen Vorgaben musste ich feststellen, dass in einigen Fällen die erforderlichen Negativprognosen nicht vorlagen. Hierzu habe ich Stichproben von ausgewählten Fällen geprüft, in denen das BKA von einer Landesbehörde eingestellte und mittlerweile nicht mehr benötigte Daten weitergespeichert hat.

Das BKA teilte mir noch vor der Kontrolle mit, speziell für die ED-Daten in keinem der Fälle eine schriftlich dokumentierte Prognoseentscheidung getroffen zu haben, obwohl das BKA Gesetz (BKAG) eine spezielle Negativprognose zu erkennungsdienstlichen Daten (§ 16 Abs. 5 Nr. 2 lit. a) fordert. Vor Ort habe ich daher mit Blick auf eine allgemeine Negativprognose nach §§ 18, 19 BKAG geprüft, welche der speziellen Regelung nach § 16 Abs. 5 Nr. 2 lit. a) fast wortgleich entspricht. Daher bin ich aus datenschutzrechtlicher Sicht damit einverstanden, dass für eine Prognoseentscheidung zu den ED-Daten auf die allgemeine Dokumentation für §§ 18, 19 BKAG verwiesen wird. Teilweise beschränkte sich die Negativprognose allerdings auch insoweit auf die Wiederholung des reinen Gesetzeswortlauts. Faktisch fehlt es daher an dokumentierten Prognoseentscheidungen, so dass ich diese Fälle beanstandet habe.

Bereits in früheren Tätigkeitsberichten habe ich mich zu den Anforderungen an eine sog. Negativprognose geäußert (vgl. 26. TB Nr. 10.3.2). Mit der Prognoseentscheidung muss die Erwartung eines Strafverfahrens gegen eine betroffene Person schriftlich dokumentiert werden, so dass sie gerichtlich voll überprüfbar ist. Fehlt es an dieser Dokumentation, ist die Speicherung rechtswidrig.

Aktueller Stand des Lösch-und Bereinigungsverfahrens von ED-Daten

In INPOL-Z ist die Funktion der „Löschung mit Besitzübertragung“ implementiert worden. Dadurch kann eine E-Gruppe einem anderen Land zur eigenverantwortlichen Weiterspeicherung angeboten werden. Nach meiner Auffassung ist es dabei nunmehr technisch ausgeschlossen, dass eine Übertragung „gegen den Willen“ eines potentiellen neuen Besitzers erfolgen kann.

Als Auswirkung meiner Kontrolle in dem Jahr 2011 wurde zudem die Funktionalität der „Identifizierung mittels „FastID“ in INPOL eingeführt. Eine entsprechende Funktionalität hatte ich seinerzeit aufgrund meiner Kontrolle angeregt. Auf diese Weise kann ein INPOL Teilnehmer sich die in der E-Gruppe gespeicherten Daten aus einer ED-Behandlung „zu Eigen“ machen, indem er lediglich vier Finger einscannt und mit der Fingerabdruck-Datenbank AFIS abgleicht. Im Trefferfall wird nur ein eingeschränkter Datensatz gespeichert, an den dann später die E-Gruppe des „den Besitz aufgebenden“ anderen Landes angehängt wird. Durch diese neue Funktion kann auf weitere ED-Behandlungen verzichtet und dem Grundsatz der Datensparsamkeit Rechnung getragen werden. Ende des Jahre 2020 ist zudem ein automatisiertes Fristlöschverfahren in Betrieb genommen worden.

Zum Lösch- und Bereinigungsverfahren habe ich keine grundsätzlichen datenschutzrechtlichen Bedenken. Positiv möchte ich erwähnen, dass bereits mehr als 4.5 Mio.

E-Gruppen gelöscht wurden, die das BKA als Besitzer von den Ländern ohne Negativprognose übernommen hatte (vgl. 24. TB Nr. 7.4.3). Die im BKA noch verbleibenden 70.000 E-Gruppen werden derzeit geprüft. Ich habe das BKA gebeten, den Altbestand bis zum 31. Dezember 2022 zu bereinigen.

Strukturelle Prüfung von INPOL-Anwendungen

In INPOL-Z werden Vor- und Nachnamen in einem gesonderten Bereich, der sog. P-Gruppe, gespeichert. Aliasnamen werden ebenfalls gesondert gespeichert, nämlich in der sog. A-Gruppe. Von Dritten wurde mir gegenüber die Befürchtung geäußert, diese beiden Bereiche (bzw. Gruppen) könnten möglicherweise derart miteinander verknüpft werden, dass einer Person eine „kriminelle Karriere" einer anderen Person fälschlicher Weise zugerechnet werden würde. Diesen Hinweis habe ich deshalb zum Anlass genommen, um diese Bereiche in INPOL-Z im BKA strukturell zu prüfen. Meine Kontrolle hat ergeben, dass sich die Befürchtung nicht bestätigt.

Ich habe auch noch weitere Bereiche, nämlich die E-Gruppen und die D-Gruppen, in INPOL-Z geprüft. Auch hier konnte ich nicht feststellen, dass diese Gruppen in fälschlicher Weise miteinander verknüpft werden.

ED-Datenspeicherungen aus Anlass von Ordnungswidrigkeiten

Ebenso habe ich auf Bitte einer Landesdatenschutzbehörde Fälle geprüft, in denen erkennungsdienstliche Behandlungen aus Anlass einer Ordnungswidrigkeit durchgeführt und die Daten sodann in INPOL-Z gespeichert wurden. Die Kontrolle der Landesdatensätze fällt zwar nicht in meinen Zuständigkeitsbereich, wohl aber die Prüfung struktureller Fragen in INPOL.

Für die Speicherung erkennungsdienstlicher Daten in INPOL-Z, die aufgrund von Ordnungswidrigkeiten erhoben wurden, sehe ich keine rechtliche Grundlage. Das Gesetz erlaubt es nur, Daten zu Beschuldigten und Verdächtigen einer Straftat zu speichern, bei denen zusätzlich geschilderte Negativprognosen vorliegen. Dem BKA als für die Einhaltung der INPOL-Regelungen verantwortliche Stelle nach § 31 Abs. 1 BKAG habe ich deshalb empfohlen, zukünftig sicherzustellen, dass eine Speicherung dieser Daten technisch nicht mehr umgesetzt werden kann.

Insgesamt verlief der Kontrollbesuch sehr kooperativ und positiv. Ich begrüße vor allem sehr, dass mich das BKA um einen gemeinsamen Workshop zu den gesetzlich erforderlichen Prognoseentscheidungen gebeten hat, um drängende Fragen in diesem Bereich vertieft erörtern und klären zu können.

Ich habe das BMI kurz vor Redaktionsschluss um Stellungnahme zu meinem Bericht über den Beratungs- und Kontrollbesuch gebeten, weshalb noch keine Stellungnahme vorliegt.

8.2.6 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst (BAMAD)

Beim BAMAD habe ich im Berichtsjahr die Pflichtkontrolle der Datenverarbeitungen im Zusammenhang mit Ausschreibungen im Schengener Informationssystem der 2. Generation (SIS II) durchgeführt. Ferner habe ich begonnen, die Datenverarbeitungen im Bereich der Observation zu kontrollieren.

Kontrolle verdeckter Ausschreibungen im SIS II beim BAMAD

Im dritten Quartal 2021 habe ich beim BAMAD verdeckte Ausschreibungen im SIS II kontrolliert (zu weiteren Kontrollen und Informationen rund um das SIS II vgl. o. Nr. 8.1.5). Das BAMAD kann Ausschreibungen im SIS II veranlassen, wenn die darüber zu gewinnenden Informationen zur Abwehr einer von der betroffenen Person ausgehenden erheblichen Gefährdung oder anderer erheblicher Gefahren für die Sicherheit des Staates erforderlich sind. Im Rahmen meines Beratungs- und Kontrollbesuches habe ich keinen beanstandungswürdigen Sachverhalt feststellt. Dennoch habe ich Praxisempfehlungen ausgesprochen, die insbesondere die Implementierung oder Anpassung von Prozessabläufen sowie die Vorgaben zur Löschung von Ausschreibungen betreffen. Ferner habe ich das BAMAD darauf hingewiesen, dass auch in der Corona-Pandemie und bei laufenden Fällen mit einem besonderen Geheimhaltungsbedürfnis eine effektive datenschutzrechtliche Kontrolle sichergestellt sein muss. Die Vorbereitung der Kontrolle hatte sich für mich schwierig gestaltet, da das BAMAD die Übersendung von Unterlagen für eine von mir favorisierte rein schriftliche Kontrolle aus Geheimschutzgründen abgelehnt hatte. Ich bin aber zuversichtlich, dass derartige Friktionen künftig vermieden werden können. Positiv hervorzuheben ist die zeitnahe Reaktion des BAMAD auf meinen Kontrollbericht und die Zusicherung der kurzfristigen Umsetzung meiner Verbesserungsvorschläge.

Kontrolle von Datenverarbeitungen im Bereich der Observation

Im Herbst 2021 habe ich eine Kontrolle im Bereich Observation des BAMAD durchgeführt und hierbei festgestellt, dass wegen des besonderen Umfangs des zu überprüfenden Datenbestandes ein weiterer Kontrolltermin notwendig ist. Die technologischen Möglichkeiten bei der heimlichen Beobachtung von Personen oder Objekten entwickeln sich stetig weiter und die Gewinnung sowie Verwendung von Daten mittels der Observation

sind ein schwerwiegender Eingriff in die Grundrechte der Betroffenen. Aus diesem Grund sah ich mich veranlasst, die Einhaltung datenschutzrechtlicher Bestimmungen beim BAMAD wie auch beim Bundesamt für Verfassungsschutz (vgl. u. Nr. 8.2.7) genau zu überprüfen. Mein Augenmerk bei dieser Art der Kontrolle liegt in der Überprüfung, ob die Datenerhebung im Rahmen der getätigten Observation im konkreten Einzelfall tatsächlich zweck- und verhältnismäßig ist, die Speicherfristen eingehalten werden und ggf. eine doppelte Aktenführung vermieden wird. Aus Gründen der Geheimhaltung und des Fortdauerns meiner Kontrolle kann ich hier keine weitergehenden Ausführungen machen. Über das Ergebnis meiner Kontrolle werde ich berichten.

Querverweise:

8.1.5 Schengener Informationssystem; 8.2.7 Datenschutzaufsicht und Beratung beim Bundesamt für Verfassungsschutz (BfV)

8.2.7 Datenschutzaufsicht und Beratung beim Bundesamt für Verfassungsschutz (BfV)

Beim BfV habe ich im Berichtsjahr die Datenverarbeitung im Bereich der Observation kontrolliert und die Nachbereitung der bereits 2020 durchgeführten Pflichtkontrollen bezüglich der Datenverarbeitungen im Zusammenhang mit Ausschreibungen im Schengener Informationssystem der 2. Generation (SIS II) sowie der Recherchen im Visa-Informationssystem (VIS) fortgeführt. Im Rahmen einiger geplanter Projekte bin ich beratend tätig geworden und werde den begonnenen Austausch auch im kommenden Jahr fortführen. Erfreuliche Ergebnisse konnte ich zudem bei Beratungen zu den künftigen Bescheiden des BfV im Rahmen von Auskunftsersuchen erzielen.

Schnittstellen zwischen Financial Intelligence Unit (FIU) und BfV

Besteht der Verdacht auf Geldwäsche im Zusammenhang mit Terrorismus- oder Extremismusfinanzierung, werden über die FIU dem BfV die Fälle gemeldet. Durch die Einrichtung von teilweise automatisierten Schnittstellen sollen die Übertragungswege verbessert werden. Die rechtlichen Grundlagen sind im Geldwäschegesetz bereits vorhanden. Aufgrund der Menge der Verdachtsmeldungen und zur schnelleren Bearbeitung bzw. Abklärung erscheint eine Verbesserung der Übertragungswege auch aus meiner Sicht sinnvoll. Jedoch haben sich einige Fragen zur genauen Ausgestaltung ergeben, die bislang durch das BfV noch nicht abschließend beantwortet werden konnten. So ist noch offen, auf welche Weise die Bearbeitung durch das BfV genau erfolgen soll, wie lange bestimmte Arten von Meldungen gespe ichert bleiben und welche Zugriffsmöglichkeiten des BfV auf den Datenbestand der FIU möglich sein werden. Ich werde dieses behördenübergreifende Projekt weiter begleiten.

Kontrolle von Recherchen in VIS

Die bereits Anfang des Jahres 2020 durchgeführte Kontrolle der Recherchen des BfV im VIS (vgl. 29. TB Nr. 9.5.1) konnte bislang noch nicht abgeschlossen werden. In diesem Zusammenhang habe ich einige Verbesserungen und Anpassungen der Prozesse sowie der Dokumentation gefordert, die zum Teil auch bereits erfolgt sind. Hinsichtlich der übrigen festgestellten Mängel und geforderten Datenlöschungen ist kurz vor dem Redaktionsschluss eine Stellungnahme des BfV eingegangen, die nun geprüft wird.

Kontrolle von Datenverarbeitungen im Bereich der Observation

Im Herbst 2021 hat meine Behörde eine Kontrolle im Bereich Observation des BfV durchgeführt. Zuletzt wurde dieser Bereich 2006 kontrolliert (vgl. 21. TB Nr. 5.5.2). Gerade vor dem Hintergrund der sich stetig wandelnden technologischen Möglichkeiten hielt ich eine erneute Prüfung für angezeigt. Neue Themenfelder wurden erstmalig beleuchtet. Im Rahmen meines Beratungs- und Kontrollbesuchs konnte ich erfreulicherweise feststellen, dass bereits meine Kontrollankündigung Anlass dafür war, einige wesentliche Prozesse im Bereich der Observation grundlegend zu überarbeiten und datenschutzfreundlicher zu gestalten. Außerdem konnten während der Kontrolle weitere datenschutzrechtliche Schwachstellen identifiziert werden, deren Abstellung bzw. Verbesserung das BfV bereits im Abschlussgespräch zugestanden hat. Aus Geheimschutzgründen ist eine detailliertere Darstellung hierzu nicht möglich. Der Kontrollbericht befindet sich zum Zeitpunkt des Redaktionsschlusses in der Fertigstellung.

Verbund-Dokumentenmanagementsystem

Für den Verfassungsschutzverbund (BfV und alle Landesämter für Verfassungsschutz) und das Bundesamt für den Militärischen Abschirmdienst (BAMAD) soll zukünftig ein einheitliches Dokumentenmanagementsystem (Verbund-DMS) eingeführt werden, das eine weitgehend einheitliche Vorgangsbearbeitung sowie Schnittstellenanbindung für alle beteiligten Behörden gewährleisten soll. Die Art der Datenverarbeitung von Dokumenten gestaltet sich in den Behörden teilweise noch sehr unterschiedlich, so dass mit dem Verbund-DMS deutliche Verbesserungen in der Zusammenarbeit erwartet werden. In diesem Zusammenhang bin ich 2021 gegenüber dem BfV beratend tätig gewesen und habe auf der anderen Seite auch einen engen Austausch mit den Kolleginnen

und Kollegen der Landesdatenschutzbehörden gepflegt. An dieser Stelle war insbesondere die datenschutzrechtliche Einordnung des Verbund-DMS von großer Bedeutung und wird auch künftig weiter ausschlaggebend sein. Auch im kommenden Jahr wird eine gemeinsame Beratung dieses Großprojekts des BfV erforderlich sein.

Kontrolle verdeckter Ausschreibungen im SIS II beim BfV

Im Berichtsjahr 2020 habe ich beim BfV verdeckte Ausschreibungen im SIS II kontrolliert (vgl. 29. TB Nr. 9.5.1; zu weiteren Kontrollen und Informationen rund um das SIS II vgl. o. Nr. 8.1.5). Aufgrund der pandemiebedingten Einschränkungen erreichte mich die Stellungnahme zu meinem Kontrollbericht seitens des BfV erst im Frühjahr 2021. Einige datenschutzrechtliche Defizite wurden behoben sowie Verbesserungsvorschläge umgesetzt, aber über den nach den europarechtlichen Vorschriften des SIS zulässigen Umfangs der zwischen den beteiligten Behörden ausgetauschten Daten besteht noch ein Dissens. Eine Replik auf meine erneute Stellungnahme ging bis zum Reaktionsschluss nicht ein. Ich erwarte einen weiteren konstruktiven Austausch, der noch notwendige Anpassungen der Datenverarbeitungen zur Folge hat.

Ermessensausübung des BfV im Rahmen eines Auskunftsanspruchs nach § 15 Abs. 1 Bundesverfassungsschutzgesetz (BVerfSchG)

Der in § 15 Abs. 1 des BVerfSchG geregelte Auskunftsanspruch über zu ihrer Person gespeicherten Daten ist das grundlegende Kontrollrecht der betroffenen Person gegenüber dem BfV. Er ist Voraussetzung für die effektive Ausübung weiterer Rechte, insbesondere auf Berichtigung, Verarbeitungseinschränkung und Löschung personenbezogener Daten.

Gemäß § 15 Abs. 1 S. 2 BVerfSchG fallen nicht nur solche Daten unter die Auskunftspflicht, die gezielt der antragsstellenden Person in einer zu ihr angelegten sog. Personenakte zugeordnet sind, sondern auch Daten in nicht lediglich personenbezogenen Beständen, d. h. Sachakten. Dem Gesetzeswortlaut nach ist die Auskunftspflicht allerdings beschränkt sich auf „Daten, die über eine Speicherung gemäß § 10 Abs. 1 auffindbar sind", d. h. durch einen gespeicherten Nachweis von Fundstellen im Nachrichtendienstlichen Informationssystem (NADIS), der zentralen Datei des Verfassungsschutzes.

Zu der Frage, ob und wenn ja wie das BfV in den Fällen des § 15 Abs. 1 S. 2 BVerfSchG Ermessenserwägungen anstellen muss, haben sich das OVG Nordrhein-Westfalen (NRW) (Urteil vom 31. Juli 2019, Az. 16 A-1009/14) und zuletzt das BVerwG (Beschluss vom 28. Juli 2020, Az. 6 B-61/19) geäußert.

Nach den Ausführungen des BVerwG reicht es im Rahmen der Ermessensausübung nicht aus, lediglich die Suchmöglichkeiten im elektronischen Aktensystem sowie die einzelnen Schritte bis zu einer Auskunftserteilung zu Grunde zu legen. Vielmehr muss der im Einzelfall erforderliche Verwaltungsaufwand abgeschätzt werden, d. h. es muss zumindest ermittelt werden, wie viele Aktenstücke bei einer Recherche mit dem Namen der antragsstellenden Person auffindbar sind. Erst aus dieser Trefferquote kann man einen Rückschluss auf den tatsächlichen Verwaltungsaufwand ziehen.

Auf Grund dieser beiden Entscheidungen teilte das BfV allen antragsstellenden Personen im Rahmen seiner Ermessensausübung mit, wie viele Aktenstücke bei der Recherche mit ihren Namen in Sachakten auffindbar sind. Jedoch unterblieb eine weitergehende Erläuterung, wie diese Informationen einzuordnen sind. Das BfV wies lediglich pauschal darauf hin, dass sein elektronisches Aktensystem nicht feststellen kann, ob es sich bei dem Suchwort tatsächlich um einen Personennamen handelt und die aufgefundenen Informationen wirklich die antragsstellende Person betreffen.

Weil daher aufgrund der technischen Gegebenheiten jeder Treffer einzeln gesichtet und eine Identitätsprüfung vorgenommen werden muss, lehnte das BfV regelmäßig eine weitergehende Auskunft mit Verweis auf die hohe Trefferzahl und den dadurch unverhältnismäßigen Verwaltungsaufwand ab. Diese pauschale Aussage hat berechtigterweise zu Irritationen bei den antragsstellenden Personen geführt. Um mir selber ein Bild von den technischen Gegebenheiten zu machen, habe ich im dritten Quartal dieses Jahres einen Beratungs- und Kontrollbesuch beim BfV durchgeführt. Dabei bestätigte sich der vom BfV geschilderte Verwaltungsaufwand. Im Nachgang habe ich dem BfV einen Formulierungsvorschlag für einen Auskunftsbescheid unterbreitet, der die technischen Voraussetzungen der Suche in der elektronischen Akte und den damit einhergehenden Verwaltungsaufwand transparenter darstellt und somit insgesamt bürgerfreundlicher ist.

Ich freue mich daher über die Zusage des BfV, künftig meinen Formulierungsvorschlag im Wesentlichen zu übernehmen. Darüber hinaus bin ich mit dem BfV im Gespräch, welche sonstigen Verfahrensänderungen den Verwaltungsaufwand ggf. reduzieren können, um Betroffenen im Einzelfall auch eine inhaltliche Rückmeldung geben zu können.

Querverweise:

8.1.5 Schengener Informationssystem

8.2.8 Kontrollen zum Sicherheitsüberprüfungsgesetz – Viel „bad practice“ und ein wenig „best practice“

Mitte 2020 habe ich ein eigenständiges Referat für die Datenschutzkontrolle von Sicherheitsüberprüfungsverfahren eingerichtet. So konnte ich im Jahr 2021 trotz COVID-19 mehr Kontrollen als in der Vergangenheit durchführen. Die Ergebnisse zeigen, dass sich bestimmte festgestellte Fehler wie ein roter Faden durch fast alle Kontrollen ziehen, es aber auch Lichtblicke gibt.

Im Berichtszeitraum habe ich in vier Wirtschaftsunternehmen und acht Behörden kontrolliert, ob dort die Datenschutzbestimmungen des Sicherheitsüberprüfungsgesetzes (SÜG) eingehalten werden.

Nach diesem Gesetz werden alle Personen überprüft, die an ihrem Arbeitsplatz im öffentlichen Dienst oder einem Privatunternehmen Zugang zu Verschlusssachen des Bundes (geheimhaltungsbedürftigen Informationen) oder lebens- oder verteidigungswichtigen Einrichtungen erhalten. Hierbei wird eine ganze Reihe persönlicher Daten erhoben und verarbeitet.

Bei den kontrollierten Behörden handelte es sich um

- die Bundesanstalt für Finanzdienstleitungsaufsicht
- die Generaldirektion Wasserstraßen und Schifffahrt
- die Bundespolizeidirektion Sankt Augustin
- das Deutsche Patent- und Markenamt
- die Bundesanstalt für Immobilienaufgaben
- das Bundeskartellamt
- das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie
- das Bundesamt für den Militärischen Abschirmdienst.

Von den kontrollierten Wirtschaftsunternehmen sind zwei im Bereich der Bewachung und eines im Bereich der Gebäudereinigung tätig. Das vierte Wirtschaftsunternehmen ist Betreiber einer kritischen Infrastruktur.

Bei einer dieser Kontrollen handelte es sich um eine Nachkontrolle. Die Mängel, die ich in dem betreffenden Unternehmen bereits im Jahr 2017 festgestellt habe (vgl. 27. TB Nr. 9.3.13), wurden leider nicht vollständig abgestellt. Ich habe erneut mehrere erhebliche datenschutzrechtliche Verstöße festgestellt und deshalb eine Beanstandung gegenüber dem Bundesministerium für Wirtschaft und Energie ausgesprochen, das das Unternehmen hinsichtlich des Geheimschutzes betreut.

Auch bei den kontrollierten Behörden gab es Anlass für Beanstandungen. Diese richteten sich unter anderem an das Bundesministerium des Innern, für Bau und Heimat (BMI). Hintergrund waren festgestellte Datenschutzverstöße beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Eine weitere Beanstandung gegen das BMI erfolgte nach einer Bürgereingabe und betraf Datenschutzverstöße bei der Zentralen Stelle für Informationstechnik im Sicherheitsbereich. Des Weiteren habe ich eine Beanstandung gegen das Bundesministerium für Verkehr und digitale Infrastruktur aufgrund datenschutzrechtlicher Verstöße der Generaldirektion Wasserstraßen und Schifffahrt ausgesprochen.

Im Übrigen sind meine Feststellungen im Wesentlichen vergleichbar mit den Verstößen, die ich bereits in vorherigen Berichtszeiträumen aufgedeckt habe (vgl. 28. TB Nr. 6.7.4 und 29. TB Nr. 9.5.5). Zu den häufigsten Mängeln gehörte ein unzureichender Informationsfluss zwischen Geheimschutz- und Sabotageschutzbeauftragten bzw. Sicherheitsbevollmächtigten einerseits und der Personalstelle anderseits. Ebenso führten Mängel bei der Wiedervorlage wiederholt zur Missachtung von Vernichtungs- und Löschfristen. Des Weiteren habe ich immer wieder unzulässige Inhalte in den Sicherheitsakten festgestellt, wie beispielsweise Kopien von Bundespersonalausweisen, Pässen und Aufenthaltstiteln sowie Dokumente mit personenbezogenen Daten unbeteiligter Dritter, die gar nicht oder unzureichend geschwärzt waren.

Sieben der Kontrollen waren bei Redaktionsschluss noch nicht endgültig abgeschlossen. Obwohl bei allen Kontrollen Datenschutzverstöße oder Mängel im Bereich des Sicherheitsüberprüfungsverfahrens aufgedeckt wurden, konnte ich teilweise von Beanstandungen absehen, weil Mängel umgehend behoben wurden oder es sich um Einzelfälle ohne schwerwiegende Folgen handelte. Auffällig war, dass der Bereich Geheim- und Sabotageschutz bei den zuständigen Stellen oft keine angemessene Aufmerksamkeit erfährt. Ursächlich sind unter anderem Unkenntnis, Zeit- oder Personalmangel. Häufig war hier meine Beratung gefragt, um Geheimschutz- und Sabotageschutzbeauftragte oder Sicherheitsbevollmächtigte zu unterstützen und für ein datenschutzkonformes Vorgehen in Sicherheitsüberprüfungsverfahren zu sensibilisieren und zu ertüchtigen. Ich freue mich sehr, dass dieses Angebot von den geprüften Stellen angenommen wurde.

Best Practice / Positives

Bei manchen Kontrollen befanden sich datenschutzrechtliche Verstöße im weit überwiegenden Teil der geprüften Akten. Ich begrüße es jedoch, dass die kontrollierten Stellen sich durchweg kooperationsbereit zeigten und bereits einige festgestellte Mängel behoben haben. Im Einzelfall konnte vor Ort abgeholfen und der Schutz der informationellen Selbstbestimmung der jeweils betroffenen Person unmittelbar wiederhergestellt werden.

Besonders positiv hob sich ein Wirtschaftsunternehmen hervor. Dort waren 99,39 Prozent der Akten vorbildlich geführt. Durch eine Kennzeichnung der betroffenen Person im Personalverwaltungssystem stellt das Wirtschaftsunternehmen eine zuverlässige und datenschutzfreundliche Verarbeitung der Informationen sicher, die zur Sicherheitsakte genommen werden müssen. Das System erinnert den Sicherheitsbeauftragten nach fünf Jahren daran, dass eine Aktualisierungs- bzw. Wiederholungsprüfung zu erfolgen habe oder die entsprechende Akte zu vernichten sei. Dadurch wird sichergestellt, dass die Wiedervorlagen entsprechend funktioniert. Verstöße habe ich hier nicht festgestellt. Stattdessen bestätigt dies, dass ein technisch und organisatorisch durchdachtes System für die Führung der Sicherheitsakten und Steuerung der damit verbundenen Arbeitsprozesse förderlich ist.

Positiv fiel mir außerdem bei der Bundespolizeidirektion Sankt Augustin auf, dass der Geheimschutzbeauftragte einen jährlichen Geheimschutzbericht fertigt, der die Behördenleitung über dessen Tätigkeit und Entwicklungen im Bereich des Sicherheitsüberprüfungsrechts informiert. Der Geheimschutzbericht stellt einen gewissen Informationsfluss sicher und ist gleichzeitig ein sehr gutes Beispiel dafür, wie sich dieser spezielle Bereich in einer Behörde Gehör verschaffen kann.

Querverweise:

6.20 Das Sicherheitsüberprüfungsgesetz – Ein Gesetz mit vielen Fragezeichen

8.2.9 Kontrolle und Beratung bei der Financial Intelligence Unit (FIU)

Seit ihrer Verlagerung vom Bundeskriminalamt (BKA) zur Generalzolldirektion (GZD) im Jahre 2017 hat die FIU keine Löschungen in ihrer Datenbank vorgenommen. Daneben habe ich weitere datenschutzrechtliche Mängel feststellen müssen, die zu mehreren Beanstandungen geführt haben. Außerdem habe ich die FIU zur Verwendung von Echtdaten in Softwaretests beraten.

In meinem 29. Tätigkeitsbericht (Nr. 6.8) habe ich bereits über die FIU und ihre Arbeitsweise berichtet. Im Fokus standen dabei die Neugestaltung ihrer IT-Landschaft und die Entwicklung des Informationsverbundes FIU 2.0. Im aktuellen Berichtszeitraum habe ich nun erstmalig eine Kontrolle bei der FIU zur Löschung personenbezogener Daten durchgeführt.

Mit Wirkung zum 26. Juni 2017 hat die FIU als unabhängige administrative Behörde ihren Wirkbetrieb unter dem Dach der GZD aufgenommen. Sie ist zuständig für die Entgegennahme, Sammlung und Auswertung von Meldungen über verdächtige Finanztransaktionen, die im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung stehen können. Sie verarbeitet in diesem Zusammenhang eine immense Anzahl von Geldwäscheverdachtsmeldungen, die sensible personenbezogene Daten enthalten.

Im Juni 2020 sind nach der Verlagerung der FIU vom BKA zur GZD erstmalig die in der Errichtungsanordnung (EAO) zum jetzigen Informationsverbund-FIU vorgesehenen Löschfristen abgelaufen. Dies habe ich zum Anlass genommen, mich sowohl bei der FIU als auch bei der verantwortlichen Fach- bzw. Rechtsaufsicht im Bundesministerium der Finanzen (BMF) nach dem Sachstand der Umsetzung der Löschvorgaben zu erkundigen. In mehreren Stellungnahmen wurde mir mitgeteilt, dass zu diesem Zeitpunkt weder der erforderliche Löschmechanismus im System implementiert werden konnte, noch manuelle Löschungen personenbezogener Daten durch die Sachbearbeitung erfolgt sind. Diese Aussagen habe ich zum Anlass genommen, ein förmliches Kontrollverfahren bei der FIU einzuleiten.

Die Kontrolle ergab mehrere datenschutzrechtliche Mängel, die ich jeweils gegenüber dem BMF beanstandet habe.

So sehen die gesetzlichen Regelungen vor, dass bereits vor der Inbetriebnahme eines Systems sowohl technische als auch manuelle Vorkehrungen getroffen werden müssen, um Datenschutzgrundsätze wirksam umzusetzen und die Rechte der betroffenen Personen zu schützen. Dies hat die FIU versäumt. Der Informationsverbund-FIU wurde sogar mehrere Jahre betrieben, ohne die Löschvorgaben des für ihre Arbeit maßgeblichen Geldwäschegesetzes und der o. g. EAO zu beachten. Gleichzeitig hat die FIU es unterlassen, ihre Mitarbeitenden mit entsprechenden Berechtigungen für manuelle Löschungen auszustatten. Meine Einzelfallprüfungen haben dies bestätigt. In meiner Stichprobenkontrolle konnte ich bei mehr als einem Drittel der Einzelfälle das Vorliegen der Löschvoraussetzungen feststellen. Eine Löschung erfolgte in keinem dieser Fälle. Die FIU und das BMF verweisen als Kompensation für die unterbliebenen Löschungen auf eine eingeführte Einschränkung der Verarbeitung. Dies vermag die datenschutzrechtlichen Verstöße aber nicht abzumildern. Ich habe dem

BMF in diesem Kontext mitgeteilt, dass es bereits am Vorliegen der gesetzlichen Voraussetzungen für eine Anwendbarkeit der Ausnahmeregelung mangelt.

Die FIU bzw. das BMF haben die Implementierung technischer Löschvoraussetzungen im System in die Wege geleitet und mir eine schnellstmögliche Umsetzung zugesichert. Manuelle Löschungen durch die Sachbearbeitung lehnt das BMF jedoch in weiten Teilen ab. Manuelle Löschungen seien unter anderem mit dem Kernauftrag der FIU nicht vereinbar. Es müsse ein möglichst großer Datenpool zu Analysezwecken zur Verfügung stehen, da vermeintlich harmlose Sachverhalte im späteren Verlauf zu werthaltigen Meldungen erstarken könnten.

Dies führt zu meinem nächsten Kritikpunkt: Das pauschale, ungeprüfte Überführen von Geldwäscheverdachtsmeldungen in den Datenpool der FIU zwecks Datenhaltung auf Vorrat und zur Nutzung der Daten zu Analyse- und Recherchezwecken verstößt gegen den Grundsatz der Datenminimierung. Einer Datenspeicherung auf Vorrat hat das Bundesverfassungsreicht bereits in anderem Kontext mehrfach eine Absage erteilt. Zudem widerspricht eine solche Vorgehensweise den ausdrücklichen Vorgaben des Geldwäschegesetzes, das neben regelmäßigen Aussonderungsprüfungen auch explizit Prüfungen bei der Einzelfallbearbeitung vorsieht. Selbiges gilt für die o. g. EAO. Sofern Daten für die Aufgabenerledigung der FIU nicht mehr erforderlich sind, sind diese zu löschen.

Bei meiner Kontrolle musste ich zudem eine mangelnde Dokumentation und Aktenführung bei der FIU feststellen, die mir meine Prüfung erheblich erschwerte. Hierzu zählen beispielsweise unvollständige, uneinheitliche oder widersprüchliche Angaben im Vorgangsbearbeitungssystem, das Fehlen von Fristeintragungen sowie fehlende Begründungen und Entscheidungen für eine Weiterspeicherung. Eine größer angelegte Datenschutzkontrolle und auch eine Eigenkontrolle der Behörde halte ich vor diesem Hintergrund für kaum durchführbar.

Insgesamt besteht Nachbesserungsbedarf bei der FIU. Die Umsetzung der gesetzlichen Vorgaben muss sich künftig im Arbeitsablauf der Sachbearbeitung und im Löschkonzept für den neuen FIU-Informationsverbund 2.0 wiederfinden. Ich werde daher weiter auf eine datenschutzkonforme Aufgabenwahrnehmung durch die FIU drängen und den Umsetzungsprozess überwachen.

Beratung der FIU bezüglich Testung mittels Echtdaten

Die Verarbeitung personenbezogener Daten bei der FIU unterliegt gesetzlich festgelegten Zwecken. Testzwecke fallen nicht darunter. Da es auch im Interesse des Datenschutzes liegt, eine hohe Qualität der eingesetzten Software sicherzustellen, habe ich die FIU zu grundrechtsschonenden Alternativen beraten.

Die FIU ist mit der Ankündigung an mich herangetreten, für verschiedene Test- bzw. Entwicklungsvorhaben Echtdaten verwenden zu wollen. Hierfür solle eine Kopie ihrer gesamten operativ genutzten Datenbank verwendet werden. Konkret ging es um die Aktualisierung bestehender Software, die Einführung des bereits erwähnten Löschmechanismus sowie einer Rechercheschnittstelle. Auch für das (kontinuierliche) Training der Künstlichen Intelligenz-Modelle von FIU-Analytics seien unveränderte Echtdaten zwingend notwendig. Die FIU gab an, dass sie dies auf Grundlage des Echtbetriebs für rechtlich zulässig halte.

Hinsichtlich der Verwendung von Echtdaten zu Testzwecken habe ich jedoch meine Bedenken geäußert. Zwar ist das Testen von Software auch aus Datenschutzsicht unerlässlich, um die Integrität der Datenverarbeitung zu gewährleisten. Personenbezogene Daten unterfallen jedoch dem Zweckbindungsgrundsatz. Dem für die FIU relevanten Geldwäschegesetz (GwG) dürfte es allerdings bislang an einer hinreichend bestimmten und normenklaren Rechtsgrundlage für die Testung von IT-Anwendungen mit Echtdaten fehlen. Tests mit einer Kopie der gesamten Produktivdatenbank würden auch dem Datenschutzgrundsatz der Datenminimierung widersprechen. Bevor eine Testung mit Echtdaten überhaupt in Betracht gezogen werden kann, ist immer zu prüfen, ob keine weniger eingriffsintensiven Möglichkeiten zur Verfügung stehen, um den mit dem Softwaretest verfolgten Zweck zu erreichen.

Im weiteren Verlauf bin ich mit der FIU in einen Austausch eingetreten, um vielfältige Alternativen zur Testung mit Echtdaten aufzuzeigen. Vor allem habe ich die systematische Erstellung von Testfällen angeregt, die spezifische Anforderungen, aber auch Randfälle und Negativ-Tests abdecken. Eine weitere Alternative wäre die Generierung künstlicher Testdaten. Um unvorhergesehene Fehler aufzuspüren, könnten dabei auch Techniken wie Fuzzing zum Einsatz kommen. Zur Vermeidung von Fehlern habe ich auch auf die Gewährleistung der Datenqualität hingewiesen. Zuletzt wäre auch eine vorherige Anonymisierung oder Pseudonymisierung von Echtdaten vor einer Nutzung zu Testzwecken denkbar.

Neben der Problematik einer fehlenden Rechtsgrundlage wären diese Testmöglichkeiten prioritär auszuschöpfen, bevor ggf. die Verwendung personenbezogener Echtdaten im Rahmen eines Pilotbetriebs in Betracht kommt. Die Verarbeitung von Daten durch die FIU werde ich weiter begleiten.

8.2.10 Kontrolle nicht lizenzierter Postdienstleister

Im Berichtsjahr habe ich das erste Mal den großen Bereich der nicht lizenzierten Postdienstleister kontrolliert. Pandemiebedingt konnte die Kontrolle nur schriftlich erfolgen. Auch wenn ich auf diesem Wege einen guten Einblick in die Datenverarbeitung der kontrollierten Unternehmen gewinnen konnte, werde ich in Zukunft wieder einen Schwerpunkt auf die Beratung und Stichprobenkontrolle vor Ort legen.

Unternehmen, die beabsichtigen, in Deutschland Briefe bis zu einem Gewicht von 1.000 Gramm zu befördern, benötigen als Postdienstleister eine Lizenz der Bundesnetzagentur. Werden nur schwerere Briefsendungen und Pakete befördert oder Kurierdienste erbracht, benötigt ein Postdienstleister keine Lizenz, aber die Tätigkeit als Postdienstleister ist anzuzeigen. Als nicht lizenzierte Postdienstleister sind mehrere zehntausend Unternehmen bei der Bundesnetzagentur angezeigt, vom Einzelunternehmen über Fahrrad-Kurierdienste bis hin zu großen Speditionen.

Eine datenschutzrechtliche Kontrolle muss sich daher auf Stichproben beschränken. Ich habe im Berichtsjahr einer zufälligen Auswahl von nicht lizenzierten Postdienstleistern einen Fragebogen mit allgemeinen Fragen zum Datenschutz sowie zur Verarbeitung personenbezogener Daten bei der Erbringung der Postdienstleistung übermittelt.

Im Ergebnis habe ich bei den kontrollierten Postdienstleistern keine gravierenden datenschutzrechtlichen Mängel festgestellt. Die kontrollierten Unternehmen verarbeiteten oft nur in sehr geringem Umfang personenbezogene Daten im Rahmen ihrer Dienstleistung, der Sortierung und Postzustellung vor Ort. Regelmäßig waren sie für lizenzierte Postdienstleister als Subunternehmer tätig und nutzten deren Infrastruktur.

Allerdings zeigte sich, dass in den Unternehmen wenig Sensibilität für datenschutzrechtliche Themen vorhanden ist und ein großer Informations- und Aufklärungsbedarf besteht, der durch Kontrollen allein nicht gedeckt werden kann. Ich werde daher auch meine Informationsangebote für diese Unternehmen ausbauen, ergänzt durch direkte Beratung im Rahmen von Kontrollbesuchen vor Ort.

8.2.11 Fragebogenkontrolle Betroffenenrechte

Die Betroffenenrechte nach der Datenschutz-Grundverordnung (DSGVO) sind vielfach Gegenstand von Anfragen, sowohl direkt gegenüber Unternehmen und Behörden als auch in Form von Eingaben und Beschwerden, die an mich als Aufsichtsbehörde gerichtet werden. Im Postdienstleistungssektor habe ich daher mehr als ein Dutzend Unternehmen zur Umsetzung der Betroffenenrechte schriftlich kontrolliert.

Betroffene, deren personenbezogene Daten verarbeitet werden oder wurden, verfügen nach dem 3. Kapitel der DSGVO über eine Reihe von Betroffenenrechten. Zum einen hat der Verantwortliche die Betroffenen über jede Verarbeitung personenbezogener Daten zu informieren, zum anderen gibt die DSGVO diesen Personen dann aktive Rechte an die Hand: Sie können Auskunft, Berichtigung, gegebenenfalls Löschung oder Einschränkung der Verarbeitung verlangen, ihre Daten in einem gängigen Format erhalten und übertragen oder Widerspruch gegen die Verarbeitung einlegen. Nähere Informationen zu den Betroffenenrechten und Hinweise dazu, wie sie ausgeübt werden können, finden sich auf meiner Internetseite (www.bfdi.bund.de).

Nach einer Vielzahl von Einzelfallprüfungen im Rahmen von Eingaben und Beschwerden zu den Betroffenenrechten habe ich in diesem Jahr eine zweistellige Anzahl an Postdienstleistern zur Umsetzung dieser Rechte kontrolliert. Die Verantwortlichen sollten detailliert Auskunft zur Umsetzung der rechtlichen Vorgaben machen und mir Einblick in ihre entsprechenden Prozesse gewähren.

Das positive Ergebnis zeigt ein durch die Bank solides Datenschutzniveau. Alle Unternehmen haben sich mit den Betroffenenrechten und der Frage, wie sie gewährt werden sollen, befasst. Vielfach liegen verschriftlichte Prozesse mit klaren Verantwortlichkeiten vor – schließlich will die Monatsfrist zur Beantwortung der Anträge der Betroffenen im Regelfall eingehalten werden.

Allerdings habe ich den Antworten durchaus auch Schwachpunkte entnommen. Gerade das zentrale Auskunftsrecht muss von dem ein oder anderen Verantwortlichen noch an die jüngsten Entwicklungen der Rechtsprechung angepasst werden. Vereinzelte Hinweise auf ein anderes Verständnis von rechtlichen Vorgaben wurden gegenüber den kontrollierten Stellen kommuniziert und werden bei Notwendigkeit auch entsprechend durchgesetzt.

Erwartungsgemäß gehen bei größeren Unternehmen wesentlich mehr Anfragen zu Betroffenenrechten ein als bei regional tätigen Postdienstleistern. Durch die Kontrolle sind aber in allen angeschriebenen Unternehmen die Betroffenenrechte stärker ins Bewusstsein der involvierten Mitarbeitenden gerückt. Ich bin daher zuversichtlich, dass Betroffene ihre Rechte gegenüber diesen Unternehmen in Zukunft noch effektiver ausüben können.

Querverweise:

3.2.5 Leitlinien Recht auf Auskunft Art. 15 DSGVO

9 BfDI intern

9.1 Organisationsuntersuchung

Die Ergebnisse einer Organisationsuntersuchung zeigen u. a., dass für eine optimale Erfüllung meines gesetzlichen Auftrags bei gewachsenen und noch wachsenden Aufgaben zusätzliche Personalkapazitäten benötigt werden.

In meiner Behörde wurde von August 2020 bis Oktober 2021 eine hausweite Organisationsuntersuchung einschließlich einer Personalbedarfsermittlung (PBE) durchgeführt. Diese sollte klären, welche aufbau- und ablauforganisatorischen Optimierungspotenziale bestehen. Besonders mit Blick auf die künftige Aufgabenwahrnehmung und damit verbundene Ressourcenverteilung sollte insbesondere die PBE für die künftigen Haushaltsaufstellungen eine valide Basis bilden. Dies entsprach auch Forderungen des Rechnungsprüfungsausschusses des Deutschen Bundestages und des Bundesrechnungshofes.

Die Federführung hatte mein Organisationsreferat mit externer Unterstützung durch ein vom Bundesverwaltungsamt ausgesuchtes Beratungsunternehmen. In die Organisationsuntersuchung waren alle Organisationseinheiten einschließlich Leitungsstab und die Zentrale Anlaufstelle (ZASt) eingebunden. Die Untersuchung orientierte sich an den methodischen Empfehlungen des Organisationshandbuchs des Bundesministeriums des Innern, für Bau und Heimat (BMI).

Aufgrund dieser Empfehlungen wurde für die PBE zunächst ein initialer Aufgabenkatalog für alle Organisationseinheiten erstellt und validiert, der anschließend mit den Organisationeinheiten abgestimmt wurde, so dass eine retrospektive Aufwandsschätzung auf Basis der zum 30. November 2020 zur Verfügung stehenden Personalkapazitäten möglich war. Aufgrund dieser Datenlage konnte sowohl eine aufgabenkritische Betrachtung (Zweck- und Vollzugskritik) der Ist-Analyse als auch eine Prozess- und Schnittstellenanalyse vorgenommen werden. Dadurch wurden Optimierungspotentiale deutlich. Die vertiefte Analyse erfolgte in den von mir als strategisch prioritär betrachteten Themenfelder „Zentrales Wissensmanagement“, „Kontrollen“ und „Bearbeitung von Bürgereingaben“.

Die sich anschließende prospektive Ressourcenbedarfsschätzung für die Fachaufgaben unter Berücksichtigung der Ergebnisse der aufgabenkritischen Betrachtung und gesetzlichen Aufgabenstellungen hat gezeigt, dass mir zur qualitativen Erfüllung meines gesetzlichen Auftrages nach wie vor Ressourcen fehlen.

Die Feststellung, dass ich zur Erfüllung meines – stetig erweiterten – gesetzlichen Auftrages, der immer stärker techniküberlagert ausgeführt werden muss, weitere IT-Spezialisten benötige, ist eine wichtige Erkenntnis dieser Organisationsuntersuchung.

Darüber hinaus konnte festgestellt werden, dass neben der Übertragung weiterer gesetzlicher Aufgaben auch die Intensität der Aufgabenwahrnehmung deutlich angestiegen ist, insbesondere durch eine gestiegene Anzahl von Verfahren und Technologien der digitalen Datenerfassung und -verarbeitung. Beides ist nur mit ausreichenden Personalressourcen umsetzbar, da die personellen Ressourcen hierfür intern nicht mehr erwirtschaftet werden können.

9.2 Personalentwicklung im Jahr 2021

Meiner Behörde standen 2021 insgesamt 346,4 Stellen zur Verfügung. Trotz der Corona-Pandemie, die auch 2021 persönliche Kontakte deutlich einschränkte, und einer Reihe neuer Stellen im Bundeshaushalt 2021 konnte ich ca. 75 % der zur Verfügung stehenden Stellen besetzen. Hierfür habe ich die hausinterne Videokonferenztechnik nutzen und viele Nachwuchskräfte und erfahrene Beschäftigte gewinnen können. Ich sehe mich auf einem guten Weg, die vom Haushaltsgesetzgeber zur Verfügung gestellten Stellen besetzen zu können.

Für das Berichtsjahr 2021 hat mir der Haushaltsgesetzgeber insgesamt 346,4 Stellen zugestanden, damit ich meine Aufgaben ordnungsgemäß erfüllen kann. Diese teilen sich in 328,9 Planstellen für Beamtinnen und Beamte sowie in 17,5 Stellen für Tarifbeschäftigte auf. Mir ist es auch in Pandemiezeiten gelungen, zahlreiche Nachwuchskräfte und erfahrene Beschäftigte für mein Haus zu gewinnen. Demgegenüber habe ich im Jahr 2021 nur sechs Personalabgänge verzeichnet, die teilweise unvorhergesehen waren. Insgesamt weist mein Haus zum 31. Dezember 2021 eine Personalstärke von 275 Personen auf.

So wie im Berichtsjahr 2020 waren die Personalgewinnungsverfahren stark von der pandemischen Situation überlagert. Aufgrund der Kontaktbeschränkungen konnte ich entgegen meiner ursprünglichen Planungen die Bewerbungsauswahlverfahren erst im 2. Quartal starten. Noch habe ich die gewünschte Anzahl an neuen Kolleginnen und Kollegen nicht erreicht. Im Jahr 2021 habe ich insgesamt 432 Bewerbungen erhalten und konnte mithilfe moderner hausinterner Videokonferenztechnik 29 Bewerbungsverfahren durchführen. 153 Personen haben sich in meinem Hause vorgestellt, aus denen ich über 44 neue Kolleginnen und Kollegen gewinnen konnte. Hiervon haben bereits 26 Kolleginnen und Kollegen ihren Dienst bei mir angetreten, weitere 18 Personen folgen im Jahr 2022. Ich bin weiterhin zuversichtlich, als attraktiver Arbeitgeber in den kommenden Monaten die noch offenen Positionen in meinem Haus besetzen zu können.

Um auch auf diese Weise für meine Behörde als Arbeitgeber zu werben, habe ich in den vergangenen Monaten wieder acht Studierende und zehn Referendarinnen und Referendare eingeladen, Ausbildungstage in meinem Hause zu absolvieren. Zudem habe ich begonnen über den üblichen Girls and Boys Day in Bonn hinaus, Schülerpraktika durchzuführen. Das erste hat im November 2021 mit gutem Erfolg und regem Interesse stattgefunden. Auch das von mir geplante Gesamtpersonalentwicklungskonzept wird derzeit nach thematischen Modulen konzipiert und mit den Interessensvertretungen abgestimmt Zudem ist mir ein wertschätzender Umgang miteinander wichtig, deshalb habe ich auch ein Konzept zum Konfliktmanagement in Kraft gesetzt. Zudem konnte ich ein umfängliches Aufstiegskonzept vorlegen und mit den Interessensvertretungen abstimmen.

9.3 Presse- und Öffentlichkeitsarbeit

Die Pressearbeit meiner Behörde wurde auch 2021 weitgehend von Themen im Zusammenhang mit der Corona-Pandemie bestimmt. Ein Dauerbrenner insbesondere für die Fachpresse bleibt außerdem die elektronische Patientenakte. Mit der Öffentlichkeitsarbeit erreichen wir immer mehr Bürgerinnen und Bürger. Der offizielle Account meiner Behörde beim dezentralen Kurznachrichtendienst Mastodon hat mittlerweile über 3.000 Abonnenten. Die interessierte Öffentlichkeit konnte durch digitale Formate zum ersten Mal live an zwei BfDI-Veranstaltungen teilnehmen. Und: Bei unseren Kinderbüchern zum Thema Datenschutz ist die Nachfrage sehr hoch.

Pressearbeit

Die meisten Anfragen an meine Pressestelle hatten auch 2021 einen thematischen Bezug zur Corona-Pandemie: Mit Corona-Warn-App, Digitalem Impfnachweis und 3G am Arbeitsplatz seien nur ein paar der wichtigsten Schlagworte genannt. Wie im Vorjahr wurde ich dabei häufig mit dem Vorurteil konfrontiert, Datenschutz würde eine effektive Bekämpfung der Pandemie verhindern, mindestens aber verzögern oder unnötig bürokratisieren. Ich werde nicht müde werden, die Öffentlichkeit davon zu überzeugen, dass hier ein Gegensatz konstruiert wird, den es nicht gibt. Gleiches gilt für die Auflistung vermeintlicher „Datenschutzpannen“ oder „Schildbürgerstreiche“, die mit dem Verweis auf angeblich überbordenden Datenschutz in Deutschland enden. So wurde beispielsweise immer wieder behauptet, der Versand von Impfeinladungen in Niedersachsen sei am Datenschutz gescheitert. Gleiches gilt für die öffentlichen Klagen der Deutschen Gesellschaft für Orthopädie und Unfallchirurgie, dass die Befüllung des Traumaregisters durch den Datenschutz erschwert werde. Dort, wo meine Behörde gefragt wurde, konnten wir solche Mythen sehr schnell durch Fakten widerlegen.

Im Zusammenhang mit der Pandemie muss wohl auch das kurzfristige aber gleichwohl in den Medien ausführlichst diskutierte Phänomen des Sozialen Netzwerks „Clubhouse“ gesehen werden. In digitalen Räumen sollte dort ausschließlich verbal diskutiert werden. Entsprechende Anfragen habe ich an meine Kolleginnen und Kollegen in den Bundesländern weitergeleitet, da ich die App aufgrund fehlender Zuständigkeit nicht geprüft habe.

Umgekehrt hatte meine Ankündigung, die Nutzung von Facebook Pages bei den Bundesministerien ab Januar 2022 zu prüfen, keine Auswirkungen auf die Nutzung durch Landesbehörden oder Kommunen. Ich habe viele

dieser Anfragen mit einem Verweis auf die föderale Organisation des Datenschutzes in Deutschland beantwortet und mein Schreiben an die Bundesbehörden im Transparenzbereich meiner Internetseite veröffentlicht.

Ein ebenfalls sehr hohes Interesse gab es bei bestimmten Einzelthemen. Dazu zählt meine Untersagung der Nutzung der Studie Kindeswohl und Sorgerecht, die Gesetzgebung zur Registermodernisierung, meine Untersuchung von journalistischen Anfragen an den Bundesbeauftragten für die Stasiunterlagen und die Entwicklungen zur elektronischen Patientenakte. Während die ersten Themen nur temporär großes mediales Interesse nach sich zogen, wird die elektronische Patientenakte immer mehr zum „Dauerbrenner".

Im Zusammenhang mit der Flutkatastrophe gab es ein herausragendes mediales Interesse am Thema „Cell Broadcasting" (vgl. 11.2 Datenschutzfreundliche Katastrophenwarnung). Neben den Fragen zum Datenschutz musste ich hier insbesondere die Funktionsweise von Cell Broadcasting immer wieder erläutern. Leider lese ich trotzdem in der Berichterstattung immer noch die fälschliche Bezeichnung „Warn-SMS". Ich kann Medienschaffende daher nur auffordern, sich weiterhin vertrauensvoll mit Anfragen an meine Pressestelle zu wenden, um Datenschutz-Mythen vorzubeugen.

Ich habe im Berichtszeitraum 16 Pressemitteilungen herausgegeben und war einmal zu Gast in der Bundespressekonferenz. Außerdem habe ich sieben Gastbeiträge bzw. Aufsätze für verschiedene Medien verfasst. Meine Pressestelle hat 526 Anfragen per Mail und 511 telefonische Anfragen beantwortet.

Internetseite und Social Media

2020 habe ich eine eigene Instanz des dezentralen Kurznachrichtendienstes Mastodon in Betrieb genommen. Der offizielle Account meiner Behörde (social.bund.de/@bfdi) hat mittlerweile über 3.000 Abonnenten. Neben der Veröffentlichung von Pressemitteilungen und neuen Dokumenten auf meiner Internetseite beantworte ich auch Fragen von Nutzenden. Diesen Austausch möchte ich in Zukunft intensivieren und so noch mehr Einblicke in die Arbeit meiner Behörde geben.

Ich habe meine Instanz außerdem für alle Bundesministerien und oberste Bundesbehörden sowie den Deutschen Bundestag, die Landesparlamente und die Landesdatenschutzbeauftragten geöffnet. Auf meine offizielle Einladung habe ich allerdings bisher nur wenige positive Rückmeldungen erhalten. Ich werde mein Angebot gegenüber der neuen Regierung wiederholen und weiter für datenschutzfreundliche Social Media Angebote werben.

Ich möchte zusätzlich den Erfahrungsaustausch der interessierten Öffentlichkeit in den Bereichen Datenschutz und Informationsfreiheit stärken. Zu diesem Zweck habe ich im Frühjahr 2021 das „Datenschutzforum" (https://forum.bfdi.bund.de) wiederbelebt. Die rege Beteiligung im Forum und das positive Feedback bestärken mich darin, auch in Zukunft den Austausch mit der Datenschutz-Community zu suchen.

Im Sommer 2021 habe ich außerdem meinen Internetauftritt (https://bfdi.bund.de) überarbeitet. Der neue Aufbau und die neue Optik sollen Inhalte einfacher auffindbar machen. Die neue Seite richtet sich stärker danach, nach welchen Informationen gesucht wird. So gibt es zielgerichtete Angebote für Bürgerinnen und Bürger, Fachleute oder Medienschaffende. Auch Kontaktdaten und Formulare sind nun einfacher aufzufinden. Allerdings kam es bei der Neugestaltung der Internetseite zu einer kurzen Datenpanne, bei der über den Zeitraum von mehreren Tagen aufgrund eines Konfigurationsfehlers keine Beschwerden über die neuen online-Formulare an meine Behörde weitergeleitet wurden. Der Fehler konnte jedoch schnell behoben werden.

Veranstaltungen

Im Berichtszeitraum konnten aufgrund der Einschränkungen durch die Corona-Pandemie keine Präsenzveranstaltungen mit größerem Teilnehmerkreis durchgeführt werden. Allerdings konnte ich erstmals mit dem Informationsfreiheit-Symposium 2021 und dem Symposium zu polizeilichen Informationssystemen digitale Veranstaltungen anbieten. Durch datenschutzkonforme Streams erreichte ich hierdurch sogar mehr interessierte Personen, als es mit einer Präsenzveranstaltung möglich gewesen wäre.

Im Rahmen der Veranstaltungsreihe „Bonner Tage der Demokratie" habe ich mich an der virtuellen Diskussion zum Thema „Wieviel Grundrechtsverlust ist mir die Nutzung von Instagram Wert?" beteiligt.

Ich hoffe, dass es die Lage im nächsten Jahr zulässt, nicht nur mehr solcher Veranstaltungen anbieten zu können, die dann hoffentlich auch wieder in Präsenz oder hybrid durchgeführt werden.

Besuchergruppen

Durch die Corona-Pandemie hat leider in diesem Jahr keine Besuchergruppen-Betreuung stattgefunden.

Informationsmaterial

Als Teil meiner Beratungs- und Aufklärungsarbeit konnte ich im Dezember 2021 meine mit dem CARLSEN Verlag entwickelten Kinderbücher zum Thema Datenschutz veröffentlichen. Das Pixi-Buch „Die Daten-Füchse – Das

ist privat!“ wurde für Kinder im Kindergartenalter, deren Eltern und alle Pixi-Liebhaber entworfen. Das Buch aus der Pixi Wissen-Reihe „Die Daten-Füchse – Was ist Datenschutz?“ ist für Kinder der Grund- und weiterführenden Schulen sowie für alle interessierten Leserinnen und Leser erstellt worden.

Um zu erleben wie die junge Leserschaft meine neuen Pixi-Bücher findet, war ich zu Besuch in je einer Bonner Grund- und Gesamtschule. Ich war begeistert wie schnell und ohne Scheu wir ins Gespräch kamen, wie viele Fragen gestellt wurden und auch wie kritisch die Schülerinnen und Schüler gegenüber Abfragen von persönlichen Daten beim Downloaden von Apps oder Spielen gegenüberstehen.

Die Nachfrage an kind- und jugendgerechten Informationsmaterial war und bleibt ungebrochen. In weniger als einer Woche gingen mehr als 9.000 Bestellungen zu meinen Pixi-Büchern ein. Dies zeigt mir einmal wieder, dass wir auf einem guten Weg sind. Aus diesem Grund gibt es in 2022 eine zweite Auflage der „Daten-Füchse“.

Gleichzeitig werden die beiden aktuellen Pixi-Bücher in Videos umgesetzt. Hiermit möchte ich eine weitere Informationsquelle öffnen und sicherstellen, dass unsere wichtigen Botschaften dauerhaft und jederzeit zur Verfügung stehen.

Auch unsere anderen Publikationen waren dieses Jahr wieder gefragt. Bei den Broschüren für das Fachpublikum und interessierte Bürgerinnen und Bürger ist und bleibt die „Info 1“ mit ihren Texten und Erläuterungen zur Datenschutzgrundverordnung (DSGVO) und zum Bundesdatenschutzgesetz (BDSG) der Dauerbrenner. Aber auch die neue aufgelegte „Info 6“ mit den Hinweisen zur DSGVO in der Bundesverwaltung stieß auf großes Interesse. Bei meinen Flyern war besonderes „Telearbeit und Mobiles Arbeiten – Ein Datenschutz-Wegweiser“ in Zeiten der Corona-Pandemie und Homeoffice ein wichtiges und gefragtes Informationsmaterial für Bürgerinnen und Bürger.

Fokusgruppentest

Ein wichtiger Teil meines gesetzlichen Auftrags ist es, die Öffentlichkeit für das Thema Datenschutz zu sensibilisieren. Dabei sollen spezifische Maßnahmen für Kinder besondere Beachtung finden. Um eine zielgruppengerechte Ansprache bei der Schaffung von Angeboten an Kinder und Jugendliche zu ermöglichen, habe ich einen Fokusgruppentest durchführen lassen. Damit haben wir in der Zielgruppe ermittelt:

- wie das Thema Datenschutz im Bewusstsein von Kinder und Jugendliche ausgeprägt ist und wie sie zum Thema stehen,
- wo Kinder und Jugendliche in ihrem Alltag mit dem Thema in Berührung kommen,
- was Kinder und Jugendliche spannend an dem Thema finden und was sie weniger interessiert und
- mit welcher Ansprache Kinder und Jugendliche für das Thema begeistert werden könnten.

Mit den Ergebnissen aus dem Fokusgruppentest werden wir nun zielgerichtet weitere Angebote für Kinder und Jugendliche schaffen.

Querverweise:

11.2 Datenschutzfreundliche Katastrophenwarnung

9.4 Am Ort des Geschehens: Das Hauptstadtteam des BfDI

Meine Behörde unterhält schon lange ein kleines Verbindungsbüro in der Bundeshauptstadt mit Kolleginnen und Kollegen aus verschiedenen Fachreferaten. Angebunden an den Leitungsbereich habe ich dort nun zusätzlich ein Hauptstadtteam gebildet, das rund um das politische Geschehen als zentraler Ansprechpartner vor Ort fungiert.

Ganz wesentlicher Teil meines gesetzlichen Auftrags ist die Beratung von Bundestag und Bundesrat sowie der Bundesregierung und anderer Einrichtungen und Gremien. Dies gilt insbesondere hinsichtlich legislativer und administrativer Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten.

Berlin ist die Drehscheibe des nationalen politischen Geschehens und des damit einhergehenden gesellschaftlichen, wirtschaftlichen und wissenschaftlichen Austausches. Dies fordert von meiner in Bonn angesiedelten Behörde eine örtliche Vertretung auch an der Spree, während die europäische Vernetzung besser vom Rhein aus gewährleistet werden kann. Für die strukturierte Vernetzung im politischen Raum habe ich zur Bündelung der Informations- und Austauschwege und so auch als Entlastung für meine Fachebenen in einem ersten Schritt im Verbindungsbüro ein Hauptstadtteam gebildet. Es ist beim Leitungsbereich angesiedelt und soll spezifische politische Informationen sowie die Kommunikation im Kontext des Berliner Politikbetriebs bündeln und für mein Haus aufbereiten. Ich verstehe mich zudem aufgrund meines gesetzlichen Auftrags insbesondere auch als Dienstleister für Parlament und Regierung und messe dieser Schnittstelle besonderer Bedeutung zu.

Mit dem neuen Hauptstadtteam ist es mir nun möglich, mein Informationsangebot für den Parlamentarischen Bereich auszubauen. So erscheint regelmäßig mit dem Parlamentsbrief ein spezielles Informationsformat für Abgeordnete und deren Mitarbeiterinnen und Mitarbeiter. Dieser ist auf meiner Homepage, aber auch anschließend öffentlich verfügbar (www.bfdi.bund.de/parlamentsbrief). Daneben biete ich für die genannte Zielgruppe Workshops zu Datenschutzgrundlagen und ausgewählten Einzelthemen an. Dies soll neben der Informationsvermittlung helfen, Verständnis und Einfühlungsvermögen für die Belange des Datenschutzes zu schärfen. Dieses Angebot machen wir auch den deutschen Europaabgeordneten.

Überdies zählt auch der Kontakt und Austausch mit allen übrigen Hauptstadtakteuren aus Wirtschaft, Wissenschaft und Gesellschaft zu den Aufgaben des Hautstadtteams. Schließlich bin ich gehalten, maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und von Geschäftspraktiken. Hinter beiden Aufgaben steht der Gedanke, dass dem Schutz der Daten der Bürgerinnen und Bürger am besten gedient ist, wenn ich als Sachwalter frühzeitig auf grundrechtsfreundliche Lösungen hinwirke und helfe, Fehlentwicklungen zu vermeiden.

9.5 BfDI in Zahlen

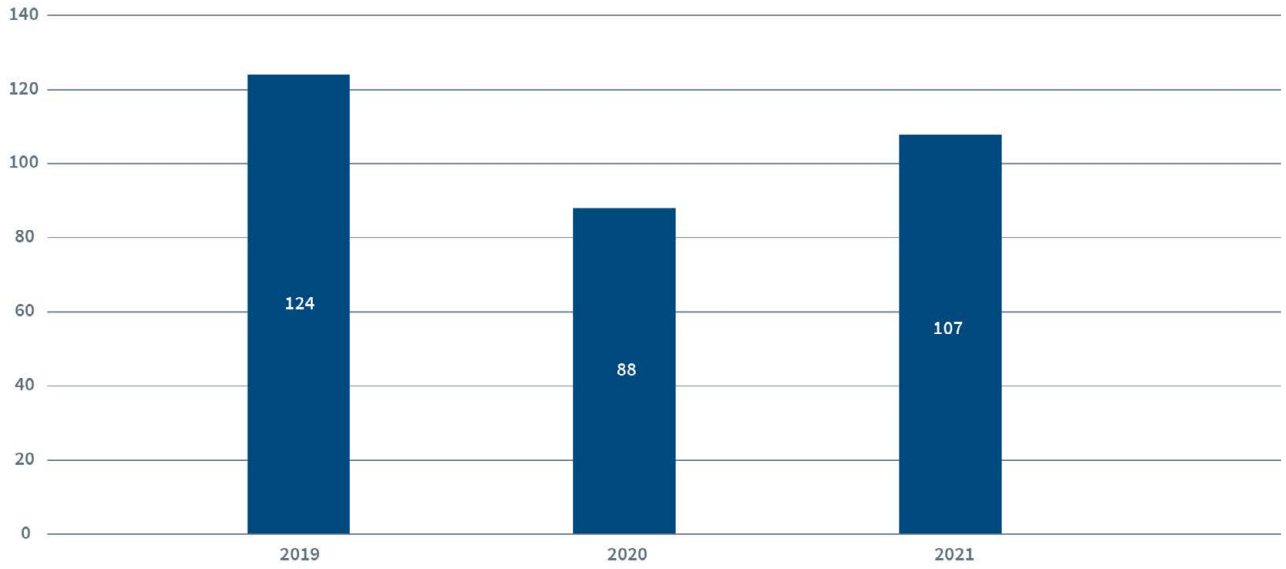
In den vorangegangenen Kapiteln habe ich über die über ausgewählte einzelne Punkte des Datenschutzjahres 2021 berichtet. Die alltägliche Arbeit meiner Behörde spiegelt dies allerdings nur in Teilen wieder. Die folgenden Zahlen und Statistiken liefern einen besseren Überblick, womit ich im vergangenen Jahr befasst war.

Beratung und Kontrolle

Eine der wichtigsten Tätigkeiten meiner Behörde ist die Beratung und Kontrolle der beaufsichtigten Stellen. Kontrollbesuche kann ich pandemiebedingt weiterhin leider nur eingeschränkt durchführen. Hinter der Zahl von 107 Kontrollen im Berichtsjahr verbergen sich deshalb 82 schriftliche Kontrollen.

Zusätzlich zur Kontrolltätigkeit bin ich mit insgesamt 37 – teils virtuellen – Beratungs- und Informationstreffen auf die beaufsichtigten Stellen zugegangen, um über die konkrete Umsetzung des Datenschutzes im Gespräch zu bleiben.

Beratungen und Kontrollen bei beaufsichtigten Stellen



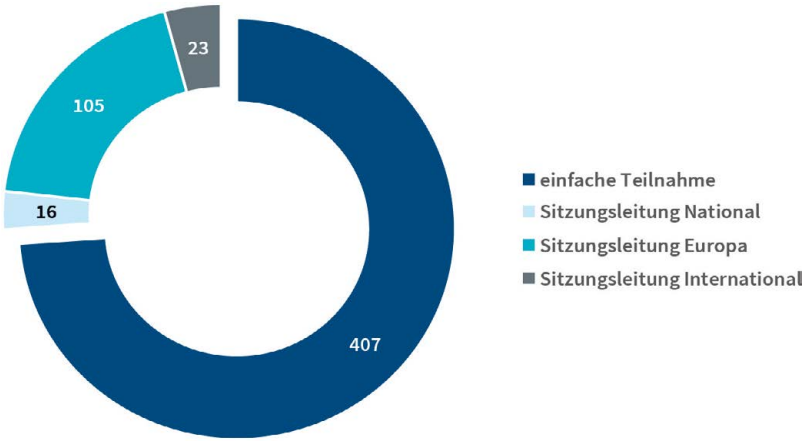
Gremienarbeit

Die Datenschutzaufsicht erfordert nicht nur auf nationaler, sondern auch auf europäischer Ebene eine ständige Koordinierung, um auf eine einheitliche Um- und Durchsetzung der Datenschutz-Grundverordnung (DSGVO) hinzuwirken. Darüber hinaus nimmt auch die weitergehende internationale Vernetzung der Datenschutzbehörden eine immer wichtigere Rolle ein.

In diesen Prozess bringe ich mich aktiv im Sinne der Weiterentwicklung von Datenschutz und Informationsfreiheit ein. So habe ich im Berichtsjahr die Leitung der Berlin Group übernommen und aktiv im Executive Commitee der Global Privacy Assembly mitgewirkt.

Dies stellt einen umfangreichen Aufwand für mich und meine Mitarbeiterinnen und Mitarbeiter dar. Alle Treffen von Hauptgremien, Arbeitskreisen und Subgroups zusammengenommen, war meine Behörde im Berichtsjahr bei 551 Sitzungen vertreten. Besonders hervorzuheben ist dabei, dass in gut einem Viertel dieser Sitzungen die Sitzungsleitung (bzw. stellvertretende Sitzungsleitung) von meiner Behörde gestellt wurde.

Sitzungen in nationalen und internationalen Gremien



Beschwerden und Anfragen

Im Berichtsjahr richteten Bürgerinnen und Bürger insgesamt 6.829 Beschwerden und Anfragen an mich. Außerdem konnte ich 7.124 Personen telefonisch beraten. Das entspricht grob den Zahlen der beiden Vorjahre. Nach der großen Welle des Anfrageaufkommens zum Start der DSGVO hat sich der Beratungsbedarf von Bürgerinnen und Bürgern damit scheinbar auf dem gegenwärtigen Level eingependelt.

Eine Eingabe gilt dann als Beschwerde, wenn die betroffene Person annimmt, sie sei bei der Erhebung, Verarbeitung oder Nutzung ihrer persönlichen Daten in ihren Rechten verletzt worden. Andernfalls ist sie als allgemeine Beratungsanfrage zu werten. Der Unterschied zwischen den Eingabearten liegt in deren Rechtsfolge, da Beschwerden grundsätzlich förmlich beschieden werden. Das Beschwerderecht ist sowohl in der DSGVO als auch in Spezialgesetzen geregelt.

Beschwerden und Anfragen

	2019	2020	2021
Allgemeine Anfrage	4.280	4.897	4.329
Beschwerde Art. 77 DSGVO	3.118	2.861	2.383
Beschwerde Art. 80 DSGVO	3	25	19
Beschwerde § 60 BDSG	44	56	54
Eingabe gegen Nachrichtendienste	44	39	44

Meldung von Datenschutzverstößen

Sämtliche öffentlichen und nicht-öffentlichen Stellen müssen gegenüber der zuständigen Aufsichtsbehörde Datenschutzverstöße melden. Ich habe im Berichtszeitraum 10.157 entsprechende Meldungen erhalten. Die Meldungen an meine Behörde stammen insbesondere von Finanzämtern, Jobcentern und Telekommunikationsanbietern.

Die bei Einführung der DSGVO teilweise beobachteten überobligatorischen Meldungen gehören mittlerweile der Vergangenheit an. Das jährliche Aufkommen pendelt sich bei ca. 10.000 Meldungen ein.

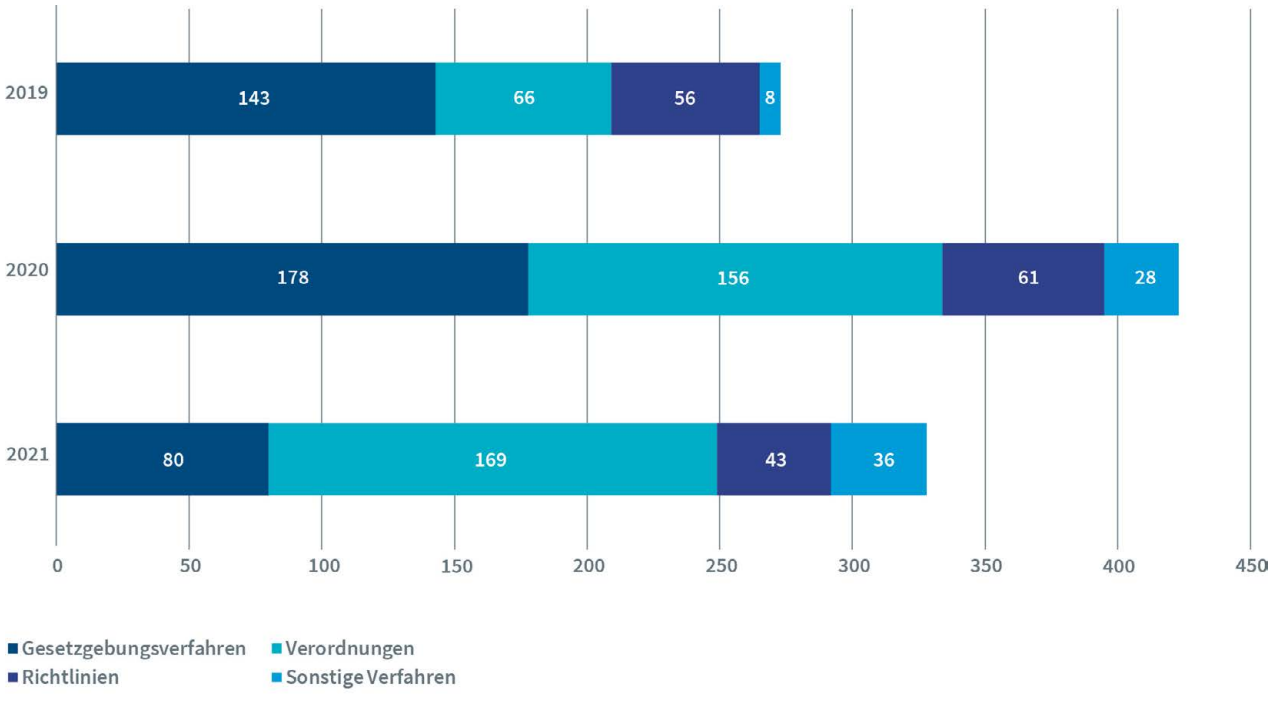
Meldungen von Datenschutzverstößen	2019	2020	2021
Meldungen nach DSGVO	14.649	9.987	10.106
Meldungen nach § 109a TKG	40	37	51

Förmliche Begleitung bei Rechtsetzungsvorhaben

Gemäß § 21 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) hat das federführende Ressort mich bei der Erstellung von Gesetzesvorlagen frühzeitig zu beteiligen, soweit dadurch meine Aufgaben berührt werden. Wie an mehreren Stellen in diesem Bericht ausgeführt, funktioniert dies leider nicht immer reibungslos. Im Berichtsjahr sind, trotz der Bundestagswahl, wieder einige Beteiligungen zusammengekommen, mehr als in vergleichbaren wahlfreien Jahren mit Ausnahme des durch die COVID-Pandemie geprägten Jahres 2020. Insbesondere die Beteiligungen an Gesetzgebungsverfahren entfielen dabei auf das erste Halbjahr.

Neben den in der Grafik aufgeführten 328 Beteiligungen nach § 21 GGO habe ich zu 43 Dateianordnungen, 18 EU-Rechtsakten und einem Verfahren des Bundesverfassungsgerichts Stellung genommen. Außerdem konnte ich mich als Sachverständiger in zwölf Anhörungen von Ausschüssen des Deutschen Bundestages einbringen.

Beteiligungen nach § 21 GGO



Eingaben mit Bezug zum Informationsfreiheitsrecht

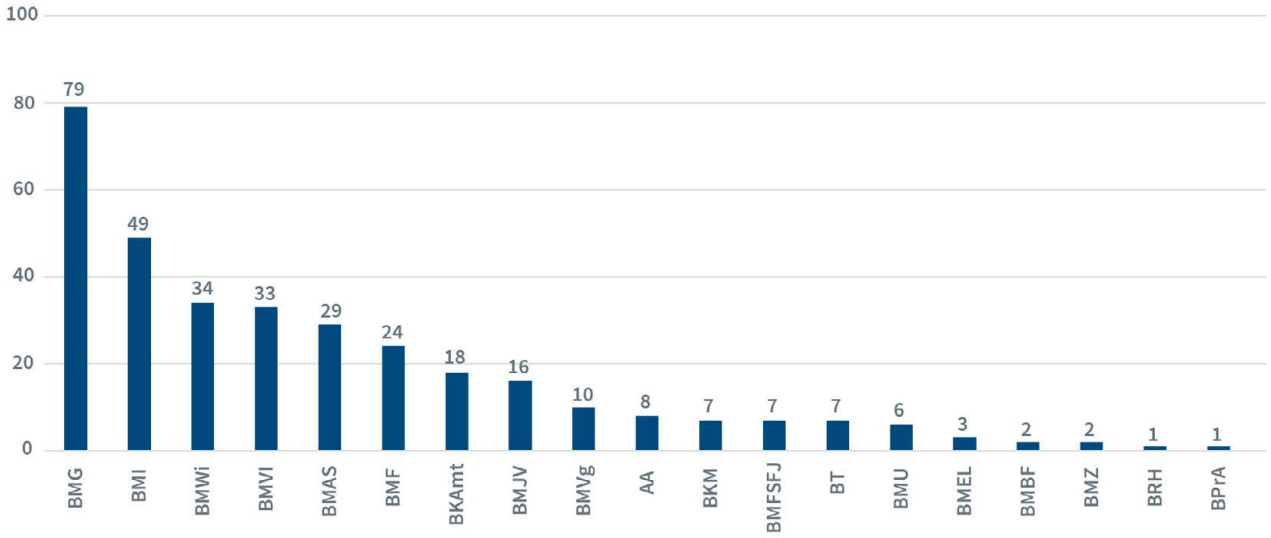
Mich erreichten im Berichtszeitraum insgesamt 622 Eingaben. Nach einem Ausreißer im letzten Jahr ist die Anzahl der Eingaben damit wieder auf dem Niveau der Vorjahre angekommen.

Meine Ombudsfunktion im Bereich des Informationsfreiheitsgesetzes (IFG) wurde durch eine Änderung des Umweltinformationsgesetzes (UIG) ab März 2021 auch auf umweltinformationsrechtliche Belange des UIG erweitert. Seither erreichten mich im Berichtszeitraum insgesamt 10 Bitten um Vermittlung bei Anträgen nach dem UIG. Die den Eingaben zugrundeliegenden Anträge bezogen sich mehrheitlich auf Emissionen, etwa durch Strahlung oder im Zusammenhang mit dem sog. „Diesel-Skandal“. Ich gehe davon aus, dass die Zahlen mit zunehmender Bekanntheit meiner neuen Aufgabe weiter ansteigen werden.

Bei den Eingaben zu Fragen und Themen aus dem Bereich des IFG handelte es sich in 276 Fällen um allgemeine Anfragen zur Informationsfreiheit.

In 336 Fällen riefen mich Petenten in meiner Funktion als Ombudsperson nach § 12 Abs. 1 IFG an und rügten eine Verletzung ihres Rechts auf Informationszugang. Der größte Teil der Eingaben betrafen dabei das Bundesministerium für Gesundheit und seinen Geschäftsbereich, was – wie im Vorjahr – am starken Interesse der Antragsteller an Informationen im Zusammenhang mit der Corona-Pandemie liegt. Antragsinhalte waren unter anderem das Risikomanagement bei Coronaerkrankungen, Anfragen im Zusammenhang mit Impfstoffen und der Beschaffung von FFP2-Masken.

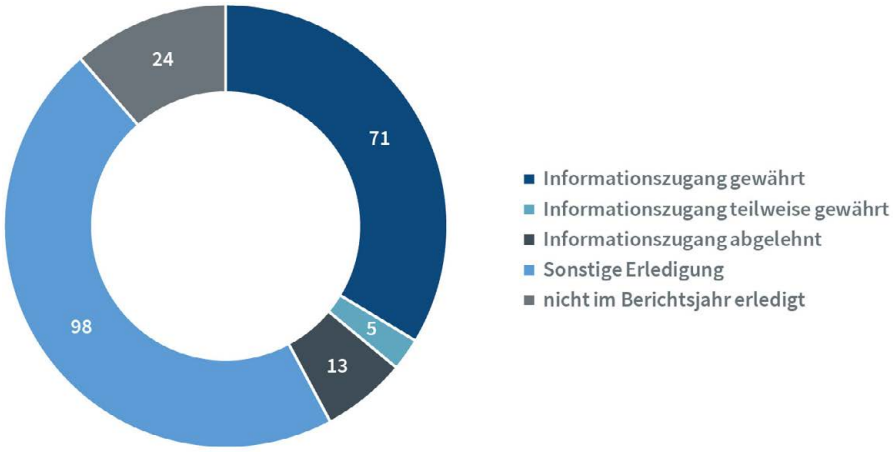
Statistik der Anrufungen nach § 12 Abs. 1 IFG



IFG-Anträge an meine Behörde

Im Berichtszeitraum gingen insgesamt 211 Anträge auf Informationszugang bei mir ein. Diese Anträge richteten sich sowohl auf den Zugang zu Akteninhalten über selbst an den meine Behörde gerichtete Eingaben, als auch auf meine Stellungnahmen zu Gesetzesvorhaben. Im Vergleich zu den Vorjahren bleibt das Aufkommen auf diesem Niveau stabil.

IFG-Anträge an meine Behörde



10 Zentrale Anlaufstelle

10.1 Rückblick

Die Zentrale Anlaufstelle (ZASt) koordiniert die grenzüberschreitende Zusammenarbeit den Datenschutzaufsichtsbehörden des Bundes und der Länder mit den anderen Mitgliedstaaten der Europäischen Union, dem Europäischen Datenschutzausschuss (EDSA) und der Europäischen Kommission. Aus Sicht der ZASt war das Jahr 2021 geprägt von ersten wegweisenden Entscheidungen gegen führende Technologieunternehmen. Darüber hinaus wurde die Zusammenarbeit der deutschen Aufsichtsbehörden Richtung Europa intensiviert, befördert durch die nunmehr erfolgte Wahl eines Stellvertreters des gemeinsamen Vertreters durch den Deutschen Bundesrat.

Das Jahr 2021 markiert eine Zeitenwende in der Arbeit des EDSA. So wurden erste wichtige, teils lang ersehnte Entscheidungen zu großen Technologieunternehmen getroffen. Damit verbunden sind maßgebliche Weichenstellungen für die Durchsetzung der Datenschutzrechte von Millionen Betroffener. Die Entscheidung der luxemburgischen Datenschutzbehörde zum Online-Versandhändler Amazon mit einem Bußgeld von 746 Mio. Euro hat die Durchschlagskraft der DSGVO demonstriert. Sie wird eine erhebliche Signalwirkung für mehr datenschutzgerechtes Handeln entfalten. Das intensive Ringen der nationalen und europäischen Datenschutzaufsichtsbehörden lässt sich gut an den Entscheidungen zum sozialen Netzwerk Facebook und dem Messenger-Dienst WhatsApp nachvollziehen.

Erstes Dringlichkeitsverfahren in Sachen Facebook: irische Aufsichtsbehörde zu Untersuchung verpflichtet

Die angekündigten Änderungen bei der Datenschutzerklärung und den Nutzungsbedingungen des Messenger-Dienstes WhatsApp ließen befürchten, dass personenbezogene Daten von WhatsApp an Facebook weitergegeben würden. Mit Blick auf die erheblichen Gefahren für die Datenschutzrechte der WhatsApp-Nutzenden in Deutschland hatte der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) am 10. Mai 2021 der europäischen Hauptniederlassung von Facebook in Irland per einstweiliger Maßnahme für drei Monate untersagt, personenbezogene Daten von WhatsApp-Nutzenden mit Wohnsitz in Deutschland zu eigenen Zwecken zu verarbeiten.

Um eine endgültige Maßnahme gegen Facebook zu erhalten, ersuchte HmbBfDI den EDSA im Dringlichkeitsverfahren binnen einer Frist von zwei Wochen um einen verbindlichen Beschluss. Dies war keine einfache Aufgabe für dieses Gremium, das sich aus Aufsichtsbehörden der 27 EU- und der drei EWR-Staaten sowie dem Europäischen Datenschutzbeauftragten zusammensetzt. Zudem handelte es sich um das erste Verfahren dieser Art überhaupt und es waren innerhalb der kurzen Frist eine Reihe schwieriger prozeduraler und datenschutzrechtlicher Fragen zu beantworten. Prozedural ging es um die Frage, welche Anforderungen an die Dringlichkeit zu stellen sind und ob gegebenenfalls eine Konstellation vorliegt, bei der die Dringlichkeit gesetzlich vermutet wird. In der Sache befasste sich der EDSA mit den verschiedenen Zwecken, zu denen personenbezogene Daten zwischen WhatsApp und Facebook ausgetauscht werden. Nach Auffassung des EDSA sind einige der Datenaustausche mit hoher Wahrscheinlichkeit rechtswidrig, auch wenn eine abschließende Bewertung anhand der im Dringlichkeitsverfahren vorliegenden Informationen nicht möglich ist.

Die ZASt sah sich vor die Herausforderung gestellt, vorgelagert zur Abstimmung auf europäischer Ebene in einem engen Zeitrahmen die Abstimmung zwischen den deutschen Aufsichtsbehörden der 16 Länder und des Bundes zu organisieren. Dass diese nationale Abstimmung gelang, ist einer besonderen Kraftanstrengung und der konsequenten Umsetzung der etablierten Prozesse der deutschen Aufsichtsbehörden zu verdanken. Allerdings konnte sich die so gefundene deutsche Position im EDSA trotz erreichter Unterstützung nicht mehrheitlich durchsetzen. Anders als von HmbBfDI erbeten, ordnete der EDSA nicht unmittelbar die Verhängung endgültiger Maßnahmen gegen Facebook an. Er

beschränkte sich darauf, der irischen Aufsichtsbehörde lediglich aufzugeben, den Vorwürfen weiter nachzugehen.

Streitbeilegungsverfahren in Sachen WhatsApp: höheres Bußgeld erwirkt

Etwas erfolgreicher aus deutscher Sicht verlief ein Verfahren zur Erfüllung datenschutzrechtlicher Transparenzpflichten durch den Messenger-Dienst WhatsApp. Die europaweit federführende irische Aufsichtsbehörde legte hierzu – nach langwierigen Untersuchungen – an Heiligabend 2020 einen Beschlussentwurf vor, der u. a. die Verhängung eines Bußgelds vorsah. Neben Deutschland hatten zahlreiche weitere europäische Aufsichtsbehörden Einspruch gegen den Beschlussentwurf erhoben. Daraufhin leitete die irische Aufsichtsbehörde – in dieser Form erstmalig – ein Verfahren zur Streitbeilegung vor dem EDSA ein. Auch wenn aufgrund eines einfach gelagerten früheren Falles sowie kurz zuvor erarbeiteter Leitlinien (vgl. Nr. 3.2.6) schon Orientierungspunkte zum Streitbeilegungsverfahren vorlagen, stellten sich zahlreiche schwierige Fragen, auch verfahrensrechtlicher Art. So musste zunächst für jeden Einspruch und zu jedem Einspruchspunkt über dessen Zulässigkeit entschieden werden. Der EDSA nutzte diese Gelegenheit, um die Anforderungen an eine ordnungsgemäße Einspruchsbegründung weiter zu entwickeln. Das ist eine Voraussetzung für eine weitere Befassung in der Sache. Inhaltlich ging es um die Transparenz der Datenverarbeitung bei WhatsApp. Als Vorfrage war zu klären, bei welchen Vorgängen personenbezogene Daten verarbeitet werden. Hier prüfte der EDSA auch die Adressbuchuploadfunktion von WhatsApp. Er kam zu dem Ergebnis, dass die übertragenen Rufnummern im konkreten Fall auch dann personenbezogene Daten sind, wenn sie einem verlustbehafteten Streuwertverfahren (englisch „Hashing“) unterzogen werden.

Wegen der Komplexität verlängerte die EDSA-Vorsitzende die Verfahrensfrist auf zwei Monate. Der EDSA-Beschlussentwurf sah vor, den Einsprüchen teilweise stattzugeben. Die Nichtberücksichtigung einiger deutscher Einspruchspunkte stieß bei einzelnen deutschen Aufsichtsbehörden auf Bedenken.

Durch Nichtberücksichtigung dieser Einsprüche vergebe der EDSA die Chance, neben der Transparenz auch die Rechtmäßigkeit der zugrundeliegenden Datenverarbeitungen von WhatsApp in den Blick zu nehmen, die die federführende Aufsichtsbehörde als nicht vom Untersuchungsumfang umfasst sehe. Mit Blick auf die ansonsten positiv bewerteten Ergebnisse fand der Beschluss dennoch im Ergebnis die Zustimmung aller deutschen Aufsichtsbehörden. Am 28. Juli 2021 verabschiedete der EDSA seinen Beschluss, der u. a. zur Folge hatte, dass ein deutlich höheres Bußgeld gegen WhatsApp in Höhe von 225 Mio. Euro verhängt wurde. Zwischenzeitlich hat WhatsApp Rechtsmittel eingelegt, so dass die Entscheidung noch nicht rechtskräftig ist.

Zunehmend sichtbare Ergebnisse in der grenzüberschreitenden Fallbearbeitung

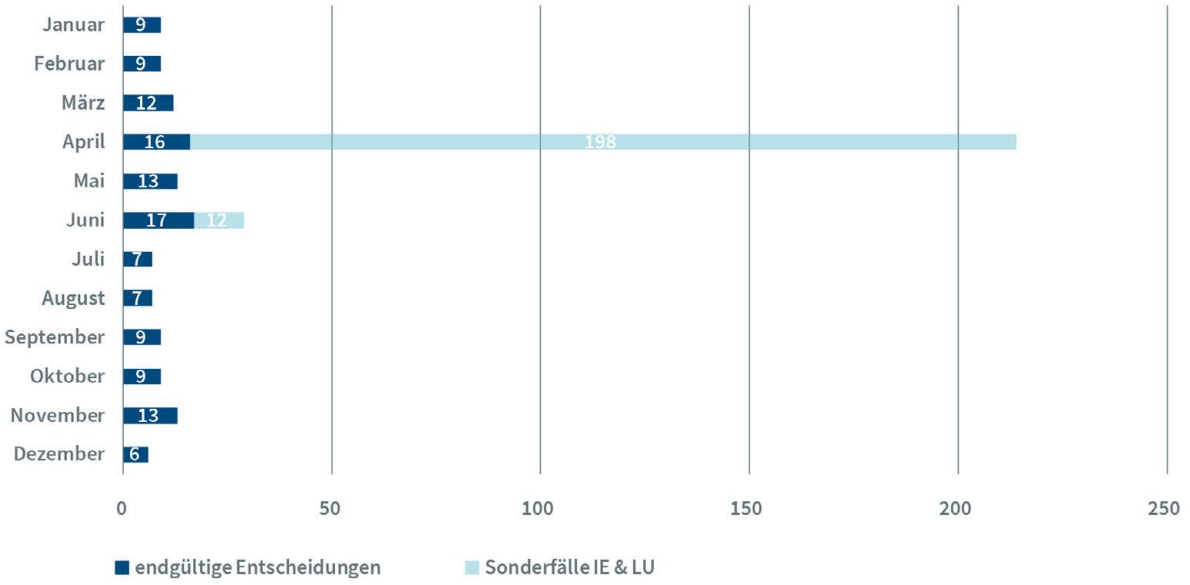
Der Abschluss grenzüberschreitender Fälle durch endgültige Entscheidungen nach Art. 60 DSGVO konnte im Jahr 2021 deutlich gesteigert werden (2018: 2, 2019: 77, 2020: 89, 2021: 139[24]). Diese Form des Verfahrensabschlusses ist der in der DSGVO am detailliertesten geregelte und zugleich derjenige, an dem die Öffentlichkeit das stärkste Interesse hat. Diese Entscheidungen haben zuvor das Kooperationsverfahren durchlaufen, das der europaweiten Vereinheitlichung der Rechtsanwendung dient. Dies, indem sich die europaweit federführenden sowie die jeweils betroffenen Aufsichtsbehörden untereinander austauschen und abstimmen. So getroffene Entscheidungen sind keine Einzelauffassungen, sondern Ergebnis des Zusammenwirkens der beteiligten Aufsichtsbehörden. Wenn dort Aussagen zur datenschutzrechtlichen Bewertung von Verarbeitungen getroffen werden, ist dies von besonderem Gewicht. Die so getroffenen Entscheidungen werden auf dem Internetauftritt des EDSA veröffentlicht.[25]

Nachfolgend eine Auswertung der Entscheidungen in grenzüberschreitenden Fällen, die von den Aufsichtsbehörden im Jahr 2021 als endgültige Entscheidungen nach Art. 60 DSGVO vorgelegt wurden:

24 Bei der Ermittlung der Gesamtzahl der endgültigen Entscheidungen des Jahres 2021 für diesen Tätigkeitsbericht wurden 198 Verfahrensabschlüsse, die die irische Aufsichtsbehörde durch gütliche Einigung erzielt hat, nicht mit einbezogen.

25 https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_de

Endgültige Entscheidungen nach Art. 60 DSGVO im Jahr 2021



Wie die monatsweise Betrachtung zeigt, war in den Monaten April und Juni ein deutlicher Anstieg der endgültigen Entscheidungen zu verzeichnen.

Der Anstieg im April ist darauf zurückzuführen, dass die irische Aufsichtsbehörde auf einen Schlag 198 Verfahrensabschlüsse vorgelegt hatte. Rechtlich handelt es sich bei diesen Verfahrensabschlüssen allerdings nicht um endgültige Entscheidungen nach Art. 60 DSGVO, sondern um gütliche Einigungen (englisch „amicable settlements“) zwischen Beschwerdeführenden und Verantwortlichen, ohne dass es zu einer behördlichen Sachentscheidung kam. Hierin inbegriffen sind Fälle, bei denen die Verantwortlichen Zugeständnisse machten, die Beschwerdeführenden sich im weiteren Verfahren aber nicht mehr zurückgemeldet haben. Bei der Ermittlung der Gesamtzahl der endgültigen Entscheidungen des Jahres 2021 für diesen Tätigkeitsbericht wurden die 198 Verfahrensabschlüsse, die die irische Aufsichtsbehörde durch gütliche Einigung erzielt hat, nicht mit einbezogen.

Der Anstieg im Juni liegt darin begründet, dass sich die Aufsichtsbehörden zuvor darauf verständigt hatten, auch in einfach gelagerten grenzüberschreitenden Fällen, bei denen kein Datenschutzverstoß festgestellt wurde, eine Entscheidung vorzulegen. In Umsetzung dessen hat Luxemburg zu einer Reihe bereits abgeschlossener Verfahren nochmals deklaratorisch verfahrensabschließende Entscheidungen verfasst.

Deutschland war sehr aktiv bei der Bearbeitung grenzüberschreitender Fälle und konnte hier im Jahr 2021 zusammen mit Frankreich den Spitzenplatz einnehmen: Bei Betrachtung der endgültigen Entscheidungen nach Art. 60 DSGVO stammen 22 von 139 Entscheidungen aus Deutschland. Dabei wurden die gütlichen Einigungen der irischen Aufsichtsbehörde außer Acht gelassen. Aus Frankreich stammen ebenfalls 22 Entscheidungen. Auf den weiteren Plätzen folgen Luxemburg mit 13 und Schweden mit 12 Entscheidungen.

Zusammenarbeit zwischen Gemeinsamen Vertreter und ZASt mit dem neu gewählten Stellvertreter

Mehr als drei Jahre nach Inkrafttreten der Vorschrift im Bundesdatenschutzgesetz (BDSG) hat der Bundesrat am 25. Juni 2021 den Bayerischen Landesbeauftragten für den Datenschutz – Herrn Prof. Dr. Petri – zu meinem Stellvertreter im EDSA gewählt. Der Stellvertreter hat u. a. die Aufgabe, zusammen mit mir möglichst im Einvernehmen gemeinsame Standpunkte für die Verhandlungsführung im EDSA vorzuschlagen. Darüber hinaus vertritt er mit mir zusammen die Positionen der deutschen Aufsichtsbehörden im Plenum. Zudem wird dem Stellvertreter in bestimmten Länderangelegenheiten das Stimmrecht im EDSA übertragen. Nach der Wahl wurden mit dem Stellvertreter organisatorische Maßnahmen vereinbart, die eine effiziente Zusammenarbeit zwischen BfDI als gemeinsamen Vertreter, den Aufsichtsbehörden der Länder und der beim BfDI angesiedelten ZASt sicherstellen.

Optimierung des Abstimmungsprozesses für die Herstellung gemeinsamer Standpunkte im Kontext schriftlicher Verfahren

Zur Vorbereitung des Abstimmungsverhaltens im EDSA ist es bei schriftlichen Verfahren Aufgabe der ZASt, die Herstellung eines gemeinsamen Standpunktes zwischen den Aufsichtsbehörden des Bundes und der Länder nach § 18 BDSG zu koordinieren. Schriftliche Verfahren des EDSA kommen seit Beginn der Pandemie besonders häufig vor (2018: 6, 2019: 4, 2020: 47, 2021: 52) und Abstimmungen erfolgen über das Europäische Binnenmarktinformationssystem IMI. Parallel führt die ZASt die nationale Abstimmung über den gemeinsamen Standpunkt durch, was bislang außerhalb vom IMI per E-Mail erfolgte. Um diesen in Europa einzigartigen internen Abstimmungsprozess zu optimieren, wurde auf Anregung der ZASt im Jahr 2020 begonnen, ein neues Modul im IMI zu konzipieren (vgl. 29. TB Nr. 11.2). Dieses Modul wurde auf die Bedürfnisse der deutschen Aufsichtsbehörden zugeschnitten. Nach einem Test des neuen IMI-Moduls mit den Aufsichtsbehörden des Bundes und der Länder konnte die Umstellung auf den neuen optimierten Abstimmungsprozess Mitte 2021 abgeschlossen werden. Dies erleichtert die Stimmabgabe und -auswertung, die jetzt nicht mehr per E-Mail erfolgt, sondern medienbruchfrei, arbeitseffizient und sicher direkt im IMI.

Querverweise:

3.2.6 Leitlinien für Streitbeilegungsverfahren vor dem EDSA

11 Wo bleibt das Positive?

In den Beiträgen der vorherigen Kapitel muss es naturgemäß oft leider vor allem um die kritische Begleitung von Gesetzgebung, die ungenügende Umsetzung von Datenschutzvorschriften oder das Auffinden von Fehlern bei Kontrollen gehen. Auch in diesen Beiträgen zeige ich allerdings stets auf, dass im Rahmen der Beratungen und Kontrollen vieles zum Besseren gelöst wird.

Um aber noch deutlicher zu machen, wie das Zusammenwirken zwischen Aufsicht und beaufsichtigter Behörde zu richtig positiven Ergebnissen führen kann, weil gut zusammengearbeitet wurde, führen wir auch dafür einige zusätzliche Beispiele an. Unser Ziel: Gerne mehr davon.

11.1 Erfolgreiche Zusammenarbeit mit BMU

Viele ambitionierte Gesetzgebungsverfahren des vergangenen Jahres entsprachen leider nicht immer den Vorgaben der Gemeinsamen Geschäftsordnung der Bundesministerien – insbesondere wegen zu enger Zeitpläne. Das BMU zeigt: Es geht auch anders!

Hervorheben möchte ich das erfreuliche Beispiel für die erfolgreiche Kooperation zwischen dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU) und mir. Im Rahmen der Beratungen in dem Gesetzgebungsverfahren der Dritten Verordnung zur Änderung der Strahlenschutzverordnung, in der es unter anderem um die Übertragung messungsbezogener Daten ging, erfolgte meine Beteiligung frühzeitig und unter Einhaltung angemessener Fristen.

Dank meiner frühzeitigen Einbindung waren konstruktive Beratungen möglich. Meine datenschutzrechtlichen Anregungen, insbesondere zur Präzisierung und Datenminimierung, wurden aufgegriffen und die besprochenen Änderungswünsche im weiteren Gesetzgebungsverfahren vereinbarungsgemäß umgesetzt.

So ist es gemeinsam mit dem BMU gelungen, eine datenschutzfreundliche Ausgestaltung der Regelung auf den Weg zu bringen.

Ich wünsche mir weiterhin eine solch vertrauensvolle und erfolgreiche Zusammenarbeit – ausdrücklich auch mit anderen Bundesministerien und Bundesbehörden!

11.2 Datenschutzfreundliche Katastrophenwarnung

Seit der Flutkatastrophe im Jahr 2021 ist geplant, auf eine bereits in anderen Ländern bewährte Technik für die Alarmierung der Bevölkerung zurückzugreifen.

Sirenen oder UKW- bzw. DAB-Radios sind sehr datenschutzfreundliche Medien für die Alarmierung der Bevölkerung. Hier werden keine Daten der Empfangenden verarbeitet, da die Nachricht ohne Rückkanal versendet wird. Anders sieht es bei Warn-Apps aus, bei denen beim Anbieter, Betriebssystemhersteller und ggf. bei Dienstleistern Datenspuren entstehen können. Diese Apps sind außerdem nicht optimal zur Alarmierung geeignet, insbesondere da nur ein begrenzter Teil der Bevölkerung diese installiert oder installieren kann. Dennoch setzte die Bundesregierung auf diese Apps, die auch die Anforderungen von Artikel 110 der Richtlinie über den europäischen Kodex für die elektronische Kommunikation erfüllen sollten. Hierin ist geregelt, dass die Mitgliedsstaaten bis zum 21. Juni 2022 ein technisches Warnsystem etablieren sollen, mit dem Mobilfunknutzende öffentliche Warnungen leicht(er) empfangen können.

Nach den Flutkatastrophen in Nordrhein-Westfalen und Rheinland-Pfalz im Juli 2021 will man nun auf eine bereits in anderen Ländern bewährte Technik für die Alarmierung der Bevölkerung zurückgreifen. Noch bevor das überarbeitete Telekommunikationsgesetz (TKG) in Kraft trat, wurde der § 164 a TKG eingefügt, der die Einführung von öffentlichen Warnungen über Cell-Broadcast regelt. Wie bei Sirenen und Radios ist kein

Rückkanal erforderlich und somit fallen keine Daten der Empfangenden an. Durch das neue System wird es blitzschnell möglich sein, Warnungen an empfangsbereite Mobilfunkendgeräte, die sich in dem von der auslösenden Behörde bestimmten geographischen Gebiet befinden, auszusenden. Auch wenn der ursprüngliche Anstoß für die Einführung der Warnungen über Cell-Broadcast nichts mit dem Datenschutz zu tun hatte, begrüße ich die Einführung dieser datenschutzfreundlichen Technologie ausdrücklich.

Querverweise:

5.1 Telekommunikationsgesetzgebung TKG/TTDSG

11.3 Deaktivierung von Zugängen in der Abordnung

Bei der Zollfahndung konnten durch die gemeinsame Aufarbeitung einer Datenschutzverletzungsmeldung Verbesserungen im Umgang mit Zugangsrechten zu polizeilichen Datenbanken erreicht werden.

Die Zollfahndung meldete mir den unberechtigten Abruf personenbezogener Daten über eine dienstliche Nutzerkennung als Datenschutzverstoß. Hintergrund war, dass eine beschäftigte Person kurzzeitig zu einer externen Behörde abgeordnet war und ihren bestehenden Zugang zum automatisierten Abruf aus einem amtlichen Verzeichnis weisungswidrig zur dortigen Aufgabenerfüllung genutzt hat. Bei der Aufarbeitung dieses Sachverhaltes habe ich u. a. geprüft, ob die Zollfahndung ausreichende technische und organisatorische Maßnahmen ergriffen hatte, um unbefugte Abrufe aus ihren Datenbanken zu verhindern.

Im Rahmen der gemeinsamen Aufarbeitung wurden Meldewege und Geschäftsprozesse etabliert, um sämtliche Zugänge zu polizeilich genutzten Datenbanken für die Dauer einer längerfristigen Abordnung an eine externe Stelle technisch zu deaktivieren. Sofern diese eingehalten werden, sollten sich gleichartige Datenschutzverletzungen nicht wiederholen.

11.4 Öffentlichkeit herstellen, Transparenz schaffen, Datenschutz fördern!

Datenschutz schließt die Sensibilisierung der Öffentlichkeit, Schaffung der Transparenz und Förderung des fachlichen Diskurses ein. Unsicherheiten im Umgang mit personenbezogenen Daten oder Schwierigkeiten bei der Beurteilung datenschutzrechtlicher Fragen lassen sich vermeiden, indem man darüber diskutiert und im Gespräch bleibt.

Im Berichtszeitraum ist es mir im Wege einer **fachlichen Offensive** gelungen, einige wichtige datenschutzrechtliche Fragestellungen aus ihrem Schattendasein heraus- und einer breiten öffentlichen Debatte zuzuführen.

- Mit der Veröffentlichung meines **Positionspapiers zum Grundsatz der Zweckbindung** in polizeilichen Informationssystemen habe ich meinen Standpunkt betreffend die Umsetzung dieses zentralen datenschutzrechtlichen Grundsatzes in polizeilichen Informationssystemen auch im Interesse der Transparenz meiner Aufsichtstätigkeit kundgetan. In der Polizeipraxis ist die Einhaltung der Zweckbindung leider keine Selbstverständlichkeit (vgl. z. B. u. Nr. 8.2.2; 28. TB Nr. 6.7.3). Das Positionspapier enthält Ausführungen insbesondere zu Erforderlichkeit der Zweckfestlegung bzw. -trennung, Vergabe von Zugriffsrechten, Recherchemöglichkeiten und Kennzeichnungs- und Protokollierungspflichten in polizeilichen Informationssystemen.
- Im Oktober habe ich ein **Symposium** zum Thema „Polizeiliche Informationssysteme im Zeitalter von KI und Big Data – Notwendig für polizeiliche Aufgaben oder multifunktionaler Datenspeicher auf Vorrat?“ durchgeführt. Hochkarätige Vertreterinnen und Vertreter aus Wissenschaft, Politik, Datenschutzaufsicht und Polizeipraxis diskutierten über die aktuellen datenschutzrechtlichen Herausforderungen bei der Ausgestaltung polizeilicher Informationssysteme. Es handelte sich um eine öffentliche Veranstaltung im Hybrid-Format, an der 350 Personen virtuell teilgenommen haben. In der Quintessenz dieser Veranstaltung wurde erneut deutlich, dass die unterschiedlichen Standpunkte bisweilen gar nicht so weit voneinander entfernt sind, wie es zunächst scheint. Aus meiner Sicht sind weitere Diskussionen notwendig, um polizeifachliche Belange mit den Interessen der Zivilgesellschaft und der Datenschutzaufsicht auf einem soliden rechtsdogmatischen Fundament miteinander zu vereinen.

Die Videoaufzeichnung der Veranstaltung ist auf meiner Website verfügbar (www.bfdi.bund.de/mediathek). Jeder hatte die Möglichkeit, Fragen an die Diskutanten zu stellen. Von dieser Möglichkeit haben viele Bürgerinnen und Bürger Gebrauch gemacht.

→ Schließlich habe ich mit dem Konsultationsverfahren zur Künstlichen Intelligenz (KI) im Bereich der Strafverfolgung und Gefahrenabwehr sieben Thesen zur öffentlichen Diskussion gestellt. Alle waren dazu eingeladen, sich mit ihren Kommentaren und Stellungnahmen an der Konsultation zu beteiligen (vgl. u. Nr. 4.2.2). Die eingegangenen Stellungnahmen helfen dabei, die verfassungsrechtlichen Vorgaben für den Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr zu konkretisieren und eine Positionierung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) auch in internationalen Gremien zu erleichtern. Eine Positionierung kann auch angesichts der aktuellen Vorstöße der EU-Kommission in Sachen KI (vgl. u. Nr. 4.2.) nicht früh genug erarbeitet werden.

Querverweise:

4.2 Künstliche Intelligenz – Regulierung als gesamtgesellschaftliche Aufgabe, 8.2.2 Vorgangsbearbeitungssystem des Bundeskriminalamts

Themenzuordnung nach Bundestagsausschüssen

Ausschuss für Arbeit und Soziales

- 3.1.4.4 Verarbeitung des Datums „Impfstatus“ von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber
- 3.2.5.1 Auskunftsanspruch bei den Sozialleistungsträgern
- 4.3 Interdisziplinärer Beirat Beschäftigtendatenschutz
- 7.5 Transparenz im Gesetzgebungsverfahren
- 8.2.1 Fragebogenkontrolle Datenschutzbeauftragte in Jobcentern

Auswärtiger Ausschuss

- 3.3 Global Privacy Assembly
- 3.3.2 Reference Panel

Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

- 7.5 Transparenz im Gesetzgebungsverfahren

Ausschuss Digitales

- 3.1.4.3 Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail
- 3.1.3 AK Microsoft
- 3.2.2.1 Taskforce Supplementary Measures / Umsetzung Schrems II
- 3.2.2.2 Schwerpunkt Drittlandübermittlung
- 3.3 Global Privacy Assembly
- 3.3.2 Reference Panel
- 3.4.2 Berlin Group
- 4.1.1 Corona-Warn-App
- 4.1.2 SORMAS
- 4.1.3 Digitales COVID-Zertifikat der EU
- 4.2 Künstliche Intelligenz – Regulierung als gesamtgesellschaftliche Aufgabe
- 5.1 Telekommunikationsgesetzgebung TKG/TTDSG
- 5.3 Open-Data-Gesetz
- 5.3.1 Open-Data-Strategie der Bundesregierung
- 5.9 EU Digitalgesetzgebung
- 6.2 Datenstrategie der Bundesregierung
- 6.9 Erstattungsfähige Digitale Gesundheitsanwendungen
- 6.10 Digitalisierung öffentliche Verwaltung
- 6.11 Brexit – Datentransfer mit dem Vereinigten Königreich
- 6.18 Anwendungen auf elektronischer Gesundheitskarte
- 6.26 Personalverwaltungssystem PVSplus: Noch nicht gelöste datenschutzrechtliche Herausforderungen
- 7.5 Transparenz im Gesetzgebungsverfahren

Ausschuss für Ernährung und Landwirtschaft

- 7.5 Transparenz im Gesetzgebungsverfahren

Ausschuss für die Angelegenheiten der Europäischen Union

- 3.2.2.1 Taskforce Supplementary Measures / Umsetzung Schrems II
- 3.2.2.2 Schwerpunkt Drittlandübermittlung
- 6.22 Eurojust, Europäische Staatsanwaltschaft: Neue Zuständigkeiten des BfDI9 EU Digitalgesetzgebung
- 7.5 Transparenz im Gesetzgebungsverfahren

Ausschuss für Familie, Senioren, Frauen und Jugend

7.5 Transparenz im Gesetzgebungsverfahren

Finanzausschuss

7.5 Transparenz im Gesetzgebungsverfahren

8.1.3 VIS

8.1.4 Kontrolle der getätigten Abfragen im Zollfahndungsinformationssystem INZOL

8.2.9 Kontrolle und Beratung bei der Financial Intelligence Unit (FIU)

Ausschuss für Gesundheit

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

3.1.4.1 Coronavirus: Es ist notwendig, Nachweise über Impfungen, Testergebnisse und Genesungen gesetzlich zu regeln

3.2.5.2 Auskunftserteilung nach Art. 15 durch Krankenkassen

4.1.1 Corona-Warn-App

4.1.2 SORMAS

4.1.3 Digitales COVID-Zertifikat der EU

4.1.4 Coronamelde-Verordnung

4.1.5 Die Bundesnotbremse und die Ausnahmeverordnung

4.1.6 Coronavirus-Testverordnung

4.1.7 Das „EpiLage-Fortgeltungsgesetz“

4.1.8 Zweites Infektionsschutz-Änderungsgesetz: digitale Nacherfassung der Impfungen und 3G am Arbeitsplatz

4.1.9 Digitales Impfquotenmonitoring

5.10 Entwicklungen bei Gesundheitsregistern

5.11 Datenerhebungsbefugnisse der Krankenkassen im Krankengeldfallmanagement

6.1 Elektronische Patientenakte

6.4 Neustart des Forschungsdatenzentrums beim BfArM

6.5 Nutzung der Krankenversichertennummer in der Telematikinfrastruktur

6.6 Modellvorhaben Genomsequenzierung

6.7 Pränataltests in Hongkong

6.8 Umsetzung des Diagnose-Korrektur-Anspruch § 305 SGB V

6.9 Erstattungsfähige Digitale Gesundheitsanwendungen

6.18 Anwendungen auf elektronischer Gesundheitskarte

7.5 Transparenz im Gesetzgebungsverfahren

Haushaltsausschuss

9.1 Organisationsuntersuchung

9.2 Personalentwicklung im Jahr 2021

Ausschuss für Inneres und Heimat

3.1.3 Arbeitskreis Microsoft

5.4 Änderungen am Ausländerzentralregistergesetz

5.5 Bundespolizeigesetz

5.6 Änderungen am BND-Gesetz treten in Kraft

5.7 Evaluierung des BDSG

5.8 IT-Sicherheitsgesetz

6.2 Datenstrategie der Bundesregierung

6.10 Digitalisierung der öffentlichen Verwaltung

6.12 Outing von Asylbewerbern

6.13 Handydatenauswertung durch Bundesamt für Migration und Flüchtlinge rechtswidrig?

6.14 P 20 – Polizei 20/20: Der Weg zu einem gemeinsamen Datenhaus

6.15 GETZ: Unzureichende Evaluation

6.16 Datenverarbeitung beim BND

6.20 Das Sicherheitsüberprüfungsgesetz – Ein Gesetz mit vielen Fragezeichen

6.22 Pilotprojekt zur „intelligenten“ Videoüberwachung am Bahnhof Berlin Südkreuz, 2. Teil

6.23 Zusammenarbeit mit anderen Kontrollorganen im Bereich der Nachrichtendienste des Bundes

6.24 Passenger Name Records (PNR) – Zentrale Fragen sind weiterhin ungeklärt

6.26 Personalverwaltungssystem PVSplus: Noch nicht gelöste datenschutzrechtliche Herausforderungen

7.3 Open Government Partnership

7.5 Transparenz im Gesetzgebungsverfahren

8.1.1 Kontrollen und Beanstandungen bei Anti-Terror-Datei (ATD) und Rechtsextremismus-Datei (RED)

8.1.2 Eurodac

8.1.3 VIS

8.1.5 Schengener Informationssystem

8.2.1 Fragebogenkontrolle Datenschutzbeauftragte in Jobcentern

8.2.2. Vorgangsbearbeitungssystem des Bundeskriminalamts

8.2.3 Erste Anordnung gegenüber dem BKA

8.2.4 Funkzellendatenbank des Bundeskriminalamts

8.2.5 Verarbeitung erkennungsdienstlicher Daten durch das Bundeskriminalamt in INPOL-Z

8.2.6 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst (BAMAD)

8.2.7 Datenschutzaufsicht und Beratung beim Bundesamt für Verfassungsschutz (BfV)

8.2.8 Kontrollen zum Sicherheitsüberprüfungsgesetz

11.4 Öffentlichkeit herstellen, Transparenz schaffen, Datenschutz fördern!

Ausschuss für Klimaschutz und Energie

7.5 Transparenz im Gesetzgebungsverfahren

Ausschuss für Kultur und Medien

6.17 Überführung der Stasi-Akten ins Bundesarchiv

7.5 Transparenz im Gesetzgebungsverfahren

Ausschuss für Menschenrechte und humanitäre Hilfe

6.12 Outing von Asylbewerbern

Rechtsausschuss

3.1.2 Positivdaten Auskunfteien

3.1.4.3 Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail

3.2.2.1 Taskforce Supplementary Measures / Umsetzung Schrems II

3.2.2.2 Schwerpunkt Drittlandübermittlung

3.2.5 Leitlinien Recht auf Auskunft Art. 15 DSGVO

6.13 Handydatenauswertung durch Bundesamt für Migration und Flüchtlinge rechtswidrig?

6.20 Das Sicherheitsüberprüfungsgesetz – Ein Gesetz mit vielen Fragezeichen

6.22 Eurojust, Europäische Staatsanwaltschaft: Neue Zuständigkeiten

6.24 Passenger Name Records (PNR) – Zentrale Fragen sind weiterhin ungeklärt

7.5 Transparenz im Gesetzgebungsverfahren

Sportausschuss

7.5 Transparenz im Gesetzgebungsverfahren

Ausschuss für Tourismus

7.5 Transparenz im Gesetzgebungsverfahren

Ausschuss für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

3.1.2 Positivdaten Auskunfteien

7.5 Transparenz im Gesetzgebungsverfahren

7.9.2 UIG oder IFG? Eine manchmal nicht einfache Abgrenzungsfrage

11.1 Erfolgreiche Zusammenarbeit mit BMU

Verkehrsausschuss

7.5 Transparenz im Gesetzgebungsverfahren

7.6 Beanstandung des BMVI wegen der Verweigerung des Informationszugangs ohne Grund

Verteidigungsausschuss

7.5 Transparenz im Gesetzgebungsverfahren

8.1.1 Kontrollen und Beanstandungen bei Anti-Terror-Datei (ATD) und Rechtsextremismus-Datei (RED)

8.2.6 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst (BAMAD)

Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung

5.2 Lobbyregistergesetz

Wirtschaftsausschuss

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

3.1.3 Arbeitskreis Microsoft

3.1.2 Positivdaten Auskunfteien

3.2.2.2 Schwerpunkt Drittlandübermittlung

3.4.2 Berlin Group

5.1 Telekommunikationsgesetzgebung TKG/TTDSG

5.9 EU Digitalgesetzgebung

6.3 Kooperation zwischen Kartell- und Datenschutzaufsichtsbehörden

6.11 Brexit – Datentransfer mit dem Vereinigten Königreich

6.20 Das Sicherheitsüberprüfungsgesetz – Ein Gesetz mit vielen Fragezeichen

7.5 Transparenz im Gesetzgebungsverfahren

8.2.10 Kontrolle nicht lizenzierter Postdienstleister

8.2.11 Fragebogenkontrolle Betroffenenrechte

11.2 Datenschutzfreundliche Katastrophenwarnung

Ausschuss für Wirtschaftliche Zusammenarbeit und Entwicklung

7.5 Transparenz im Gesetzgebungsverfahren

Ausschuss für Wohnen, Stadtentwicklung, Bauwesen und Kommen

7.5 Transparenz im Gesetzgebungsverfahren

Anlagen

Anlage 1

Kontrollierte und besuchte Stellen

Vier Unternehmen aus den Branchen Gebäudebewachung, Gebäudereinigung, Strom

allgäu mail GmbH

Amazon Deutschland Transport GmbH

Auswärtiges Amt

Betriebszentrum IT-System der Bundeswehr

BS Saar-Mosel GmbH

Bundesagentur für Arbeit

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Bundesamt für den Militärischen Abschirmdienst

Bundesamt für Justiz

Bundesamt für Verfassungsschutz

Bundesamt für Wirtschaft und Ausfuhrkontrolle

Bundesanstalt für Finanzdienstleistungsaufsicht

Bundesanstalt für Immobilienaufgaben

Bundesfamilienkasse beim Bundesverwaltungsamt

Bundeskartellamt

Bundeskriminalamt

Bundesministerium der Verteidigung

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung

Bundesnachrichtendienst

Bundespolizeidirektion Koblenz

Bundespolizeidirektion Sankt Augustin

Bundespolizeipräsidium

BundeswehrFuhrparkService GmbH

BWPOST GmbH

Cuma Gün Kuriertransporte e. K.

Deutsche Post AG

Deutsches Patent- und Markenamt

DHL Paket GmbH

Direktmarketing Kusche GmbH

DPD Deutschland GmbH

dvs – Deutscher Versand Service GmbH

Engagement Global gGmbH

Eurojust

Europol-Kontrolle, Teilnahme an Expertenmission

Familienkasse Baden-Württemberg-Ost

Familienkasse Baden-Württemberg-West

Familienkasse Bayern Nord

Familienkasse Bayern Süd

Familienkasse Berlin-Brandenburg

Familienkasse Hessen

Familienkasse Niedersachsen-Bremen

Familienkasse Nord

Familienkasse Nordrhein-Westfalen Nord

Familienkasse Nordrhein-Westfalen Ost

Familienkasse Nordrhein-Westfalen West

Familienkasse Rheinland-Pfalz Saarland

Familienkasse Sachsen

Familienkasse Sachsen-Anhalt-Thüringen

FedEx Express Germany GmbH

Financial Intelligence Unit

Funke Postservice GmbH, Erfurt

General Logistics Systems Germany GmbH & Co. OHG

Generaldirektion Wasserstraßen und Schifffahrt

Generalsekretariat der Europäischen Schulen in Brüssel

Hanse Jobcenter Rostock

Hermes Germany GmbH

Jobcenter Berlin Friedrichshain-Kreuzberg

Jobcenter Bremen

Jobcenter Dresden

Jobcenter Erfurt

Jobcenter Kaiserslautern Stadt

Jobcenter Kiel

Jobcenter Köln

Jobcenter Landeshauptstadt Potsdam

Jobcenter Landkreis Diepholz

Jobcenter Landkreis Kaiserslautern

Jobcenter Landkreis Karlsruhe

Jobcenter Magdeburg

Jobcenter Mainz

Jobcenter Mannheim

Jobcenter München

Jobcenter Region Hannover

Jobcenter Regionalverband Saarbrücken

Jobcenter Stadt Kassel

Jobcenter team.arbeit.hamburg

Jobcenter Vorpommern-Greifswald Nord

Jobcenter Zollernalbkreis

Lehmensiek Kabelnetze & Antennentechnik GmbH

Niederlande, Teilnahme an Expertenmission zur Schengen-Evaluierung

Ostfriesische Transportgesellschaft Janssen

Parlamentarisches Kontrollgremium

pd.MEDIENLOGISTIK GmbH

Physikalisch-Technische Bundesanstalt

PIN AG

Postcon NRW GmbH

T-Systems Rechenzentrum Biere in Bördelund

United Parcel Service Deutschland S. à r. l. & Co. OHG

Vodafone GmbH

Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Zollkriminalamt

Diese Liste enthält auch schriftliche Kontrollen. Manche der aufgeführten Stellen wurden mehrfach kontrolliert.

Bei den in dieser Liste genannten Stellen wurde während des Berichtszeitraums ein Kontroll- oder Beratungsgespräch vor Ort, virtuell oder in schriftlicher Form begonnen. Dies bedeutet jedoch nicht, dass alle Gesamtverfahren ebenfalls im Berichtszeitraum abgeschlossen werden konnten. Insbesondere liegt noch nicht für sämtliche Verfahren ein Abschlussbericht vor. Diese veröffentlicht der BfDI im Rahmen der rechtlichen Möglichkeiten zeitnah nach der Fertigstellung auf seiner Website unter: www.bfdi.bund.de/kontrollberichte

Anlage 2

Übersicht über Maßnahmen/Beanstandungen gegenüber öffentlichen Stellen

Stelle	Maßnahme/Beanstandung	Grund
BARMER GEK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Artikel 5 Abs. 1 lit. a) und f) und Art. 32 Abs. 1 lit. b) wegen unerlaubter Übermittlung und Verarbeitung von Sozialdaten. Ebenfalls Verstoß gegen Artikel 33 DSGVO wegen nicht fristgerechter Meldung des Verstoßes nach Bekanntwerden.
BARMER GEK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO i.V.m. § 35 Abs. 1 SGB I indem die Gesundheitsdaten einer Versicherten entgegen der gebotenen Sorgfalt an ein Sanitätshaus zur Beschaffung von Pflegehilfsmitteln weitergegeben wurden, ohne dass hierfür eine wirksame Rechtsgrundlage vorlag.
BARMER GEK	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der elektronischen Patientenakte (ePA) bis zum 31.12.2021 so auszugestalten, dass Versicherte eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 SGB V in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen („feingranulares Zugriffsmanagement“) können.
BARMER GEK	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der ePA binnen eines Jahres so auszugestalten, dass auch Frontend-Nichtnutzer auch ohne die Bestellung eines Vertreters in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.
BIG direkt Gesund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 i. V. m. Art. 9 Abs. 2 DSGVO indem fahrlässig und nicht datenschutzkonform im Rahmen des Krankengeldfallmanagements bei einer Versicherten besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet wurden ohne ihre vorherige schriftliche Einwilligung nach § 44 Abs. 4 SGB V einzuholen.
BKK ProVita	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO i.V.m. § 35 Abs. 1 SGB I indem von der Versicherten ohne Rechtsgrundlage aktuelle Facharztbefunde (Gesundheitsdaten) zur Prüfung des Krankgeldbezuges angefordert wurden.
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 DSGVO wegen zunächst rechtswidriger Ablehnung und nicht fristgerechter vollständiger Erteilung einer Auskunft nach Art. 15 DSGVO unter Missachtung der gebotenen Sorgfalt
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO und Anweisung gem. Art. 58 Abs. 2 lit. d) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. c) DSGVO wegen des Abdrucks der vollständigen Bankverbindung auf Beihilfebescheiden ohne entsprechende Erforderlichkeit, Anweisung zur Anonymisierung oder Wegfall der Bankverbindung auf den Beihilfebescheiden

Stelle	Maßnahme/Beanstandung	Grund
Bundesagentur für Arbeit	Verwarnungen gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) und Art. 6 Abs. 1 DSGVO wegen der Übermittlung personenbezogener Daten ohne Rechtsgrundlage und Verstoß gegen Art. 5 lit. d) DSGVO wegen der sorgfaltswidrigen Missachtung der Richtigkeit der gespeicherten personenbezogenen Daten
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 DSGVO wegen der Negativauskunft zur Verarbeitung von Sozialdaten, obwohl personenbezogene Daten verarbeitet werden
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 lit. a) DSGVO wegen der sorgfaltswidrigen Kontakaufnahme des ärztlichen Dienstes zum behandelnden Arzt ohne vorherige Schweigepflichtentbindung
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) DSGVO wegen der Verwendung einer E- Mail-Adresse zur Kontaktaufnahme obschon die Löschung ebendieser Mailadresse bereits bestätigt war
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 5 lit. a) und Art. 6 Abs. 1 lit. c) DSGVO wegen der Übermittlung einer Telefonnummer und Mailadresse an einen Maßnahmeträger ohne Rechtsgrundlage
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art 32 Abs. 1 DSGVO wegen des Versäumnisses, personenbezogene Daten gegen unberechtigte Zugriffe zu schützen
Bundesagentur für Arbeit	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 12 Abs. 3 DSGVO wegen nicht fristgerecht erteilter Auskunft
Bundesagentur für Arbeit/ Agentur für Arbeit Leipzig	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a), Art. 6 Abs. 1 lit. a) bzw. Art. 5 Abs. 1 lit. a), Art. 6 Abs. 1 lit. b) bis f) DSGVO wegen der Speicherung von Personaldaten auf der Teamablage ohne Rechtsgrund und damit der unrechtmäßigen Verarbeitung von Personaldaten
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 BDSG	Verstoß gegen § 18 Abs. 1 SÜG wegen unzureichende Dokumentation von Bearbeitungs- und Verfahrensschritten und Verstoß gegen § 19 Abs. 2 SÜG wegen Missachtung von Vernichtungs- und Löschfristen
Bundesamt für das Personalmanagement der Bundeswehr	Verwarnungen gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f), Art. 12 Abs. 3 i.V.m. Art. 15 und Art. 32 Abs. 1 lit. b) DSGVO wegen nicht fristgerechter Beauskunftung und Versand der beantragten Auskunft per einfacher, unverschlüsselter Mail an eine nicht verifizierte Mail-Adresse
Bundesamt für Migration und Flüchtlinge	Verwarnung gemäß Art. 58 Abs. 2 lit b DSGVO	Verstoß gegen Art. 32 Abs. 1 DSGVO wegen nicht ausreichender technisch-organisatorischer Maßnahmen im Zusammenhang mit dem Fehlversand einer E-Mail
Bundesamt für Verfassungsschutz	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 2 ATDG wegen nicht durchgeführter Löschung
Bundesamt für Verfassungsschutz	Drei Beanstandungen gemäß § 16 Abs. 2 BDSG	Drei Verstöße gegen § 11 Abs. 2 ATDG wegen Verlust der Datenhistorie und unverhältnismäßiger Erschwernis der Datenschutzkontrolle
Bundesamt für Verfassungsschutz	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 3 Abs. 1 Nr. 1 b) aa) RED-G wegen fehlender Rechtsgrundlage für Speicherung erweiterter Grunddaten
Bundesamt für Verfassungsschutz	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 12 Abs. 3 RED-G wegen Verlust der Datenhistorie und unverhältnismäßiger Erschwernis der Datenschutzkontrolle

Stelle	Maßnahme/Beanstandung	Grund
Bundesamt für Wirtschaft und Ausfuhrkontrolle	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 28 Abs. 3 DSGVO wg. Einsatzes eines Auftragsverarbeiters ohne entsprechende Vereinbarung
Bundesanstalt für Immobilienaufgaben	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoßes gegen Art. 34 Abs. 1 DSGVO wegen Unterlassung der Benachrichtigung über eine Datenschutzverletzung
Bundesanstalt für Post und Telekommunikation	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) i.V.m. Art. 32 Abs. 1 DSGVO wegen nicht ordnungsgemäßem Versand von Unterlagen zur Überprüfung einer Dienstunfähigkeit und der damit einhergegangenen Sichtbarkeit des Betreffs im Sichtfenster des Briefumschlages
Bundesanstalt für Post und Telekommunikation	Verwarnungen gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f), Art. 32 Abs. 1 lit. b) sowie Art. 12 Abs. 3 i.V.m. Art. 15 DSGVO wegen des Versandes sensibler personenbezogener Daten per unverschlüsselter Mail und verfristete Erteilung des Auskunftsersuchens
Bundesanstalt Technisches Hilfswerk	Verbot gemäß Art. 58 Abs. 2 lit. f), Löschung gem. Art. 58 Abs. 2 lit. g) i.V.m. Art. 17 Abs. 1 lit. d), Verwarnung gem. Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) DSGVO wegen Verarbeitung besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO in Form des Impfstatus in Bezug auf eine Corona-Impfung ohne rechtliche Grundlage
Bundesanstalt Technisches Hilfswerk	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 DSGVO wegen der Verarbeitung personenbezogener Daten von Beschäftigten ohne wirksame Rechtsgrundlage durch Vorgesetzte
Bundeskriminalamt	Beanstandung gemäß § 16 Abs. 2 S. 1 BDSG	Verstoß gegen Art. 20 Abs. 1 Eurodac-VO wegen u. a. fehlender vorgeschalteter Abfrage des Visa-Informationssystems (VIS)
Bundeskriminalamt	Warnung gemäß § 16 Abs. 2 Satz 4 BDSG	drohender Verstoß gegen § 91 BKAG wegen Änderung einer Errichtungsanordnung
Bundeskriminalamt	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen Gesetztesvorbehalt wegen Betriebs ein Funkzellendatenbank und Datenabgleich
Bundeskriminalamt	Warnung gemäß § 16 Abs. 4 BDSG	drohender Verstoß gegen beabsichtigte Datenverarbeitung unterhalb der Schwellen der Vorschriften der §§ 29 ff. BKAG zwischen den Polizeibehörden der Länder mit dem BKA als Auftragsverarbeiter
Bundeskriminalamt	Anordnung gemäß § 69 Abs. 2 BKAG	Verstoß gegen §§ 56, 57 BDSG sowie § 483 StPO wegen Verweigerung einer Auskunft und unzulässiger Speicherung einer Person
Bundeskriminalamt	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen das Auskunftsrecht nach § 57 BDSG
Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)	Anweisung gemäß Art. 58 Abs. 2 lit. g) DSGVO	Anordnung, 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
Bundesministerium für Verkehr und digitale Infrastruktur	Beanstandung gemäß § 12 Abs. 3 IFG iVm § 25 Abs. 1 Nr. 1 BDSG (alt)	Verstoß gegen § 3 Nr. 1 lit g IFG wegen Verweigerung des Informationszugangs ohne Grund
Bundesnachrichtendienst	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 8 ATDG wegen Mängeln in der Synchronisierung Quelldatei zur ATD

Stelle	Maßnahme/Beanstandung	Grund
Bundesnachrichtendienst	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 16 Abs.4 BDSG wegen für BfDI nicht nachvollziehbarer Dokumentation
Bundesnachrichtendienst	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 10 Abs. 1 ATDG wegen Verifikation der Kontrollzuständigkeit im Zusammenwirken mit der G10-Kommission
Bundespolizei	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 16 Abs. 4 BDSG wegen fehlender Bereitstellung von Informationen
Bundespolizei	Warnung gemäß § 16 Abs. 2 S. 4 BDSG	Keine Nennung wegen Einstufung
Bundespolizei	Beanstandung gemäß § 16 Abs. 2 BDSG	Keine Nennung wegen Einstufung
Bundespolizeipräsidium	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a), Art. 88 DSGVO i. V. m. § 106 Abs. 4 BBG wegen der Verwendung eines sorgfaltswidrig gestalteten Formulars Vordruck BPOL 4 40 004 01 20 zur Erhebung von Personalausweisnummern von Bewerberinnen und Bewerbern durch niedergelassene Zahnärztinnen und Zahnärzte im Auftrag der Bundespolizei
Bundeswehrdienstleistungszentrum Mayen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) in Verbindung mit Art. 32. Abs. 1 DSGVO wegen fehlender Zugangsbeschränkung zu einem Dienststellenlaufwerk und damit Ermöglichung des Zugang zu den dort gespeicherten personenbezogenen Daten durch einen nicht begrenzten Kreis von Beschäftigten
Bundeszentralamt für Steuern	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 12 Abs. 3 DSGVO wegen der nicht fristgerechten Auskunftserteileung eines Ersuchens nach Art. 15 DSGVO
DAK Gesundheit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Artikel 5 Abs. 1 lit. d) ; Verstoß gegen Art. 16 und 17 DSGVO sowie gegen § 284 Abs. 1 SGB V wegen Speicherung und Verarbeitung falscher Diagnosedaten und der Verweigerung trotz Antrag der Betroffenen diese zu löschen
DAK Gesundheit	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der elektronischen Patientenakte (ePA) bis zum 31.12.2021 so auszugestalten, dass Versicherte eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 SGB V in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen („feingranulares Zugriffsmanagement“) können.
DAK Gesundheit	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der ePA binnen eines Jahres so auszugestalten, dass auch Frontend-Nichtnutzer auch ohne die Bestellung eines Vertreters in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.
Deutsche Rentenversicherung Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO wegen der Anforderung einer Personalakte bei einem früheren Arbeitsgeber ohne wirksame Einwilligung oder andere Rechtsgrundlage unter Missachtung der gebotenen Sorgfalt
Deutsches Patent- und Markenamt	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 BDSG	Verstoß gegen § 22 Abs. 2 Nr. 1 SÜG wegen Missachtung von Löschfristen

Stelle	Maßnahme/Beanstandung	Grund
Deutsches Zentrum für Luft- und Raumfahrt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen gegen Art. 5 Abs. 1 lit. f) i.V.m. Art. 32. Abs. 1 DSGVO wegen der Verletzung der gebotenen Sicherheit und Integrität durch den Versand personenbezogener Daten im dienstlichen Kontext mittels eines Computerfaxes über einen privaten Account
Eisenbahnbundesamt	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen gegen Art. 6 Abs. 1 Satz 1 lit. e), 9 Abs. 2 lit. b), g) DSGVO i.V.m. § 26 Abs. 3 BDSG wegen eines nicht datenschutzkonform gestalteten Meldeweges zu Corona-Infektionen von Beschäftigten
Familienkasse Sachsen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 12 Abs. 3 DSGVO aufgrund mangelhafter Auskunftserteilung
Financial Intelligence Unit (FIU)	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen gegen § 71 Abs. 1 BDSG wegen Betrieb eines Systems, das nicht über technische Vorkehrungen verfügt, Löschvorgaben umzusetzen
Financial Intelligence Unit (FIU)	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen § 71 Abs. 1 BDSG wegen Betrieb eines Systems, das nicht über manuelle Vorkehrungen zur Umsetzung der Löschvorgaben verfügt
Financial Intelligence Unit (FIU)	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen §§ 37 Abs. 2, Abs. 4, 39 Abs. 2 Satz 1 Nr. 8 GwG wegen fehlener Löschung in geprüften Einzelfällen, trotz Vorliegen der Löschvoraussetzungen
Financial Intelligence Unit (FIU)	Beanstandung gemäß § 16 Abs. 2 BDSG	Verstoß gegen die Pflicht zur ordnungsgemäßen Aktenführung wegen fehlender Dokumentation der Entscheidungen und Begründungen zur Löschung oder weiteren Speicherung personenbezogener Daten
Financial Intelligence Unit (Zoll)	Beanstandungen gemäß § 16 Abs. 2 BDSG	Verstoß gegen Art. 5 Abs. 1 lit. c) VIS-Zugangsbeschluss wegen Durchführung von VIS-Recherchen, obwohl die sie betreffenden Personen kein Schengen-Visum benötigten.
Financial Intelligence Unit (Zoll)	Beanstandungen gemäß § 16 Abs. 2 BDSG	Verstoß gegen Art. 8 Abs. 4 VIS-Zugangsbeschluss wegen der Übermittlung von VIS-Daten an Drittstaaten, ohne dass die Voraussetzungen des VIS-Zugangsbeschlusses erfüllt waren. Außerdem wurden nicht alle nationalen Übermittlungsvoraussetzungen geprüft.
Finanzamt Hannover-Land I	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß wegen einer Fehlüberweisung, verspätete Meldungen an betroffene Person und BfDI
Finanzamt Lübbecke	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 33 Abs. 1 DSGVO wegener einer verspätete Meldung an den BfDI
Finanzamt Stralsund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) i.V.m. Art. 32 Abs. 1 DSGVO wegen ungeeignetem Sichtfensterumschlag mit einsehbaren Daten
Generaldirektion Wasserstraßen und Schiffahrt	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 BDSG	Verstoß gegen § 18 Abs. 1 SÜG wegen unzureichende Dokumentation von Bearbeitungs- und Verfahrensschritten und Verstoß gegen § 19 Abs. 2 SÜG wegen Missachtung von Vernichtungs- und Löschfristen

Stelle	Maßnahme/Beanstandung	Grund
Generalzolldirektion	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 DSGVO durch die Ermöglichung des Zugriffs durch nicht berechtigten Personen Zugriff auf personenbezogene Daten aus Personalauswahlverfahren. Zu den offenbarten personenbezogenen Daten zählten auch besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO.
Generalzolldirektion	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) und Art. 5 Abs. 1 lit. a), 6 Abs. 1 DSGVO wegen der Adressierung eines Amtshilfeersuchens um Zweifel an der Vollständigkeit des dort Beschäftigten zu den im Rahmen seiner Nebentätigkeit erzielten Einkünfte aufzuklären, ohne dass hierfür eine Zustimmungserklärung im Sinne des § 62 Abs. 2 S.2 BeamtVg vorlag.
Hauptzollamt Düsseldorf	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen gegen Art. 88 Abs. 1 DSGVO i. V. m. § 26 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG) sowie Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO wegen der Außerachtlassung der erforderlichen Sorgfalt beim Umgang mit zwei Schreiben an einen Beschäftigten
Hauptzollamt Frankfurt am Main	Anweisung gemäß Art. 58 Abs. 2 lit. c) und Verwarnung gem. Art. 58 Abs. lit. b) DSGVO	Verstoß gegen Art. 12 Abs. 3 DSGVO wegen nicht fristgerecht erteilter Auskunft, Anweisung zur Erteilung einer vollständigen Auskunft nach Art. 15 DSGVO, Verwarnung wegen nicht fristgerechter Beauskunftung
Hauptzollamt Hamburg	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) i.V.m. Art. 32 Abs. 1 DSGVO wegen der Speicherung personenbezogener Daten zur Steuerung des Impfangebotes durch die Bundeswehr auf einem nicht zugangsbeschränkten Lauf und damit die Ermöglichung des Zugriffs durch Unbefugte und mithin zumindest mittelbar auf besondere Kategorien personenbezogener Daten in Form des Impfstatus
Hauptzollamt München	Anweisung gemäß Art. 58 Abs. 2 lit. d) und Verwarnungen gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen gegen Art. 5 lit. a), b) und f) DSGVO wegen der Offenlegung personenbezogener Daten durch eine am Auswahlverfahren beteiligte Person und die Offenlegung gegenüber anderen Hauptzollämtern durch Übermittlung; Anweisung zur Sicherstellung dass im Rahmen der Fachtätigkeit nach SGB II und SGB X dienstlich außerhalb eines Bewerbungsverfahrens oder einer Tätigkeit für die Personalabteilung bekannt gewordene personenbezogene Daten von Beschäftigten oder Bewerberinnen und Bewerbern weder intern durch Mitarbeitende für Zwecke im Rahmen der Begründung eines Beschäftigungsverhältnisses oder nach der Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung im Sinne des § 26 BDSG verarbeitet werden, noch an externe Dritte für Zwecke im Rahmen der Begründung eines Beschäftigungsverhältnisses oder nach der Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung im Sinne des § 26 BDSG übermittelt werden.
Hauptzollamt Osnabrück	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß wegen Offenbarung personenbezogener Daten im Rahmen einer Vollstreckungsmaßnahme gegenüber unbeteiligten Dritten

Stelle	Maßnahme/Beanstandung	Grund
HIL Heeresinstandsetzungs-logistik GmbH	Verwarnungen gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstöße gegen Art. 5 Abs. 1 lit. a), 9 Abs. 1, 32 Abs.1 DSGVO wegen der Verarbeitung von Vorerkrankungen von Beschäftigten ohne Rechtsgrundlage, die Verarbeitung von Informationen zu krankheitsbedingten Abwesenheiten, mithin Informationen zum Gesundheitszustand von Beschäftigten durch eine unzuständige Stelle innerhalb der HIL GmbH, nicht ausreichender Schutz und Ermöglichung des Zugriffs auf die in Rede stehenden Daten durch unbefugte Personen
IKK Classic	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der elektronischen Patientenakte (ePA) bis zum 31.12.2021 so auszugestalten, dass Versicherte eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 SGB V in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen („feingranulares Zugriffsmanagement“) können.
IKK Classic	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der ePA binnen eines Jahres so auszugestalten, dass auch Frontend-Nichtnutzer auch ohne die Bestellung eines Vertreters in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.
Jobcenter im Landkreis Diepholz	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO und Anweisungen gem. Art. 58 Abs. 2 lit. d) DSGVO	Verstoß gegen Art. 38 Abs. 3 Satz 2 DSGVO wegen rechtswirdriger Abberufung des behördlichen Datenschutzbeauftragten
Jobcenter Berchtesgadener Land	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 lit. e) DSGVO wegen der Offenbarung eines Leistungsbezuges durch sorgfaltswidrige Kontaktaufnahme zu einem Stromversorger
Jobcenter Berlin Marzahn-Hellersdorf	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f), Art. 24 Abs. 1 S. 1 und Art. 32 Abs. 1 lit. b) DSGVO wegen der nicht hinreichenden technischen und organisatorischen Maßnahmen gegen interne Zugriffe auf personenbezogene Daten der Beschäftigten in elektronischen Ordnern der Geschäftsführung durch Nichtberechtigte
Jobcenter Berlin Marzahn-Hellersdorf	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 DSGVO wegen des Zugriffs aller impfwilligen Beschäftigten auf die Termine anderer impfwilliger Beschäftigter und somit zumindest die Möglichkeit der mittelbaren Offenbarung des Impfstatus und damit einer besonderen Kategorie personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO
Jobcenter Berlin Spandau	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. d) DSGVO wegen der Übermittlung falscher Sozialdaten an ein Bezirksamt
Jobcenter Berlin Treptow-Köpenick	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 lit. e) DSGVO wegen der sorgfaltswidrigen Anforderung von Unterlagen ohne Hinweis auf Schwärzungsmöglichkeiten
Jobcenter Bremerhaven	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a), Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 1 BDSG wegen der Offenbarung personenbezogener Daten gegenüber dem Personalrat und weiteren nicht beteiligten Personen ohne Rechtsgrundlage

Stelle	Maßnahme/Beanstandung	Grund
Jobcenter Dessau-Roßlau	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 lit a) und f) sowie Art. 6 Abs. 1 S. 1 lit. c) DSGVO wegen der Übermittlung von Daten über ein Mietverhältnis ohne Rechtsgrund an das Finanzamt Dessau-Roßlau und gegen Art. 5 lit. a) und Art. 6 Abs. 1 S. 1 lit. e) 2. Alt. DSGVO wegen der Bitte um Übermittlung von Steuerdaten ohne Rechtsgrund
Jobcenter Deutsche Weinstraße	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO und Anweisung gem. Art. 58 Abs. 2 lit. e) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) i.V.m. Art. 32 Abs. 1 DSGVO wegen der Ermöglichung des Zugangs zum Laufwerk der Personalabteilung für unbefugte Beschäftigte aufgrund fehlender Zugangsbeschränkungen und Anweisung zur Benachrichtigung der von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen aufgrund des hohen Risikos für die persönlichen Recht und Freiheiten gem. Art. 34 DSGVO
Jobcenter Düsseldorf	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen § 35 Abs. 1 SGB I wegen unrechtmäßiger und sorgfaltswidriger Offenbarung personenbezogener Daten
Jobcenter Frankfurt am Main	Verwarnungen gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 17 Abs. 1 lit. b) DSGO wegen der nicht unverzüglichen Entsprechung eines Antrags auf Löschung personenbezogener Daten, Verstoß gegen Art. 5 Abs. 1 lit. a) und Art. 6 Abs. 1 lit. a) DSGVO wegen der Verwendung einer E-Mail-Adresse zur Kommunikation mit einer betroffenen Personen ohne deren Einwilligung und damit in nicht rechtmäßiger Weise, Verstoß gegen Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. a) DSGVO wegen der Verwendung ebendieser Mailadresse zur Kommunikation mit der betroffenen Person ohne dabei die erforderliche angemessene Sicherheit der Verarbeitung, z. B. durch die technische Maßnahme der Verschlüsselung zu gewährleisten.
Jobcenter im Regionalverband Saarbrücken	Verwarnungen gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) und c) DSGVO wegen der sorgfaltswidrigen Erhebung personenbezogener Daten
Jobcenter Kempten	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) und Art. 6 Abs. 1 DSGVO wegen der Übermittlung von personenbezogener Daten an einen Maßnahmeträger ohne Rechtsgrundlage
Jobcenter Kreis Siegen-Wittgenstein	Anweisung gemäß Art. 58 Abs. 2 lit. d) und Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 lit. e) DSGVO wegen der Anforderung ungeschwärzter Kontoauszüge; Anweisung bei künftigen Anforderungen von Kontoauszügen auf die Schwärzungsmöglichkeit hinzuweisen
Jobcenter Landau-Südliche Weinstraße	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) und Art. 6 Abs. 1 DSGVO wegen der Aufforderung zur Einreichung ungeschwärzter Kontoauszüge
Jobcenter Landkreis Harburg	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 lit. e) DSGVO wegen der unrechtmäßigen Anforderung und Speicherung eines Mietvertrages
Jobcenter München	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 lit. e), 5 Abs. 1 lit. a) und c) DSGVO wegen der Übermittlung personenbezogener Daten ohne Einwilligung und ohne Rechtsgrundlage an die Staatsanwaltschaft
Jobcenter München	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 12 Abs. 3 DSGVO wegen nicht fristgerecht erteilter Auskunft
Jobcenter Stadt Kassel	Verwarnung gemäß Art. 58 Abs. 2 lit b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) dSGVO wegen der Datenerhebung bei Dritten unter Missachtung des Ersterhebungsgrundsatzes aus § 67a Abs. 2 S. 1 SGB X und die damit verbundene Offenbarung des Leistungsbezugs gegenüber Dritten

Stelle	Maßnahme/Beanstandung	Grund
Kaufmännische Krankenkasse KKH	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO i. V. m. § 35 Abs. 1 SGB I, Art. 5 Abs. 1 lit. e) i. V. m. Art. 17 Abs. 1 lit. d) DSGVO sowie Art. 33 Abs. 1 DSGVO da im Zeitraum vom 04.06.2020 bis 09.09.2020 entgegen der gebotenen Sorgfalt Gesundheitsdaten ohne Rechtsgrundlage verarbeitet und deren unverzügliche Löschung sowie die Meldung der Datenschutzverletzung unterlassen wurden.
Kommando Cyber- und Informationsraum der Bundeswehr	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen gegen Art. 5 Abs. 1 lit. f) i.V.m. Art. 32. Abs. 1 DSGVO wegen fehlender Zugangsbeschränkung zu einer Share-Point-Arbeitsumgebung und damit Ermöglichung des Zugriff zu den dort gespeicherten Daten durch einen nicht begrenzten Kreis von unbefugten Beschäftigten
Panzergrenadierbataillon 212	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) i.v.m. Art. 32 Abs. 1 DSGVO wegen der Ermöglichung des Zugang durch fehlende Zugangsbeschränkung zu einem Laufwerk durch einen nicht begrenzten Kreis von Beschäftigten
Physikalisch-Technische Bundesanstalt	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 12 Abs. 3 S. 1 DSGVO wegen der Bescheidung eines Auskunftsersuchens erst auf mein Tätigwerden hin
pronova BKK	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 DSGVO i.V.m. § 305 Absatz 1SGB V und § 35 Abs. 1 SGB I wegen rechtswidriger Offanbarung von Diagnosedaten an einen unbeteiligten Dritten sowie gegen Art. 33 Abs. 1 DSGVO wegen fristüberschreitender Meldung des Datenschutzverstoßes trotz vorheriger Kenntnis
Siemens-Betriebskrankenkasse	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der elektronischen Patientenakte (ePA) bis zum 31.12.2021 so auszugestalten, dass Versicherte eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 SGB V in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen („feingranulares Zugriffsmanagement“) können.
Siemens-Betriebskrankenkasse	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der ePA binnen eines Jahres so auszugestalten, dass auch Frontend-Nichtnutzer auch ohne die Bestellung eines Vertreters in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.
Stiftung Erinnerung, Verantwortung und Zukunft	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen gegen Art. 5 Abs. 1 lit. f) i.V.m. Art. 32. Abs. 1 DSGVO wegen fehlender Zugangsbeschränkung auf das Laufwerk des Justiziariates un damit Ermöglichung des Zugriffs zu den dort gespeicherten personenbezogenen Daten durch Unbebefugte
Techniker Krankenkasse	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der elektronischen Patientenakte (ePA) bis zum 31.12.2021 so auszugestalten, dass Versicherte eine Einwilligung gegenüber Zugriffsberechtigten nach § 352 SGB V in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen („feingranulares Zugriffsmanagement“) können.

Stelle	Maßnahme/Beanstandung	Grund
Techniker Krankenkasse	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Anweisung, das Zugriffsmanagement der ePA binnen eines Jahres so auszugestalten, dass auch Frontend-Nichtnutzer auch ohne die Bestellung eines Vertreters in die sie betreffenden personenbezogenen Daten (sowohl Dokumente und Datensätze der ePA als auch Protokolldaten) Einblick nehmen können.
Techniker Krankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) i.V.m. Art. 6 Abs. 1 DSGVO wegen der Übersendung einer vollständigen und ungeschwärzten Versorgungsbezügemitteilung an das Amtsgericht Schleswig und der unrechtmäßigen Offenbarung nicht geforderter und nicht erforderlicher Daten
Verpflegungsamt der Bundeswehr	Verwarnungen gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. c) und f) i.V.m. Art. 32 Abs. 1 DSGVO wegen der Verarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO ohne entsprechende Rechtsgrundlage und entgegen der gebotenen Sorgfalt durch vorgesetzte Personen und unzuständige Stellen innerhalb des Verpflegungsamtes der Bundeswehr und gegen Art. 5 Abs. 1 lit. f) DSGVO wegen der Öffnung und unterlassenen Weiterleitung verschlossener Umschläge mit ärztlichen Unterlagen
Zentrale Stelle für Informationstechnik im Sicherheitsbereich	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 BDSG	Verstoß gegen § 21 Abs. 1 Satz 4 SÜG wegen Übermittlung unter Missachtung der Zweckbindung und Verstoß gegen § 6 Abs. 1 SÜG wegen Verstoß gegen Verfahrensrechte
Zentrum für Geoinformationswesen der Bundeswehr	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) – c), Art. 6 DSGVO und § 26 BDSG wegen der Erhebung und Verarbeitung personenbezogener Daten von Beschäftigten in Form von monatlichen Tätigkeitsberichten ohne Rechtsgrundlage

Nicht alle der oben aufgelisteten Maßnahmen und Beanstandungen sind bisher rechtskräftig.

Übersicht über Maßnahmen/Beanstandungen gegenüber nicht-öffentlichen Stellen

Stelle	Maßnahme/Beanstandung	Grund
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) DSGVO sowie Art. 32 Abs. 1 lit. b) DSGVO wegen unberechtigter Offenlegung personenbezogener Daten
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) DSGVO sowie Art. 32 Abs. 1 lit. b) DSGVO wegen unberechtigter Offenlegung personenbezogener Daten
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) DSGVO sowie Art. 32 Abs. 1 lit. b) DSGVO wegen unberechtigter Offenlegung personenbezogener Daten
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) DSGVO und Art. 5 Abs. 1 lit. c) i. V. m. Art. 6 Abs. 1 DSGVO wegen unrechtmäßiger und nicht dem Zweck angemessener Verarbeitung personenbezogener Daten
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 i. V. m. Art 12 Abs. 3 und 4 DSGVO wegen Nichttätigsein des Verantwortlichen trotz zweimaliger kostenloser Erinnerung und Anrufung der Aufsichtsbehörde
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) DSGVO sowie Art. 32 Abs. 1 lit. b) DSGVO wegen unberechtigter Offenlegung personenbezogener Daten
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 i. V. m. Art. 12 Abs. 3 DSGVO wegen Fristüberschreitung der Auskunftserteilung
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 S. 1 DSGVO sowie § 39 Abs. 3 PostG wegen wiederholter Falschzustellungen
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 i. V. m. Art. 12 Abs. 3 DSGVO wegen Fristüberschreitung der Auskunftserteilung
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 S. 1 und Art. 32 Abs. 1 lit. b) DSGVO sowie § 39 Abs. 3 S. 1 PostG wegen fehlerhafter Kuvertierung von Sendungen
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 33 Abs. 1 DSGVO wegen verspäter Meldung einer Datenschutzverletzung
Ein Postdienstleistungs-unternehmen	Warnung gemäß Art. 58 Abs. 2 lit. a) DSGVO	drohender Verstoß gegen Art. 6 Abs. 1 S. 1 DSGVO, § 41a Abs. 3 Satz 1 sowie§ 39 Abs. 3 S. 1 PostG wegen voraussichtlicher unrechtmäßiger Verarbeitung von Empfängerdaten
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 S. 1 DSGVO wegen des Erstellens von Fotos von Ersatz-Empfängern oder deren Personalausweisen
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 S. 1 DSGVO wegen unzulässiger Übermittlung einer Mobilfunknummer an einen Dritten
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 i. V. m. Art. 12 Abs. 3 DSGVO wegen Fristüberschreitung der Auskunftserteilung
Ein Postdienstleistungs-unternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 33 Abs. 1 DSGVO wegen Versäumnis einer Meldung über eine Datenschutzverletzung

Stelle	Maßnahme/Beanstandung	Grund
Telekommunikations-dienstleistungsunterneh-men	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 12 Abs. 1 DSGVO wegen Nichtzulassens mündlicher oder telefonischer Anträge zu Betroffenenrechten
Telekommunikations-dienstleistungsunterneh-men	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 2 i.V.m. Art. 5 Abs. 1 lit. a) und c) DSGVO wegen des Versandes einer vollständigen, unbereinig-ten Kopie eines umfangreichen medizinischen Gutachtens an Betriebsratmitglieder und die Schwerbehindertenvertretung, nach teilweise erfolgter Löschung des Originals
Telekommunikations-dienstleistungsunterneh-men	Beanstandung gemäß § 115 Abs. 4 S. 2 TKG i.V.m. § 25 Abs. 1 BDSG a.F.	Verstoß gegen § 109 Abs. 1 S. 1 Nr. 2 TKG wegen mangelhafter TOM's einem Ad-hoc-Telefonkonferenzsystem
Telekommunikations-dienstleistungsunterneh-men	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO und An-weisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Verstoß gegen Art. 7 DSGVO wegen Nichteinhaltens der Vorgaben der DSGVO zum Erfordernis eines Opt-In-Verfahrens hinsichtlich einer Einwilligung zur Aufzeichnung von Telefon-gesprächen zur Qualitätskontrolle; es wurde eine Opt-Out-Lö-sung verwendet
Telekommunikations-dienstleistungsunterneh-men	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO und An-weisung gemäß Art. 58 Abs. 2 lit. c) DSGVO	Verstoß gegen Art. 15 DSGVO wegen nicht beantwortetem Auskunftsersuchen
Telekommunikations-dienstleistungsunterneh-men	Anweisung gemäß Art. 58 Abs. 2 lit. e) DSGVO	Verstoß gegen Art. 34 DSGVO wegen nicht vorgenommener Mitteilung einer Datenschutzverletzung an die betroffenen Personen
Telekommunikations-dienstleistungsunterneh-men	Beanstandung gemäß § 115 Abs. 4 S. 2 TKG i.V.m. § 95 Abs. 2 S. 2 TKG	Verstoß gegen § 95 Abs. 2 Satz 2 TKG wegen Werbung trotz Werbewiderspruch
Telekommunikations-dienstleistungsunterneh-men	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 33 DSGVO wegen verspäteter Meldung einer Datenschutzverletzung
Telekommunikations-dienstleistungsunterneh-men	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) DSGVO wegen Abbuchungen ohne Vertragsschluss
Telekommunikations-dienstleistungsunterneh-men	Anweisung gemäß Art. 58 Abs. 1 lit. a) DSGVO	Heranziehung von Informationen zu Kundendaten
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 BDSG	Verstoß gegen § 30 i.V.m. § 18 Abs. 1 SÜG wegen unzurei-chender Dokumentation von Bearbeitungs- und Verfahrens-schritten; Verstoß gegen § 36 Abs. 1 Nr. 2 SÜG i.V.m. § 51 Abs. 1 BDSG wegen fehlende Dokumentation der Einwilligung in die Datenübermittlung an Dritte; Verstoß gegen §§ 30 i.V.m. 19 Abs. 2 und §§ 30 i.V.m. 22 Abs. 2 Nr.1 SÜG wegen Verstoß gegen Vernichtungs- und Löschfristen; Verstoß gegen § 2 Abs. 2 S. 3 und 4 SÜG wegen fehlende Dokumentation der Zustimmung der mitbetroffenen Person

Nicht alle der oben aufgelisteten Maßnahmen und Beanstandungen sind bisher rechtskräftig.

Abkürzungsverzeichnis

AA	Auswärtiges Amt
Abs.	Absatz
a. F.	alte Fassung
AFIS	Automatisiertes Fingerabdruck-identifizierungssystem
AG	Aktiengesellschaft
AK	Arbeitskreis
AkkStelleG	Gesetz über die Akkreditierungsstelle
AlVi	alternativen Versichertenidentität
AO	Abgabenordnung
API-Daten	Advanced Passenger Information (Vorab-Passagier-Information)
API-RL	RICHTLINIE 2004/82/EG DES RATES vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln
App(s)	Applikation(en)
Art.	Artikel
AsylG	Asylgesetz
ATD	Anti-Terror-Datei
ATDG	Antiterrordateigesetz
Az.	Aktenzeichen
AZR	Ausländerzentralregister
AZRG	Ausländerzentralregistergesetz
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BAMF	Bundesamt für Migration und Flüchtlinge
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfR	Bundesinstitut für Risikobewertung
BfV	Bundesamt für Verfassungsschutz
BImA	Bundesanstalt für Immobilienaufgaben
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BKAmt	Bundeskanzleramt
BKartA	Bundeskartellamt
BKM	Die Beauftragte der Bundesregierung für Kultur und Medien
BMAS	Bundesministerium für Arbeits und Soziales
BMBF	Bundesministerium für Bildung und Forschung
BMEL	Bundesministerium für Ernährung und Landwirtschaft
BMF	Bundesministerium für Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMG	Bundesmeldegesetz (auch wenn es identisch zum Bundesministerium für Gesundheit ist)
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMU	Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit
BMVg	Bundesministeriums der Verteidigung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministeriums für Wirtschaft und Energie
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BND-Gesetz	Gesetz über den Bundesnachrichtendienst
BNetzA	Bundesnetzagentur
bpb	Bundeszentrale für politische Bildung
BPol	Bundespolizei
BPolG	Gesetz über die Bundespolizei
BPrA	Bundespresseamt
BRH	Bundesrechnungshof
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Deutscher Bundestag
BTLE ESG	Expert Subgroup Borders, Travel and Law Enforcement
BVerfG	Bundesverfassungsgericht
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BvR	Aktenzeichen einer Verfassungsbeschwerde beim Bundesverfassungsgericht
bzw.	beziehungsweise
CCF	Competence Center Fachlichkeit
CCOD	Kompetenzzentrum Open Data
CISPE	Cloud Infrastructure Services Providers in Europe, Anbieter von Cloud-Infrastruktur-Services in Europa
CoC	Codes of Conduct
CSC	Coordinated Supervision Committee (Ausschuss für koordinierte Aufsicht)
CWA	Corona Warn App

DA	Data Act
DaTraV	Datentransparenzverordnung
DB AG	Deutsche Bahn AG
DGA	Data Governance Act
d. h.	das heißt
DiGA	Digitale Gesundheitsanwendungen
DiGAV	Digitale Gesundheitsanwendungen Verordnung
DigFamG	Gesetz zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
DMA	Digital Markets Act
DMS	Dokumentenmanagementsystem
DSA	Digital Services Act
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DVPMG	Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz
eAMS	einheitliches Asservatenmanagementsystem
EAS	elektronische Akte in Strafsachen
ED-Daten	Erkennungsdienstliche Daten
EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
EDSA	Europäischer Datenausschuss
EDSB	Europäische Datenschutzbeauftragte
EG	Europäische Gemeinschaft
eGK	elektronische Gesundheitskarte
EGovG	E-Government-Gesetzes
eID	elektronische Identität
eIDAS	Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen
eIDKG	eID-Karte-Gesetz
ePA	Elektronische Patientenakte
ePKA	Elektronische Patientenkurzakte
ERP	Enterprise-Resource-Planning
EU	Europäische Union
EuGH	Europäischer Gerichtshof
Eurodac	European Dactyloscopy
EUStA	Europäische Staatsanwaltschaft
EWR	Europäischer Wirtschaftsraum
ExCo	Executive Committee
FBS	Fallbearbeitungssysteme
FDZ	Forschungsdatenzentrum
ff.	fortfolgende
FIU	Zentralstelle für Finanztransaktionsuntersuchungen, Abk. für Financial Intelligence Unit
FlugDaG	Gesetz über die Verarbeitung von Fluggastdaten
GAEN	Google/Apple Exposure Notifications
gem.	gemäß
GETZ	Gemeinsames Extremismus- und Terrorismusabwehrzentrum
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GKV	Gesetzliche Krankenversicherung
GKV-SP	Spitzenverband Bund der Krankenkassen
GmbH	Gesellschaft mit beschränkter Haftung
GPA	Global Privacy Assembly
GVWG	Gesundheitsversorgungsweiterentwicklungsgesetz
GWB	Gesetz gegen Wettbewerbsbeschränkungen
GWG	Geldwäschegesetz
HmbBfDI	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit
HZI	Helmholtz-Zentrum für Infektionsforschung
ITS ESG	Expert Subgroup International Transfers
IWGDPT	International Working Group Data Protection in Technology“
ICIC	International Conference of Information Commissioners
IFG	Informationsfreiheitsgesetz
IfSG	Infektionsschutzgesetz
INPOL	Das elektronische Informationssystem der Polizei
INPOL-Z	Das bundesweite zentrale polizeiliche Informationssystem
INZOLL	Informationssystem des Zollfahndungsdienstes
IP	Internet Protocol
IRegG	Implantateregistergesetz
i. S. d.	im Sinne des
IT	Informationstechnik
ITZ Bund	Informationstechnikzentrum Bund
i. v. m.	in Verbindung mit
JI-Richtlinie	Richtlinie zum Datenschutz bei Polizei und Justiz
KI	Künstliche Intelligenz
KVNR	Krankenversichertennummer
LfD	Landesbeauftragter für den Datenschutz
LfDI	Landesbeauftragte/r für den Datenschutz und die Informationsfreiheit

lit.	Litera
MAD-Gesetz	Gesetz über den Militärischen Abschirmdienst
MIO	Medizinischen Informationsobjekten
Mio.	Millionen
NADIS	Nachrichtendienstliches Informationssystem
NIPT	nicht invasiver pränataler Bluttest
Nr.	Nummer
NRW	Nordrhein-Westfalen
OECD	Organisation für wirtschaftliche-Zusammenarbeit und Entwicklung
OGP	Open Government Partnership
oOKF	Open Knowledge Foundation
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
OZG	Onlinezugangsgesetz
PAuswG	Personalausweisgesetz
PBE	Personalbedarfsermittlung
PDSG	Patientendaten-Schutz-Gesetz
PEPP-PT	Pan-European Privacy-Preserving Proximity Tracing
PIMS	Personal Information Management Systems
PKGr	Parlamentarisches Kontrollgremium
PKV	Private Krankenversicherung
PNR-Daten	Fluggastdatensätze
PNR-RL	Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen
PoC	Proof of Concept
PTB	Physikalisch-Technische Bundesanstalt
PüP	periodenübergreifenden Pseudonyms
PVSplus	Personalverwaltungssystem
Quellen-TKÜ	Telekommunikationsüberwachung
RED	Rechtsextremismus-Datei
RKI	Robert Koch-Institut
RL	Richtlinie
S.	Seite
s.	siehe
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
SIS II	Schengener Informationssystem der 2. Generation
SMS	Short Message Service
sog.	so genannte
SORMAS	Surveillance Outbreak Response Management und Analysis System
StPO	Strafprozessordnung
StrlSchV	Strahlenschutzverordnung
StUG	Stasi-Unterlagen-Gesetz
SÜG	Sicherheitsüberprüfungsgesetz
TB	Tätigkeitsbericht
TI	Telematikinfrastruktur
TIM	TI-Messenger
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKMoG	Telekommunikationsmodernisierungsgesetz
TTDSG	Telekommunikations-Telemedien-Datenschutz-Gesetz
u. a.	unter anderem
UIG	Umweltinformationsgesetz
UrhG	Urheberrechtsgesetz
USA	United States of America
VBS	Vorgangsbearbeitungssystem
VG	Verwaltungsgericht
vgl.	vergleiche
VIS	Visa-Informationssystem
VISZG	VIS-Zugangsgesetz (Gesetz über den Zugang von Polizei- und Strafverfolgungsbehörden sowie Nachrichtendiensten zum Visa-Informationssystem)
vs.	versus
z. B.	zum Beispiel
ZASt	Zentrale Anlaufstelle
ZFdG	Gesetz über das Zollkriminalamt und die Zollfahndungsämter
ZfKD	Zentrum für Krebsregisterdaten
ZKA	Zollkriminalamt
56ID	Identifikation der federführenden Aufsichtsbehörde
60FD	endgültiger Beschluss der federführenden Aufsichtsbehörde (Final Decision)

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Graurheindorfer Str. 153
53117 Bonn

Tel. +49 (0) 228 997799-0
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Bonn 2022
Dieser Bericht ist als Bundestagsdrucksache erschienen.

Bildnachweis: Erzaehlmirnix

Druck:
Druckerei Franz Paffenholz GmbH
Königstraße 82
53332 Bornheim