Abgeordnetenhaus BERLIN

Drucksache 19/2355
02.04.2025

19. Wahlperiode

Vorlage – zur Kenntnisnahme –

Stellungnahme des Senats zum Bericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2023

Der Senat von Berlin
SenInnSport – I AbtL 1
Tel. (9223) 2066

An das
Abgeordnetenhaus von Berlin

über Senatskanzlei G Sen

V o r l a g e
des Senats von Berlin
- zur Kenntnisnahme -

über Stellungnahme des Senats zum Bericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2023

Der Senat legt nachstehende Vorlage dem Abgeordnetenhaus zur Besprechung vor:

Nach § 12 Abs. 1 Berliner Datenschutzgesetz sowie § 18 Abs. 3 Berliner Informationsfreiheitsgesetzes erstattet die Beauftragte für Datenschutz und Informationsfreiheit dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis ihrer Tätigkeit. Der Senat hat dazu nach § 12 Abs. 2 des Berliner Datenschutzgesetzes eine Stellungnahme herbeizuführen und legt diese hiermit dem Abgeordnetenhaus vor.

Berlin, den 1. April 2025

Der Senat von Berlin

Kai Wegner	Iris Spranger
---	---
Regierender Bürgermeister	Senatorin für Inneres und Sport

Stellungnahme des Senats

zum Bericht der

Berliner Beauftragten für

Datenschutz und

Informationsfreiheit

für das

Jahr 2023

(nach § 12 Abs.2 Berliner Datenschutzgesetz)

Inhaltsverzeichnis

Vorwort

Der vorliegende Jahresbericht dokumentiert auf 174 Seiten die umfangreichen Tätigkeiten meiner Behörde und zeigt die Vielfalt an Themen, mit denen wir uns im letzten Jahr befasst haben. Herzlich möchte ich mich bei meinen Mitarbeiter:innen für diese Arbeit bedanken.

In Zeiten, in denen große Technologiekonzerne mit der Fortentwicklung von Modellen generativer Künstlicher Intelligenz über digitale Infrastruktur und die Ausgestaltung des digitalen Lebens bestimmen, muss sich auch die Datenschutzaufsicht globalisieren. Unser Wirken auf nationaler wie internationaler Ebene ist unerlässlich, um unsere Aufgaben zu erfüllen, die Grundrechte und Grundfreiheiten von Personen zu schützen und für deren Recht auf den Schutz personenbezogener Daten einzutreten. In Beschwerde- und Prüfverfahren kooperieren wir mit den nationalen und europäischen Datenschutzbehörden und entwickeln gemeinsam Leitlinien für die Praxis sowie Stellungnahmen in Gerichts- und Gesetzgebungsverfahren. Unser Ziel ist es, gemeinsame Standards in der Aufsichts- und Beratungspraxis zu etablieren und auf dieser Basis unsere von Amts wegen veranlassten und strukturellen Prüfungen auszubauen.

Informationsfreiheit und Transparenz des Verwaltungshandelns sind wichtige Instru- mente, um gegen die Spaltung von Gesellschaften zu wirken. Gerade das proaktive Veröffentlichen von Informationen bietet der öffentlichen Hand die Chance, ihr Handeln nachvollziehbarer zu machen und die Menschen an staatlichen Entscheidungen teil- haben zu lassen. Wir setzen uns daher weiter für ein Berliner Transparenzgesetz und ein stetiges Umdenken ein, das die Förderung von Transparenz in der Verwaltung nicht als Bürde, sondern als eigenes öffentliches Interesse und öffentliche Aufgabe begreift. Die digitale Transformation kann diesen Prozess unterstützen, wenn das Konzept der Informationsfreiheit by Design von Anfang an mitgedacht und umgesetzt wird.

Der Jahresbericht enthält Highlights und Lowlights des Jahres 2023. Manches ist schon gut, vieles ist zu optimieren. Wir bleiben dran.

Eine aufschlussreiche Lektüre wünscht Ihnen

Meike Kamp
Berliner Beauftragte für Datenschutz und Informationsfreiheit

A. Wir in Berlin

I. Gesetzesvorhaben und Landesverordnungen

1. Das Transparenzgesetz lässt weiter auf sich warten

Seit Jahren soll das Berliner Informationsfreiheitsgesetz (IFG) durch ein modernes Transparenzgesetz abgelöst werden. Auch die neue Landesregierung hat sich dies zum Ziel gesetzt. Bisher haben aber nur die Oppositionsparteien einen Gesetzesentwurf vorgelegt, der in diesem Jahr im Abgeordnetenhaus diskutiert wurde.

Bereits 2016 hatten die damaligen Regierungsparteien das Vorhaben in ihren Koalitionsvertrag aufgenommen, das IFG von 1999 durch ein modernes Transparenzgesetz zu ersetzen. Trotz verschiedener Entwicklungen, über die wir in den vergangenen Jahren berichtet haben,[1] wurde das Vorhaben bisher nicht in die Tat umgesetzt. Auch die neue Koalition hat die Forderung nach einer Gesetzesreform in ihrem Koalitionsvertrag aufgegriffen. Danach will die Koalition „schnellstmöglich ein Transparenzgesetz nach Hamburger Vorbild“ einführen, wobei „die hohen Standards des Berliner Informationsfreiheitsgesetzes erhalten“ bleiben und lediglich der „Verfassungsschutz aus dem Geltungsbereich“ herausgenommen werden soll.[2]

Während auf Seiten der Landesregierung noch keine Schritte zur Modernisierung des Informationsfreiheitsrechts erkennbar sind, haben zwei Oppositionsfraktionen einen Entwurf für ein Berliner Transparenzgesetz in das Abgeordnetenhaus eingebracht.[3] Dieser Entwurf wurde im September 2023 im Rahmen einer Expertenanhörung des federführenden Ausschusses für Digitalisierung und Datenschutz (DiDat) diskutiert und bildet aus unserer Sicht eine gute Grundlage für die weitere Diskussion.

Um das Vertrauen der Menschen und deren Möglichkeiten zur Partizipation am Gemeinwesen zu stärken, ist die Weiterentwicklung des inzwischen 24 Jahre alten IFG zu einem modernen Transparenzgesetz unverzichtbar: Neben dem Recht auf Informationszugang muss

Nach Kenntnis des Senats dauern die politischen Gespräche der Koalitionspartner über die mögliche Weiterentwicklung des Informationsfreiheitsgesetzes zu einem Transparenzgesetz aktuell an. Dem Ergebnis der weiterhin laufenden Abstimmungs- und Entscheidungsprozesse kann nicht vorgegriffen werden.

[1] Siehe JB 2019, 17.3; JB 2020, 19.2.2; JB 2021, 17.2.1; JB 2022, 16.2.
[2] CDU Berlin und SPD Berlin, Koalitionsvertrag 2023–2026, S. 12 f., abrufbar unter https://www.berlin.de/rbmskzl/politik/senat/koalitionsvertrag/.
[3] Siehe Abgeordnetenhaus, Antrag der Fraktion Bündnis 90/Die Grünen und der Fraktion Die Linke zum Gesetz zur Regelung von Transparenz in Berlin vom 7. Juni 2023, Drs. 19/1014, abrufbar unter https://www.parlament-berlin.de/ados/19/IIIPlen/vorgang/d19-1014.pdf.

auch die Pflicht zur proaktiven Bereitstellung von Informationen durch informationspflichtige Stellen geregelt werden. Wir begrüßen das Bekenntnis der Regierung zu diesem Gesetzesvorhaben, fordern aber auch eine zügige Umsetzung.

2. Schuldatenverordnung und Digitale Lehr- und Lernmittelverordnung

Mit dem Inkrafttreten der novellierten Schuldatenverordnung (SchuldatenV)[4] und dem Erlass einer Digitalen Lehr- und Lernmittelverordnung (DigLLV)[5] rechtzeitig zum Beginn des Schuljahrs 2023/24 hat die Senatsverwaltung für Bildung, Jugend und Familie (SenBJF) den Schulen nun die längst überfälligen Regelungen zum Umgang mit personenbezogenen Daten in der Schule und insbesondere beim Einsatz digitaler Lehr- und Lernmittel zur Verfügung gestellt.

Wir begrüßen, dass der langwierige Prozess[6] der Novellierung der SchuldatenV aus dem Jahre 1994 endlich abgeschlossen ist. Spätestens mit der Anpassung des Schulgesetzes (SchulG) im Oktober 2021 war die Anpassung der SchuldatenV nicht mehr aufschiebbar. Gleichzeitig zur SchuldatenV hat die Bildungsverwaltung die DigLLV erlassen, die die Anforderungen an den Einsatz digitaler Lehr- und Lernmittel sowie digitaler Kommunikationswerkzeuge in den Schulen näher regelt. Beide Verordnungen sind im August dieses Jahres in Kraft getreten. In diesem Prozess haben wir viele Beratungsgespräche mit der Bildungsverwaltung geführt und immer wieder auch schriftlich Stellung genommen.

Der gute regelmäßige Austausch zwischen der Senatsverwaltung für Bildung, Jugend und Familie und der Berliner Beauftragten für Datenschutz und Informationsfreiheit wird seitens des Senats für die Ziele der Digitalisierung an den Berliner Schulen als sehr förderlich eingeschätzt.

Unsere Kritikpunkte wurden nicht immer aufgegriffen. Beispielhaft nennen lässt sich die Regelung der DigLLV zur Aufzeichnung von Ton- und Bilddaten im Rahmen einer schulischen Veranstaltung und insbesondere im Unterricht. Voraussetzung hierfür ist,[7] dass die Aufzeichnung nach pädagogischem Ermessen zur Erreichung des Zwecks der jeweiligen Unterrichtseinheit „konkret förderlich“ ist. Die Regelung bleibt hinter der Anforderung zurück, dass eine Verarbeitung personenbezogener Daten „erforderlich“, also notwendig für die Erreichung des gesetzlichen Zwecks, sein muss. Sie genügt damit nicht den Vorgaben der Öffnungsklauseln der Datenschutz-Grundverordnung (DSGVO), in deren Rahmen die Mitgliedsstaaten Rechtsgrundlagen zur

[4]Verordnung über die Verarbeitung personenbezogener Daten im Schulwesen vom 7. August 2023, GVBl. 2023, 283.
[5]Verordnung über die Verarbeitung personenbezogener Daten beim Einsatz von digitalen Lehr- und Lernmitteln und sonstigen pädagogischen Zwecken dienenden digitalen Instrumenten vom 7. August 2023, GVBl. 2023, 296.
[6]Siehe JB 2019, 5.4; JB 2021, 1.2.2; JB 2022, 4.4.1.
[7]§ 5 Abs. 1 DigLLV.

Datenverarbeitung erlassen dürfen.[8] Gerade bei so eingriffsintensiven Maßnahmen wie der Aufzeichnung von Ton- und Bilddaten reicht es nicht aus, wenn die Erforderlichkeit nicht erfüllt ist. Die Vorschrift ist daher entsprechend anzupassen. Bis dahin kann die Norm in der Praxis nur angewendet werden, wenn die Aufzeichnung den datenschutzrechtlichen Anforderungen der Erforderlichkeit genügt.

Die Senatsverwaltung für Bildung, Jugend und Familie überprüft die Regelung des § 5 DigLLV erneut und wird bei Bedarf eine Anpassung des Wortlautes vornehmen.

Andere Vorschriften bewerten wir positiv. So begrüßen wir es, dass die Voraussetzungen der dienstlichen Kommunikation in der SchuldatenV ausdrücklich geregelt werden und eine solche nur noch über das von der Bildungsverwaltung zur Verfügung gestellte E-Mail-Konto erfolgen darf.[9] Es ist aus Datenschutzsicht auch richtig, dass besonders schutzbedürftige personenbezogene Daten nur mit einer dem aktuellen Stand der Technik entsprechenden Ende-zu-Ende-Verschlüsselung übermittelt werden dürfen. Allerdings halten wir es im Interesse der Praxis für notwendig zu prüfen, inwieweit gerade für besonders schutzbedürftige Kommunikation, etwa Krankmeldungen von Schüler:innen, auch andere Systeme, wie beispielsweise Portallösungen, in Betracht kommen. Solche Lösungen sollten handlich und benutzerfreundlich sein sowie den Schulen durch die Bildungsverwaltung zur Verfügung gestellt werden.

Die Hinweise zur SchuldatenV werden innerhalb der Senatsverwaltung für Bildung, Jugend und Familie und in gemeinsamen Treffen mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit erörtert und bei Bedarf in die SchuldatenV einfließen.

Um den praktischen Bedürfnissen der Schulen Rechnung zu tragen, darf die Rechtssetzung jetzt nicht stehen bleiben: So ist uns aus der Beratungspraxis bekannt, dass die Schulen ein Bedürfnis nach digitalen Klassenbüchern mit Funktionen wie Notenerfassung, Verwaltung von Fehlzeiten und Krankmeldungen sowie Mitteilungsmöglichkeiten an Erziehungsberechtigte haben. Hierfür müssen Grundlagen im SchulG geschaffen werden, um dann klare Vorgaben zur Auswahl entsprechender Produkte in den Text der SchuldatenV aufzunehmen.

Insgesamt bleibt festzustellen, dass mit den beiden Verordnungen viele der gerade in der Praxis zur Verunsicherung führenden Aspekte noch nicht ausreichend geklärt sind. Hier besteht Nachbesserungsbedarf. Eine stetige Evaluation anhand der praktischen Bedürfnisse der Schulen ist hier das Mittel der Wahl, um entsprechende Nachbesserungen zügig voranzutreiben. Gern stehen wir hierfür beratend zur Verfügung.

[8] Art. 6 Abs. 3 Satz 2 DSGVO.
[9] § 18 SchuldatenV.

2. Staatsvertrag über den Rundfunk Berlin-Brandenburg

Das Abgeordnetenhaus von Berlin und der Brandenburger Landtag haben im Dezember dieses Jahres die Novellierung des Staatsvertrags über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg (RBB-Staats-vertrag) beschlossen. Mit Inkrafttreten des Staatsvertrags zum 1. Januar 2024 ändert sich die Aufsichtszuständigkeit über die Einhaltung der Datenschutzbestimmungen beim Rundfunk Berlin-Brandenburg (RBB).

Bisher gehörte es zu den Aufgaben der Datenschutzbeauftragten des RBB, die Einhaltung der Datenschutzbestimmungen bei der Verarbeitung personenbezogener Daten für journalistische Zwecke zu überprüfen. Unsere Behörde war hingegen gemeinsam mit der Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht (LDA) Brandenburg für die datenschutzrechtliche Aufsicht über den wirtschaftlich-administrativen Bereich zuständig. Dies beinhaltete insbesondere die Kontrolle über die rechtmäßige Verarbeitung der Daten der Beitragszahler:innen und der Beschäftigten des RBB sowie dessen Hilfs- und Beteiligungsunternehmen. Seit Inkrafttreten des RBB-Staatsvertrags untersteht die Kontrolle über beide Bereiche der bzw. dem Rundfunkdatenschutzbeauftragten des RBB.

Für die Änderung der Aufsichtszuständigkeit bestand aus unserer Sicht keine Notwendigkeit, die bisherige Aufteilung hatte sich bewährt.[10]

Mit dem novellierten Staatsvertrag liegt die Kontrolle der Einhaltung der Datenschutzbestimmungen beim RBB allein in der Hand der bzw. des Rundfunkdatenschutzbeauftragen. Bei datenschutzrechtlichen Fragen oder Beschwerden müssen Beitragszahler:innen sowie Beschäftigte des RBB und seiner Hilfs- und Beteiligungsunternehmen von nun an deren bzw. dessen Hilfe in Anspruch nehmen.

II. Gerichtsurteile

1. Rechtmäßigkeit von Sanktionen gegen Unternehmen

Im Jahre 2019 haben wir einen Bescheid mit Bußgeldern in Höhe von 14,5 Millionen Euro gegen die Deutsche Wohnen SE wegen mangelnder Vorkehrungen zur regelmäßigen Löschung von Daten der Mieter:innen erlassen. Der Bescheid wurde vor Gericht angefochten. Nachdem das Kammergericht im Anschluss an das

[10] Siehe JB 2022, 13.5.

Landgericht Berlin zwei Rechtsfragen vorlegte, hat der Europäische Gerichtshof (EuGH) nun unsere Auffassung bestätigt: Datenschutzrechtliche Bußgelder können direkt gegen Unternehmen verhängt werden. Gleichzeitig stellt der EuGH fest, dass ein objektiver Verstoß gegen das Datenschutzrecht für eine Geldbuße nicht ausreicht. Nachgewiesen werden muss, dass der Verstoß vorsätzlich oder fahrlässig begangen wurde.

Auf den Einspruch der Deutsche Wohnen SE gegen unseren Bußgeldbescheid hatte das Landgericht Berlin das Verfahren im Februar 2021 zunächst eingestellt. Unserem Bußgeldbescheid wurde entgegengehalten, dass eine juristische Person in einem Bußgeldverfahren nicht Betroffene, sondern nur Nebenbeteiligte sein könne. Da eine juristische Person selbst keine Ordnungswidrigkeit begehen könne, müsse nach § 30 Ordnungswidrigkeitengesetz (OWiG) eine Tat eines Organmitglieds oder Repräsentanten festgestellt sein, um eine Geldbuße gegen die juristische Person festsetzen zu können. Die Staatsanwaltschaft legte sofortige Beschwerde ein. Das befasste Kammergericht setzte das Verfahren aus und legte dem EuGH die Frage vor, ob eine ein Unternehmen betreibende juristische Person in Deutschland nach den Grundsätzen des EU-Rechts unmittelbar für Datenschutzverstöße nach der Datenschutz-Grundverordnung (DSGVO) sanktioniert werden kann, ohne dass eine Ordnungswidrigkeit einer natürlichen und identifizierten Leitungsperson festgestellt werden muss. Zusätzlich wollte es wissen, ob es bei einem Bußgeld nach Art. 83 DSGVO das Unternehmen den durch seine Beschäftigten verursachten Verstoß schuldhaft begangen haben muss oder der bloße objektive Pflichtenverstoß (strict liability) ausreicht.

Der EuGH entschied nun im Dezember 2023,[11] dass eine juristische Person nicht nur für Verstöße hafte, die durch Leitungspersonen begangen wurden, sondern auch für solche, die im Rahmen der unternehmerischen Tätigkeit und im Namen der juristischen Person von anderen Personen begangen werden. Eine Geldbuße könne dann auch unmittelbar gegen die juristische Person verhängt werden, ohne dass die konkret handelnden natürlichen Personen identifiziert werden müssten.[12] Der EuGH begründet dies damit, dass sich die in der DSGVO vorgesehenen Grundsätze, Verbote und Pflichten insbesondere an „Verantwortliche“ i. S. d. Art. 4 Nr. 7 DSGVO richteten.[13] Diese Definition schließe ausdrücklich auch juristische Personen ein. Die Haftung der Verantwortlichen erstrecke sich auf

[11] EuGH, Urteil vom 5. Dezember 2023, C-807/21.
[12] Ebd., Rn. 44, 46.
[13] Ebd., Rn. 38.

jedwede Verarbeitung personenbezogener Daten, die durch sie oder in ihrem Namen erfolgten. In diesem Rahmen haften die Verantwortlichen dafür, geeignete und wirksame Maßnahmen zu treffen, die die DSGVO-konforme Verarbeitung sicherstellten. Diese Haftung bilde bei einem der in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstöße die Grundlage dafür, dass Geldbußen verhängt werden könnten.[14] Das Gericht sieht das europäische Zurechnungssystem des Art. 83 DSGVO damit als abschließend an, sodass kein Ermessensspielraum für die Mitgliedstaaten bestehe, materielle Regelungen zu treffen.[15]

Als Antwort auf eine zweite Vorlagefrage des Kammergerichts entschied der EuGH: Eine Geldbuße kann nur dann verhängt werden, wenn nachgewiesen ist, dass der Verstoß vorsätzlich oder fahrlässig begangen wurde. Dabei soll es ausreichend sein, wenn Verantwortliche sich über die Rechtswidrigkeit ihres Verhaltens nicht im Unklaren sein konnten, unabhängig davon, ob ihnen bewusst war, dass sie gegen die Vorschriften der DSGVO verstoßen.[16] Bei juristischen Personen setze Art. 83 DSGVO keine Handlung, nicht einmal Kenntnis seitens des Leitungsorgans dieser juristischen Person voraus.[17] Im Bescheid zum Bußgeldverfahren gegen die Deutsche Wohnen SE hatten wir ein vorsätzliches Handeln festgestellt. Nun muss zunächst das Kammergericht im Beschwerdeverfahren unter Zugrundelegung der Vorgaben des EuGH über den Beschluss des Landgerichts Berlin entscheiden. Hebt das Kammergericht den Beschluss auf, wird das Verfahren vor dem Landgericht Berlin weitergeführt.

Der EuGH bestätigt, Bußgelder können nach der DSGVO unmittelbar gegen juristische Personen verhängt werden, ohne dass die Einschränkung des § 30 Abs. 1 OWiG gilt. Mitgliedstaatliche Regelungen dürfen nur verfahrensrechtliche Anforderungen an das Bußgeldverfahren normieren und keine materiellen Regelungen treffen. Der Unternehmensbegriff nach Art. 101 und 102 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) ist für die Berechnung der Bußgeldhöhe maßgeblich. Vorsatz oder Fahrlässigkeit müssen nachgewiesen sein, um ein Verhalten mit einer Geldbuße zu sanktionieren. Dabei kommt es darauf an, dass die Verantwortlichen über die Rechtswidrigkeit nicht im Unklaren sein konnten.

[14] Ebd., Rn. 38.
[15] Ebd., Rn. 45, 48, 65.
[16] Ebd., Rn. 76.
[17] Ebd., Rn. 77.

2. Identitätsfeststellung und Mitwirkungspflichten bei Betroffenenrechten

Das Verwaltungsgericht Berlin stellte im April in einem Beschluss fest, dass Antragsteller:innen bei der Ausübung ihrer Betroffenenrechte nach DSGVO in bestimmten Fällen eine Mitwirkungspflicht haben.[18] So kann eine Auskunft verweigert werden, wenn die betroffene Person in einem Zweifelsfall auch nach Aufforderung durch die Verantwortlichen ihre Identität nicht nachweist.

Im vorliegenden Fall hatte eine Auskunftei Zweifel an der Identität des Antragstellers eines Auskunftsanspruchs, da in ihrem Datenbestand zwei weitere Personen aufgeführt waren, die denselben Vor- und Nachnamen wie der Antragsteller hatten. Um zu vermeiden, dass die sehr schutzbedürftigen Daten (Bonitätsinformationen) in unberechtigte Hände gelangen, erfragte die Auskunftei daher zur weiteren Identifizierung des Antragstellers dessen Geburtsdatum und etwaige frühere Adressen an. Dieser Aufforderung kam der Antragsteller nicht nach und beschwerte sich bei uns. Das Verfahren der Auskunftei stellte nach unserer Prüfung keinen Verstoß gegen die Betroffenenrechte dar. Der Beschwerdeführer wandte sich daraufhin an das Verwaltungsgericht, vorerst mit einem Antrag auf Prozesskostenhilfe. Das Verwaltungsgericht lehnte diesen Antrag wegen fehlender Aussicht auf Erfolg ab.

In seinem Beschluss führte das Verwaltungsgericht aus, dass die Erfüllung eines Auskunftsanspruchs nach Art. 15 DSGVO abgelehnt werden kann, wenn sich die anspruchstellende Person weigert, ihr Geburtsdatum zur Klärung ihrer Identität mitzuteilen. Das gelte aber nur, wenn Verantwortliche begründete Zweifel an der Identität der antragstellenden Person haben. Zweifel an der Identität setzten voraus, dass die vorhandenen Daten auf eine bestimmte Identität hindeuteten, aber nach den Umständen Zweifel daran beständen, ob der Antragsteller tatsächlich die als Betroffener identifizierte Person ist.[19] Das Gericht stützt sich auf die Regelung des Art. 12 Abs. 6 DSGVO, wonach Verantwortliche, wenn sie begründete Zweifel an der Identität einer antragstellenden Person haben, zusätzliche Informationen anfordern können, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

Die Verantwortlichen müssen die Zweifel nach Auffassung des Gerichts darlegen. Die Mitwirkungsobliegenheit der antragstellenden Person sei in logischer Konsequenz notwendig, denn ohne deren Mitwirkung

[18] Verwaltungsgericht (VG) Berlin, Beschluss vom 24. April 2023, 1 K 227/22.
[19] Ebd., Rn. 10.

könnten Verantwortliche Identitätszweifel nicht entkräften. Dies diene dem Schutz der Daten jeder und jedes Einzelnen, sodass schlussendlich Informationen nur denjenigen zur Verfügung gestellt werden, die auch tatsächlich von der Datenverarbeitung betroffen sind.

An die Ausübung von Betroffenenrechten kann eine Mitwirkungspflicht geknüpft sein, wenn begründete Zweifel an der Identität der antragstellenden Person bestehen. In diesen Fällen kann die Anforderung eines Identitätsnachweises gerechtfertigt sein. Die Verantwortlichen müssen die Zweifel darlegen. Auch müssen die Grundsätze des Art. 5 DSGVO beachtet und eine nicht notwendige Neuerhebung von Daten vermieden werden. Eine allgemeine Identifizierungspflicht bei der Ausübung von Betroffenenrechten besteht nicht. Vielmehr ist in jedem Einzelfall zu prüfen, ob die Identität ohne weiteren Nachweis feststellbar ist, um den Anforderungen des Art. 12 Abs. 2 DSGVO zu genügen und die Ausübung der Rechte so einfach wie möglich zu machen.

3. Umfang einer Auskunftspflicht bei Videoüberwachung in Bahnen

In einem unserer Verfahren vor dem Verwaltungsgericht Berlin ging es um die Frage, ob betroffene Personen ihr Recht auf Kopien nach Art. 15 Abs. 3 Satz 1 DSGVO auch bei Videoaufnahmen in Bahnen geltend machen können.

Ein Bürger legte Beschwerde bei uns ein, nachdem ihm ein Verkehrsunternehmen keine Kopien nach Art. 15 Abs. 3 Satz 1 DSGVO über eine ihn mutmaßlich betreffende Videoüberwachung in einer Bahn übersenden wollte. Das Verkehrsunternehmen lehnte u. a. deswegen ab, da die vom Beschwerdeführer übersandte Beschreibung nicht geeignet gewesen sei, eine eindeutige Identifizierung seiner Person zu ermöglichen – zumal der Beschwerdeführer nach eigenen Angaben während der vermeintlichen Aufzeichnung eine Mund-Nasen-Bedeckung getragen hätte. Ebenso hätte einer Auskunftserteilung entgegengestanden, dass hierfür ein unverhältnismäßiger Aufwand hätte betrieben werden müssen: Das sich im laufenden Betrieb befindliche Fahrzeug hätte unter Umständen gestoppt, die Festplatten mit der Videoaufzeichnung hätten entnommen, die relevante Sequenz hätte ermittelt, der Beschwerdeführer hätte zweifelsfrei identifiziert und die Gesichter anderer aufgezeichneter Personen hätten unkenntlich gemacht werden müssen.

Gegen die von uns ausgesprochene Verwarnung klagte das Verkehrsunternehmen. Im Oktober entschied das

Verwaltungsgericht, dass unsere Verwarnung rechtswidrig sei, u. a. weil dem Beschwerdeführer kein Anspruch auf Kopie zugestanden habe.[20]

Das Gericht führte aus, dass der darlegungsbelastete Beschwerdeführer nicht nachgewiesen habe, dass er tatsächlich die betroffene Person i. S. d. Art. 15 DSGVO sei. Zwar habe er dem Verkehrsunternehmen einige Angaben mitgeteilt (wie Beförderungszeitraum, Zugnummer, Erscheinungsbild, Verhaltensweise sowie eine Kopie des Reisepasses), diese wären aber – auch im Hinblick darauf, dass der Beschwerdeführer zum Zeitpunkt der Videoüberwachung eine Mund-Nasen-Bedeckung getragen habe – nicht ausreichend. Die Übereinstimmung der Person des Auskunftsbegehrenden mit der auf den Videoaufnahmen aufgezeichneten Person sei ja nicht zweifelsfrei festzustellen. Es sei beispielsweise denkbar, dass ein Antragsteller derartige Angaben zu einer anderen Person mache, um an Videoaufzeichnungen dieser Person zu gelangen. Die Auskunftserteilung sei zudem für das Verkehrsunternehmen wegen des damit verbundenen unverhältnismäßigen Aufwands nicht zumutbar gewesen. Zwar sei in Art. 15 DSGVO keine ausdrückliche Ausnahme wegen unverhältnismäßigen Aufwands vorgesehen, § 275 Abs. 2 Bürgerliches Gesetzbuch (BGB) beinhalte jedoch den allgemeinen Rechtsgedanken, der auch in Erwägungsgrund 62 DSGVO zum Ausdruck komme. Danach dürfe eine Leistung verweigert werden, soweit diese einen Aufwand erfordert, der unter Beachtung des Gebots von Treu und Glauben, welches dem gesamten Verarbeitungsvorgang übergeordnet sei,[21] in grobem Missverhältnis zum Leistungsinteresse des Gläubigers stehe. Für das Gericht sei das offenkundig nur geringe Informations-interesse des Beschwerdeführers bei der insoweit vorzunehmenden Abwägung zu seinen Lasten zu berücksichtigen.

Wir sind anderer Meinung und haben gegen das Urteil Berufung eingelegt, die das Verwaltungsgericht bereits selbst wegen grundsätzlicher Bedeutung zugelassen hatte. Unter anderem vertreten wir die Auffassung, dass das Verkehrsunternehmen nach Art. 11 Abs. 2 Satz 2 Hs. 1 i. V. m. Abs. 1 DSGVO nachweisbelastet war und glaubhaft hätte machen müssen, es sei nicht in der Lage, den Beschwerdeführer zu identifizieren. Das Verkehrsunternehmen hatte die Videoaufzeichnungen stattdessen gar nicht auf Identifizierbarkeit geprüft; sie wurden ungesehen gelöscht. Der Beschwerdeführer hatte aber genau dargelegt, dass er zu einer bestimmten

[20] VG Berlin, Urteil vom 12. Oktober 2023, 1 K 561/21.
[21] Siehe Art. 8 Abs. 2 Satz 1 Charta der Grundrechte der Europäischen Union (GRCh); Art. 5 Abs. 1 lit. a DSGVO.

Uhrzeit im angegebenen Zug eine Mund-Nasen-Bedeckung mit einem eindeutigen Aufdruck trug. Auch genügt für einen Abgleich zwischen einem Passbild und den auf Videoaufnahmen trotz Maske erkennbaren Gesichtszügen einer Person (Stirn und Haare sowie insbesondere Augenpartie) regelmäßig die menschliche Wahrnehmung. Außerdem sehen wir für die Verweigerung der Auskunft aus Gründen eines „unverhältnismäßigen Aufwandes“ keinen Raum. Dieser kann unseres Erachtens auch tatsächlich nicht angenommen werden, da das Verkehrsunternehmen schließlich nach eigener Aussage auch in der Lage ist, Videoaufnahmen an die Strafverfolgungsbehörden herauszugeben.

Die Frage, ob Daten verarbeitende Stellen die Bereitstellung von Kopien nach Art. 15 Abs. 3 Satz 1 DSGVO aufgrund unverhältnismäßigen Aufwands verweigern können, war bisher nicht Gegenstand einer höchstrichterlichen Entscheidung. Art. 15 DSGVO sieht im Gegensatz zu etwa Art. 14 Abs. 5 lit. b DSGVO (auf den sich der vom Verwaltungsgericht herangezogene Erwägungsgrund 62 bezieht) gerade kein Verweigerungsrecht wegen eines unverhältnismäßig hohen Aufwands vor. Auch ist ein solches nicht in Art. 12 DSGVO geregelt. Ein Verweigerungsrecht besteht nach Art. 12 Abs. 5 Satz 2 lit. b DSGVO explizit nur dann, wenn der Antrag offenkundig unbegründet oder exzessiv ist. Allein der hohe Aufwand, den eine Auskunftserteilung ggf. mit sich bringen würde, macht einen Antrag noch nicht unbegründet oder exzessiv. Wenn Rechte Dritter mit dem Auskunftsanspruch der betroffenen Person kollidieren, sind nach der Rechtsprechung des EuGH[22] die Rechte und Freiheiten gegeneinander abzuwägen und – wenn möglich – Modalitäten der Übermittlung der Daten zu ergreifen, die die Rechte anderer nicht verletzen.[23] Solche Maßnahmen könnten sein, dass die Daten Dritter unkenntlich gemacht werden. In jedem Fall dürfen diese Erwägungen nicht dazu führen, „dass der betroffenen Person jegliche Auskunft verweigert wird“[24]. [25]

III. Bußgeldentscheidungen

1. Sammlung besonders schützenswerter Daten über Beschäftigte in der Probezeit

Arbeitgeber:innen dürfen personenbezogene Daten im Zusammenhang mit der Frage verarbeiten, ob und inwiefern Beschäftigte weiterbeschäftigt werden sollen.

[22]EuGH, Urteil vom 4. Mai 2023, C-487/21, sowie Urteil vom 22. Juni 2023, C-579/21.
[23]EuGH, Urteil vom 4. Mai 2023, C-487/21, Rn. 44.
[24]Siehe Erwägungsgrund (ErwGr.) 63 DSGVO.
[25]EuGH, Urteil vom 22. Juni 2023, C-579/21, Rn. 80.

Die verarbeiteten Daten müssen jedoch für den Zweck geeignet und erforderlich sein.

Auf Anweisung der Geschäftsführung eines Unternehmens erstellte eine Vorgesetzte kurz vor dem Ende der Probezeit ihrer Dienstkräfte eine Liste mit Informationen zu den Mitarbeiter:innen. Mit deren Hilfe sollte entschieden werden, welche Beschäftigten noch in der Probezeit eine Kündigung erhalten. Neben Stammdaten lieferte diese sog. Vorschlagsliste Einschätzungen über die Beschäftigten, Empfehlungen zu möglichen Kündigungen sowie eine als „Begründung" betitelte Tabellenspalte. In dieser Spalte wurden persönliche Äußerungen der Betroffenen zu deren sozialen und politischen Einstellung festgehalten und die Teilnahme an Psychotherapien oder ein etwaiges Interesse an der Gründung eines Betriebsrats dokumentiert. Die Informationen, bei denen es sich weitgehend um besonders schützenswerte Daten handelte – die zum großen Teil im Kontext der Dienstplanerstellung von den Mitarbeiter:innen mitgeteilt worden waren –, wurden ohne das Wissen der Betroffenen aufgezeichnet und an die Geschäftsführung des Unternehmens weitergegeben.

Die Datenverarbeitungen waren im vorliegenden Fall nicht rechtmäßig, da sie weder geeignet noch erforderlich waren, um den genannten Zweck der Evaluierung einer möglichen Probezeitkündigung zu erreichen. Es bestand kein Zusammenhang zwischen den gegenständlichen Informationen, die zu den Mitarbeiter:innen in der Liste gesammelt wurden, und deren Leistungen und Verhalten, sodass nicht erkennbar war, wie die Informationen für eine Leistungs- bzw. Verhaltensbewertung herangezogen werden konnten. Sofern zeitliche Kollisionen oder fehlende Flexibilität Grund für eine Auflistung bzw. spätere Kündigung gegeben hätten, wäre genau diese Feststellung ausreichend gewesen. Es bedurfte keiner näheren Begründung durch Informationen, die in diesem Zusammenhang keine Aussagekraft besitzen. Dies gilt in gesteigertem Maß für Informationen über die Gesundheit der Beschäftigten, die nur in eng begrenzten Ausnahmefällen im Beschäftigungsverhältnis verarbeitet werden dürfen. Die Verarbeitung solcher Daten ist nur dann zulässig, wenn die Eignung für die vorgesehene Tätigkeit auf Dauer oder in periodisch wiederkehrenden Abständen eingeschränkt, ein pünktlicher Arbeitsantritt nicht einzuhalten oder das Umfeld aufgrund möglicher Ansteckung gefährdet ist.[26] Dabei ist unerheblich, ob Informationen zur Gesundheit von den Beschäftigten selbst mitgeteilt werden. Die bloße Mitteilung ersetzt keine Einwilligung, nicht zuletzt deshalb, da nicht schon vorher über

[26]Siehe Bundesarbeitsgericht (BAG), Urteil vom 7. Juni 1984, 2 AZR 270/83.

den Zweck der späteren Verarbeitung der Mitteilung und über das Widerrufsrecht der Einwilligung aufgeklärt werden kann.

Die Ahndung dieser materiell-rechtlichen Verstöße sowie dreier weiterer Verstöße – wegen fehlender Beteiligung der betrieblichen Datenschutzbeauftragten bei der Erstellung der Liste, verspäteter Meldung einer Datenpanne und fehlender Erwähnung der Liste im Verfahrensverzeichnis – wurde von uns mit einem rechtskräftigen Bußgeldbescheid in Höhe von insgesamt 215.000 Euro bemessen, den wir im August dieses Jahres gegen das Unternehmen erlassen haben.

Vom Unternehmen gesammelte Informationen dürfen nur Rückschlüsse auf die Leistung und das Verhalten der Beschäftigten in Bezug auf ihr Arbeitsverhältnis zulassen. Folglich dürfen Arbeitgeber:innen nicht alle Informationen, die sie erhalten, insbesondere außerhalb des Erhebungskontextes weiterverwenden, selbst wenn ihnen diese durch die Beschäftigten selbst mitgeteilt worden sind. Es ist in jedem Einzelfall zu prüfen, ob die Erfassung, Speicherung oder Verwendung der jeweiligen Daten geeignet und erforderlich sind. Die Erforderlichkeit setzt voraus, dass ein legitimer Zweck verfolgt wird. Im Rahmen der Prüfung muss dann eine Abwägung zwischen den verschiedenen Interessen erfolgen.

2. Unbefugte Nutzung polizeiinterner Datenbanken
Ein großer Teil unserer Bußgeldverfahren betraf Polizeibeamt:innen, die unbefugt, d. h. zu nicht-dienstlichen Zwecken, personenbezogene Daten von Dritten aus den polizeiinternen Datenbanken abgerufen und teilweise auch weiterverwendet haben.

Die Polizei nutzt ihre Datenbank POLIKS[27] als Informationssystem für ihre gesetzlichen Aufgaben im Bereich der Strafverfolgung und der Gefahrenabwehr. In der Datenbank werden sowohl Vorgangsdaten als auch Daten von Beschuldigten, Straftäter:innen, Tatverdächtigen und Betroffenen sowie Daten von Opfern und Zeug:innen erfasst und gespeichert. Darunter befinden sich die vollständigen Namen, Geburtsdaten, Anschriften und Familienstand, aber auch Vorstrafen und Aussagen von Zeug:innen. Bedienstete der Polizei werden in regelmäßigen Abständen über die datenschutzrechtlichen Vorschriften informiert und darüber belehrt, dass es ihnen ausdrücklich untersagt ist, Daten aus POLIKS und anderen polizeilichen Informationssystemen

[27]Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung.

für private Zwecke zu nutzen. Dennoch wird der Zugang zu POLIKS immer wieder dazu missbraucht, Daten zu nichtdienstlichen Zwecken abzufragen.

In diesem Jahr haben wir 35 Verfahren gegen Polizeibeamt:innen eingeleitet und bereits insgesamt 32 Bußgelder verhängt, u. a. in den folgenden Fällen:

- Eine Polizeibeamtin fragte aus privatem Interesse Daten ihres Ex-Manns ab.
- Ein Polizeibeamter fragte als Geschädigter eines mutmaßlichen Wohnungseinbruchs den dazugehörigen Ermittlungsvorgang aus privatem Interesse ab.
- Ein Polizeibeamter fragte Daten eines seiner Dienstgruppe neu zugewiesenen Kollegen ab, um auszuschließen, dass er nicht bereits polizeilich mit diesem zu tun hatte.
- Ein Polizeibeamter schrieb eine Bürgerin, die er zuvor auf dem Parkplatz eines Lebensmittelhändlers gesehen hatte, über ihre private Handynummer an, die er der Datenbank mithilfe ihres Kfz-Kennzeichens entnahm.
- Ein Polizeibeamter schrieb eine Bürgerin über sein privates Mobiltelefon für einen Flirtversuch an, deren Nummer er im Rahmen eines Polizeieinsatzes dienstlich erhalten hatte.

All diese Datenverarbeitungen waren rechtswidrig, da die Abfragen der POLIKS-Datenbank nicht zur Erfüllung der gesetzlichen Aufgaben im Bereich der Strafverfolgung und der Gefahrenabwehr erfolgten. Es ist dabei unerheblich, welche Beweggründe der nichtdienstlichen Datenabfrage und Datennutzung zugrunde lagen.

Nach Mitteilung der Polizei sind von den von der Berliner Beauftragten für Datenschutz und Informationsfreiheit im berichtspflichtigen Zeitraum verhängten 32 Geldbußen insgesamt 14 Polizeidienstkräfte wegen unbefugter POLIKS-Abfragen betroffen. Die Namen dieser Personen sind der Polizei Berlin im Nachgang von der Berliner Beauftragten für Datenschutz und Informationsfreiheit mitgeteilt worden. Die Polizei prüft nun, ob ggfs. - zusätzlich zu den Bußgeldverfahren - disziplinarrechtliche Verfahren einzuleiten sind.

Die Polizei Berlin führt regelmäßig Kontrollen der Abfragen durch ihre Dienstkräfte durch und passt das Kontrollkonzept an, wenn Verbesserungspotenzial erkannt wird.
Auf grundlegende Probleme in diesem Zusammenhang weist die Berliner Beauftragte für Datenschutz und Informationsfreiheit nicht hin.

3. Transparenz bei automatisierter Ablehnung eines Kreditkartenantrags

Wegen mangelnder Transparenz über eine automatisierte Einzelentscheidung haben wir gegen eine Bank ein Bußgeld in Höhe von 300.000 Euro verhängt. Die Bank hatte sich geweigert, einem Kunden nachvollziehbare Auskünfte über die Gründe der automatisierten Ablehnung seines Kreditkartenantrags zu erteilen. Das Unternehmen hat umfassend mit uns kooperiert und den Bußgeldbescheid akzeptiert.

In diesem Bußgeldfall fragte das automatisierte Kreditkartenvergabesystem der Bank verschiedene Daten zu den Personalien, zum Einkommen und zum Beruf des antragstellenden Beschwerdeführers ab. Anhand dieser und zusätzlicher Informationen aus externen Quellen lehnte der Algorithmus des Vergabesystems den Antrag des Kunden ohne besondere Begründung ab. Da der Beschwerdeführer über einen guten Schufa-Score und ein regelmäßiges hohes Einkommen verfügte, bezweifelte er die automatisierte Ablehnung seines Antrags. Auf Nachfrage machte die Bank lediglich pauschale und nicht auf den Einzelfall bezogene Angaben zum Scoring-Verfahren. Sie weigerte sich, dem Betroffenen mitzuteilen, warum sie in seinem Fall von einer schlechten Bonität ausging. Für den Beschwerdeführer war somit nicht nachvollziehbar, auf welcher Datenbasis die Ablehnung beruhte und anhand welcher Kriterien sein Kreditkartenantrag abgelehnt worden war. Ohne diese auf seinen konkreten Fall bezogene Begründung war es ihm darüber hinaus nicht möglich, die automatisierte Einzelentscheidung sinnvoll anzufechten. Daraufhin beschwerte er sich bei uns.

Wir haben festgestellt, dass die Bank in diesem Fall gegen die Datenschutz-Grundverordnung (DSGVO) verstoßen hat.[28] Eine automatisierte Entscheidung ist eine Entscheidung, die ein IT-System ausschließlich auf Grundlage vorher festgelegter Algorithmen ohne menschliches Zutun trifft. Für diesen Fall sieht die DSGVO spezielle Transparenzpflichten vor: So müssen personenbezogene Daten in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden. Zudem haben betroffene Personen einen Anspruch auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung. Beantragen betroffene Personen bei den Verantwortlichen eine Auskunft, muss diese aussagekräftige Informationen über die Hintergründe der automatisierten Entscheidung enthalten.

Bei der Bußgeldzumessung berücksichtigten wir insbesondere den hohen Umsatz der Bank sowie die vorsätzliche Ausgestaltung des Antrags- und Auskunftsprozesses. Als bußgeldmindernd wurde u. a. eingestuft, dass das Unternehmen den Verstoß eingeräumt sowie Änderungen an den Prozessen bereits vorgenommen und weitere Verbesserungen angekündigt hat.

Wenn Unternehmen automatisiert Entscheidungen treffen, sind sie verpflichtet, diese stichhaltig und nachvollziehbar zu begründen. Die Betroffenen müssen in

[28] Siehe Art. 22 Abs. 3 i. V. m. Art. 22 Abs. 2 lit. a, Art. 5 Abs. 1 lit. a, Art. 15 Abs. 1 lit. h DSGVO.

der Lage sein, die automatisierte Entscheidung nachzuvollziehen. Eine Bank ist verpflichtet, die Kund:innen bei automatisierten Entscheidungen über einen Kreditkartenantrag von den ausschlaggebenden Gründen der Ablehnung zu unterrichten. Hierzu zählen konkrete Informationen zur Datenbasis und zu den Entscheidungsfaktoren sowie die am Einzelfall belegten Kriterien für die Ablehnung.

4. Videoüberwachung durch die Steckdose

Der vorliegende Bußgeldfall zeigt, dass Unternehmen Videoüberwachung häufig leichtfertig und ohne fundierte Begründung einsetzen, um Beschäftigte zu überwachen. Im konkreten Fall haben wir gegen ein Unternehmen ein Bußgeld in Höhe von 4.000 Euro verhängt, weil es für mindestens einen Monat vorsätzlich drei Praktikant:innen an ihrem Arbeitsplatz durch in Steckdosen versteckte WiFi-Kameras überwacht hatte.

Die Kameras waren in drei Räumen des Unternehmens an in Augenhöhe liegenden Steckdosen angebracht, ohne dass die Betroffenen vorab über die Videoüberwachung in Kenntnis gesetzt worden waren. Das Unternehmen teilte uns mit, dass die Praktikant:innen zum Zweck der effektiven Sicherung des Urheberrechts gefilmt worden waren, worauf auch eine Klausel in den Arbeitsverträgen der Praktikant:innen hingewiesen hatte.

Zur Erbringung der Arbeitsleistung oder zur Sicherung des Urheberrechts war die Videoüberwachung jedoch nicht erforderlich. Erforderlich ist eine Maßnahme dann, wenn etwa eine Gefährdungslage hinreichend durch Tatsachen oder die allgemeine Lebenserfahrung belegt ist und dieser nicht ebenso gut durch eine andere, gleich wirksame, aber schonendere Maßnahme begegnet werden kann.[29] Das Unternehmen konnte nicht darlegen, warum es für den Urheberrechtsschutz nicht mildere, genauso geeignete Mittel ergriffen hat. Die Videoüberwachung war auch im engeren Sinne nicht verhältnismäßig, denn eine ständige Videoüberwachung von Arbeitsplätzen ist vor dem Hintergrund des Rechts der Beschäftigten auf Schutz der sie betreffenden personenbezogenen Daten grundsätzlich unzulässig.[30] Dies gilt insbesondere, wenn sie – wie im vorliegenden Fall – verdeckt stattfindet, sodass sie gänzlich den vernünftigen Erwartungen[31] der Praktikant:innen im Arbeitsumfeld widerspricht. Angesichts des Machtungleichgewichts zwischen Unternehmen und Prakti-

[29]Siehe Bundesverwaltungsgericht (BVerwG), Urteil vom 27. März 2019, 6 C 2.18, Rn. 26.
[30]Siehe BAG, Urteil vom 20. Oktober 2016, 2 AZR 395/15, NZA 2017, S. 443.
[31]Siehe ErwGr. 47, Satz 1 DSGVO.

kant:innen war es aus unserer Sicht auch ausgeschlossen, dass sich die Praktikant:innen mit der Videoüberwachung aus freien Stücken vertraglich einverstanden erklärt hatten.

Die Videoüberwachung von Räumen, in denen Beschäftigte arbeiten, sollte datenschutzrechtlich grundsätzlich als Ultima Ratio zum Schutz von Eigentum oder vor Straftaten angesehen werden. Für die Zulässigkeit von Videoüberwachung bedarf es konkreter Anhaltspunkte zum Vorliegen einer tatsächlichen Gefährdungslage, die über das allgemeine Lebensrisiko hinausgeht und der nicht mit anderen Mitteln begegnet werden kann. Zudem gibt es geschützte Bereiche, wie etwa Umkleide-kabinen, Pausen-räume und Toiletten, die grundsätzlich nicht überwacht werden dürfen.

IV. Digitalisierung von Schule und Verwaltung

1. Datenschutzrechtliche Risikobewertung von IKT-Basisdiensten und IT-Fachverfahren

Die zentrale Bereitstellung und Standardisierung der landesweit genutzten Informations- und Kommunikationstechnologie (IKT) sind grundlegende Ziele der Verwaltungsdigitalisierung. Die zuständigen Stellen in der Hauptverwaltung entwickeln zu diesem Zweck verfahrensunabhängige IKT-Basisdienste und spezifische IT-Fachverfahren, die sie der Verwaltung zur Verfügung stellen. Die Datenschutz-Grundverordnung (DSGVO) und das Berliner Datenschutzgesetz (BlnDSG) geben für solche Digitalisierungsprojekte klare Vorgaben. Wir unterstützen die Verwaltung in diesem Bereich und entwickeln gemeinsam einen Standardprozess zur Erfüllung der Anforderungen des Datenschutzes.

Das E-Government-Gesetz Berlin (EGovG Bln) sieht vor, dass die mittlerweile bei der Senatskanzlei angesiedelte IKT-Steuerung[32] verfahrensunabhängige Basisdienste zur Verfügung stellt und diese verbindlich durch die Verwaltung zu nutzen sind.[33] Der technische Betrieb wird regelmäßig durch das IT-Dienstleistungszentrum Berlin (ITDZ) erbracht. Die öffentlichen Stellen des Landes sind rechtlich zur Abnahme dieser Basisdienste verpflichtet.[34] Einsatz und Fortentwicklung der bereichsspezifischen IT-Fachverfahren werden demgegenüber nach dem EGovG Bln von den fachlich zuständigen Behörden – in der Regel den fachlich zuständigen Senatsverwaltungen – verantwortet, die da-

[32]Siehe §§ 20 ff. EGovG Bln.
[33]Siehe z. B. § 10 Abs. 2 Satz 3, § 12 Abs. 2 EGovG Bln.
[34]§ 24 Abs. 2 Satz 2 EGovG Bln.

bei die Vorgaben der zentralen IKT-Steuerung einzuhalten haben.[35] Die datenschutzrechtliche Verantwortung wird dann jeweils bei der einsetzenden Behörde liegen, die personenbezogene Daten zur Erfüllung ihrer Aufgaben mittels der Basisdienste und Fachverfahren verarbeitet.

Zentrale IKT-Basisdienste, bei deren Einführung und Betrieb wir die Beteiligten beraten, sind insbesondere die „Digitale Akte", der „Digitale Antrag" oder das „besondere elektronische Behördenpostfach" (beBPo). Auch hinsichtlich des geplanten Basisdienstes „Digitale Kollaboration" wurden wir um Beratung gebeten. Im Bereich der IT-Fachverfahren unterstützen wir beispielsweise die Senatsverwaltung für Finanzen (SenFin) bei der Weiterentwicklung der „Integrierten Personalverwaltung" (IPV) oder das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) bei der datenschutzrechtlichen Prüfung und Dokumentation der Softwareplattform VOIS (Verwalten, Organisieren, Integrieren, Systematisieren). Über VOIS werden mehrere IT-Fachverfahren aus dem Bereich des Meldewesens unter Nutzung derselben Basiskomponenten betrieben.

Durch die Einführung und den Betrieb von IKT-Basisdiensten und IT-Fachverfahren erfolgt die Verarbeitung personenbezogener Daten zunehmend vollständig automatisiert. Dabei entstehen regelmäßig datenschutzrechtliche Risiken, die die jeweils für die Verarbeitung verantwortliche Stelle vor der Inbetriebnahme eines Dienstes bzw. Verfahrens zu überprüfen und einzuschätzen hat. Mit geeigneten technischen und organisatorischen Maßnahmen müssen die Risiken eingedämmt werden, um sicherzustellen und nachweisen zu können, dass die Verarbeitung im Einklang mit der DSGVO erfolgt.[36] § 26 Abs. 2 BlnDSG verlangt von den projektverantwortlichen Stellen, die festgestellten Risiken in einem Datenschutzkonzept zu dokumentieren. Ergibt diese Risikoanalyse, dass die geplante automatisierte Verarbeitung personenbezogener Daten durch einen IKT-Basisdienst oder ein IT-Fachverfahren ein hohes Risiko für die betroffenen Bürger:innen und Mitarbeitenden begründet, so ist nach Art. 35 DSGVO eine Datenschutz-Folgenabschätzung durchzuführen.[37]

Die Erstellung von Datenschutzkonzepten und Datenschutz-Folgenabschätzungen ist kein bürokratischer

[35] Siehe § 20 Abs. 3 Satz 1 und 2 EGovG Bln.
[36] Art. 24, Art. 32 DSGVO.
[37] Informationen zur Erstellung einer Datenschutz-Folgenabschätzung finden sich auf unserer Website unter https://www.datenschutz-berlin.de/themen/unternehmen/datenschutz-folgenabschaetzung/.

„Papierkram“. Vielmehr handelt es sich um die Dokumentation der durchgeführten Prüfung und Risikoabschätzung mit den daraus abgeleiteten Maßnahmen. Dies erfordert eine Expertise in rechtlicher wie technischer Hinsicht. Wir beobachten, dass die notwendige Kompetenz in den für die Einführung und Entwicklung von IKT-Basisdiensten und IT-Fachverfahren verantwortlichen öffentlichen Stellen der Verwaltung und bei den implementierenden Behörden vielfach noch nicht vorhanden ist. Vor diesem Hintergrund beauftragen die Verwaltungen bzw. das ITDZ regelmäßig externe Beratungsunternehmen mit der Erstellung von Datenschutzkonzepten. Wir stellen im Rahmen unserer Beratungen immer wieder fest, dass die vorgelegten Dokumente weder eine ausreichende Analyse der entstehenden Datenschutzrisiken noch geeignete Vorschläge für Abhilfemaßnahmen enthalten. Häufig können die verantwortlichen Behörden in Ermangelung der entsprechenden Expertise weder einen ausreichend präzisen Auftrag an externe Beratungsunternehmen formulieren noch eine entsprechende Qualitätskontrolle der Prüfungen und erstellten Dokumentationen vornehmen. Im Ergebnis führt dies dazu, dass bestehende Datenschutzrisiken nicht oder nicht rechtzeitig erkannt werden und aufwändige Anpassungen im Verlauf des Projekts vorgenommen werden müssen. Dadurch bedingte Zeitverzögerungen ließen sich vermeiden, wenn Datenschutzaspekte möglichst von Projektbeginn an in den Blick genommen würden.

In der Verwaltung muss neben der Digitalisierungsauch eine entsprechende Datenschutzkompetenz aufgebaut werden. Gemeinsam mit den zuständigen Behörden und insbesondere mit dem ITDZ sind wir im Austausch, um einen Datenschutz-Standardprozess zu entwickeln, der die Datenschutzprüfung anleiten und für sämtliche Verwaltungen nutzbar sein soll. Wir halten dies für einen guten Weg, die Erfüllung der Anforderungen des Datenschutzes in die Projekte der Verwaltungsdigitalisierung von Anfang an effektiver und zielführender einzufädeln.

Bei der Entwicklung und Einführung von IKT-Basisdiensten und IT-Fachverfahren müssen die verantwortlichen Stellen das dabei entstehende Datenschutzrisiko prüfen und entsprechende Abhilfemaßnahmen ergreifen. Diese Risikoanalyse ist in einem Datenschutzkonzept zu dokumentieren. Wir beraten und unterstützen die Verwaltung dabei und entwickeln einen Datenschutz-Standardprozess und skalierbare Lösungsansätze, die die Verwaltung mittelfristig in die Lage versetzen sollen, diese Aufgaben effektiver und zielführender zu erledigen. Insgesamt muss in der Verwaltung aber neben der Digitalisierungskompetenz auch mehr Datenschutzexpertise aufgebaut werden.

2. Anschluss der Digitalen Akte an das Jugend-Fachverfahren

Damit die Verwaltung tatsächlich vollständig digital arbeiten kann, bedarf es einer Anbindung der zahlreichen in der Verwaltung zum Einsatz kommenden IT-Fachverfahren an die Digitale Akte. Im Rahmen der Pilotierung der Anbindung des Fachverfahrens in den Jugendämtern hat uns die Senatsverwaltung für Bildung, Jugend und Familie (SenBJF) frühzeitig um Beratung gebeten.

Seit Ende des vergangenen Jahres führt die Senatsverwaltung ein Pilotprojekt zur Anbindung der IT-Fachverfahren über Schnittstellen an den Basisdienst der Digitalen Akte durch, welches wir von Beginn an mit der Klärung der rechtlichen und technischen Fragen unterstützen. Die IT-Fachverfahren für den Bereich der Kinder- und Jugendhilfe werden von sämtlichen Jugendämtern genutzt. Der Einsatz dieser IT-Fachverfahren wird von der Senatsverwaltung zentral für die Bezirke und das Landesjugendamt zur Verfügung gestellt und gesteuert. Dazu betreibt die Senatsverwaltung eine IT-Plattform namens „Integrierte Software Berliner Jugendhilfe“ (ISBJ), über die für den Jugendhilfebereich beispielsweise das IT-Fachverfahren „SoPart“ bereitgestellt wird, dessen Einführung wir seinerzeit ebenfalls begleitet haben.

IT-Fachverfahren wie „SoPart“ verfügen über dedizierte Rollen- und Berechtigungskonzepte. Diese gewährleisten, dass nur berechtigte Personen auf die in den IT-Fachverfahren verarbeiteten Informationen und personenbezogenen Daten zugreifen können. Soll nun ein solches IT-Fachverfahren an den IKT-Basisdienst Digitale Akte angebunden werden, so müssen beispielsweise die Zugriffsrechte an den Dokumenten, die in den Verfahren erzeugt werden, entsprechend in der Digitalen Akte gesetzt werden. Andernfalls könnten die Vorgaben des Rechte- und Rollenkonzepts ganz einfach durch Aufruf von Schriftgut in der Digitalen Akte umgangen werden.

Für die Synchronisation der Berechtigungen zwischen den IT-Fachverfahren und dem Basisdienst ist es erforderlich, eine Softwarelösung zu schaffen, die den Abgleich automatisiert. Dies wird dadurch erschwert, dass es unterschiedliche Verzeichnisdienste in den einzelnen Behörden gibt, aus denen die Nutzerkonten und etwaige Berechtigungen in den Fachverfahren abgeleitet werden. Ein manueller Abgleich ist aufgrund seiner Fehleranfälligkeit angesichts der Komplexität der Berechtigungssysteme ausgeschlossen. Die Senatsverwaltung entwickelt daher Lösungsansätze, die wir im

Rahmen unserer Beratungen mit allen Beteiligten erörtern. Wir halten es für zielführend, einen berlinweit einheitlichen Ansatz zu verfolgen und die entsprechenden Synchronisationsverfahren zu standardisieren.

Die Anbindung der IT-Fachverfahren an den zurzeit eingeführten IKT-Basisdienst Digitale Akte ist ein zentraler Bestandteil der Verwaltungsdigitalisierung. Dabei müssen insbesondere die in den Fachverfahren gesetzten Berechtigungen auch in der Digitalen Akte nachgezogen werden, damit die Vorgaben des Rechte- und Rollenkonzepts des Fachverfahrens nicht umgangen werden können. Dazu sollten berlinweit einheitliche Synchronisationsverfahren eingesetzt werden. Wir stehen der Verwaltung mit unserer Expertise beratend zur Seite.

3. Beratungsprozess mit der Bildungsverwaltung zur Schuldigitalisierung

Angesichts der besonderen Bedeutung der Klärung datenschutzrechtlicher Fragen bei der Schuldigitalisierung haben wir uns Anfang des Jahres mit der Bildungsverwaltung verständigt, einen regelmäßigen fachlichen Austausch zwischen unseren Behörden durchzuführen. Ziel soll es sein, frühzeitig Datenschutzfragen bzw. -risiken bei der Durchführung einzelner Projekte der Schuldigitalisierung zu identifizieren und miteinander zu erörtern.

Wir haben immer wieder betont, dass die frühzeitige Einbeziehung unserer Behörde in die konkrete Projektplanung notwendig ist, um die datenschutzrechtlichen Möglichkeiten ausloten, aber auch rechtliche und technische Grenzen aufzeigen zu können. Dazu haben wir nun einen entsprechenden Dialog mit der Bildungsverwaltung begonnen und werden diesen im kommenden Jahr fortsetzen. Beispielhaft zu nennen sind neben dem bereits etablierten und fortgesetzten Austausch zur Weiterentwicklung der Berliner Lehrkräfte-Unterrichts-Schuldatenbank (LUSD)[38] die neu aufgenommenen Beratungen bei der Festlegung von Kriterien für eine Positivliste datenschutzkonformer Softwareprodukte für Schulen, deren Erstellung der Bildungsverwaltung gesetzlich obliegt,[39] sowie der Austausch zur Anpassung der Rechtsgrundlagen.

Den mit der Bildungsverwaltung begonnenen Austausch zu den datenschutzrelevanten Themen der Schuldigitalisierung werden wir im kommenden Jahr weiter optimieren. Uns ist es wichtig, unsere Expertise

[38] Siehe JB 2022, 4.4.6.
[39] Siehe § 7 Abs. 2a Satz 2 Schulgesetz (SchulG).

möglichst von Beginn an in die Projektplanungen einzubringen, um zu verhindern, dass die Weichen im Projektverlauf noch einmal neu ausgerichtet werden müssen. Unsere Erwartung ist, dass der strukturierte Austausch dazu führt, uns in Zukunft frühzeitig mit konkreten und belastbaren Informationen in Projekte einzubinden, damit wir die Bildungsverwaltung dann mit aussagekräftigen und klaren Hinweisen beraten können.

4. Einsatz von Microsoft 365 an Schulen

Die Schulen setzen nicht nur die von der Bildungsverwaltung zur Verfügung gestellten digitalen Werkzeuge ein, sondern orientieren sich auch selbst an den auf dem Markt angebotenen Produkten. Da die Schulen selbst datenschutzrechtlich verantwortlich sind, können sie auch über deren Einsatz entscheiden. Allerdings sind sie dabei in der Verantwortung, einen datenschutzkonformen Einsatz sicherzustellen und die notwendigen Prüfungen vorzunehmen.

Mit dem Lernraum Berlin wurde ein Lernmanagementsystem geschaffen, das datenschutzkonforme Anwendungen zur Unterrichtsplanung und -durchführung, etwa mittels des Videokonferenzsystems BigBlueButton, für die Berliner Schulen anbietet und dabei auf Open-Source-Lösungen setzt. Für die Schulen ist es transparent und bewertbar, ob und wie personenbezogene Daten verarbeitet und verwendet werden, insbesondere dass dies nur für Zwecke der Schulen geschieht. Schwierig wird es hingegen beim Einsatz von digitalen Werkzeugen, deren datenschutzgerechter Einsatz für die Schulen nicht prüfbar ist und nicht nachgewiesen werden kann. In der Praxis spielt dies etwa beim schulischen Einsatz von Microsoft 365 (MS 365) eine Rolle, zu dem auch die Kommunikationssoftware Microsoft Teams zählt. Das Problem besteht hier darin, dass das Unternehmen Microsoft personenbezogene Daten nicht nur im Rahmen des ihm erteilten Auftrags für die Verantwortlichen, d. h. für die jeweiligen Schulen, sondern darüber hinausgehend auch für eigene Zwecke verarbeitet.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat eine Arbeitsgruppe eingesetzt, die Gespräche mit Microsoft geführt hat. Nach mehrjährigen Verhandlungen kam diese Arbeitsgruppe Ende des vergangenen Jahres zu dem Ergebnis, dass sich ein Einsatz von MS 365 ohne erhebliche Anpassungen in den zugrunde liegenden Verträgen nicht datenschutzkonform abbilden

lässt.[40] Nach dem Bericht der Arbeitsgruppe[41] legt Microsoft insbesondere nicht vollumfänglich offen, welche Verarbeitungen im Einzelnen im Auftrag der Kund:innen und welche zu eigenen Zwecken stattfinden. Da das Unternehmen die personen-bezogenen Daten von Schüler:innen, Eltern und Beschäftigten als Auftragsverarbeiter nur im Dienst der Schulen verarbeiten darf, besteht für das Vorgehen, die anfallenden personenbezogenen Daten auch für die eigenen Zwecke zu verarbeiten, keine rechtliche Grundlage.

Um einen datenschutzkonformen Einsatz von MS 365 in Schulen zu erreichen, müssten die Vereinbarungen der Schulen mit Microsoft zunächst anhand der im Bericht der DSK-Arbeitsgruppe getroffenen Feststellungen überprüft und Vereinbarungen sowie Datenverarbeitungen entsprechend angepasst werden. Die Schulen als datenschutzrechtlich verantwortliche Stellen, die Microsoft als Auftragnehmer beauftragen, müssen dafür Sorge tragen, dass personenbezogene Daten von Schüler:innen, Eltern und Beschäftigten nur im Rahmen des Auftrags verarbeitet werden.

Insbesondere vor dem Hintergrund der nunmehr mit der Digitale Lehr- und Lernmittelverordnung (DigLLV) geschaffenen Vorschrift zum Einsatz von Audio- und Videokonferenzdiensten[42] wird sich die Schulverwaltung mit der Verwendung von MS 365 in Berliner Schulen auseinandersetzen müssen. Die DigLLV sieht nämlich vor, dass andere als die von der Schulaufsichtsbehörde zur Verfügung gestellte Audio- oder Videokonferenzdienste nur mit deren Genehmigung eingesetzt werden dürfen. Wir haben die Bildungsverwaltung auf die datenschutzrechtliche Perspektive beim Einsatz von MS 365 im schulischen Kontext hingewiesen und angeboten, bei Bedarf beratend zur Verfügung zu stehen. Aus unserer Sicht ist die Fortentwicklung des eigenen Lernmanagementsystems auf Open-Source-Basis der zielführendere Weg in Richtung einer digitalen Souveränität im Bildungsbereich.

Die Schulen sind verantwortlich für die Einhaltung aller datenschutzrechtlichen Vorschriften und müssen die datenschutzrechtliche Zulässigkeit selbst prüfen. § 4 Abs. 2 DigLLV regelt die Genehmigungspflicht für Audio- und Videokonferenzdienste, die nicht von der Schulaufsichtsbehörde zur Verfügung gestellt werden. Microsoft 365 ist jedoch ein umfassenderes Produkt, das neben einem Audio- und Videokonferenzdienst auch weitere umfassendere Komponenten enthält, sodass § 4 Abs. 2 DigLLV nur einen kleinen Teil des Produkts unter die Genehmigungspflicht stellt. Im regelmäßigen Austausch zwischen der Senatsverwaltung für Bildung, Jugend und Familie und der Berliner Beauftragten für Datenschutz und Informationsfreiheit werden Landeslösungen für den Einsatz von Microsoft 365 besprochen; die Diskussion hierüber befindet sich im Prozess.

[40] Siehe DSK, Festlegung vom 24. November 2022, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf.
[41] Siehe DSK-Arbeitsgruppe „Microsoft-Onlinedienste“, Bericht vom 2. November 2022, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf. Maßgeblicher Prüfungsgegenstand war der zunächst in der englischen Entwurfsfassung zur Verfügung gestellte „Datenschutznachtrag zu den Produkten und Services von Microsoft – letzte Aktualisierung: 15. September 2022“.
[42] § 4 Abs. 2 DigLLV.

V. Inneres und Justiz

1. Löschmoratorien bei Staatsanwaltschaft, Polizei und Verfassungsschutz

Parlamentarische Untersuchungsausschüsse ermöglichen der Legislative, mögliche Missstände in Regierung und Verwaltung aufzuklären und damit eine wichtige Kontrollfunktion über die Exekutive auszuüben. Auch die parlamentarische Opposition kann gleichberechtigt an den Untersuchungen teilnehmen und durch Beweisanträge wie Aktenvorlagen und Zeugenvernehmungen Einfluss nehmen. Zur Wahrnehmung dieser Rechte und um etwaige Untersuchungen nicht zu gefährden, wird die Auf-bewahrung von behördlichen Unterlagen angeordnet, die bereits löschreif sind. Die Umsetzung dieser Löschmoratorien bei der Polizei begleitet uns seit geraumer Zeit.[43] Unsere Prüfungen haben wir nun auch auf die Staatsanwaltschaften und den -Verfassungsschutz ausgeweitet.

Im Jahre 2021 wurde erstmals eine gesetzliche Norm als Rechtsgrundlage für die Datenweiterverarbeitung zu parlamentarischen Kontrollzwecken erlassen.[44] Die Vorschrift erlaubt, dass personenbezogene Daten – auch abweichend von anderen -Vorschriften über deren Löschung oder Vernichtung – für einen befristeten Zeitraum nicht gelöscht oder vernichtet werden müssen; dies aber nur, soweit es im Rahmen der Mitwirkung an der Erfüllung der Aufgaben eines parlamentarischen Untersuchungsausschusses erforderlich ist.

Die Polizei bewahrt seit 2013 inzwischen etwa 7,5 Millionen Vorgänge allein aus POLIKS auf, die ohne Löschmoratorien nicht mehr gespeichert wären. Darunter befinden sich 2,25 Millionen Vorgänge, die nicht aufgeklärt werden konnten, 30.000 Vorgänge, die vor 1995 angelegt wurden, und 400.000 aufgenommene Verkehrsunfälle.[45] Diese Vorgänge werden derzeit für einen Untersuchungsausschuss zur rechtsextremistischen Straftatenserie in Neukölln in den Jahren 2009 bis 2021[46] vorgehalten sowie für Untersuchungsausschüsse zum NSU-Komplex in Bayern[47] und in Mecklenburg-Vorpommern[48].

Bereits im Jahresbericht 2019 hatte die Berliner Beauftragte für Datenschutz und Informationsfreiheit die Speicherpraxis der Polizei mit Blick auf die Löschmoratorien kritisiert und eine Vorauswahl der aufzubewahrenden Vorgänge anhand plausibler Kriterien in Bezug auf die Untersuchungsgegenstände angemahnt. Allerdings hat sich an der Sachlage und ihrer rechtlichen Beurteilung durch den Senat seitdem nichts geändert, so dass zunächst auf die seinerzeitige Stellungnahme des Senats verwiesen wird. Danach handelt die Polizei bei der

[43] Siehe JB 2019, 3.2.
[44] Siehe § 20a Berliner Datenschutzgesetz (BlnDSG).
[45] Die Zahlen entsprechen dem Stand vom November 2022.
[46] Siehe Abgeordnetenhaus, Drs. 19/0279; die Speicherung der Datensätze ist derzeit bis zum 31. März 2025 befristet.
[47] Siehe Bayerischer Landtag, Drs. 18/22844; die Speicherung der Datensätze war bis zum 31. Dezember 2023 befristet.
[48] Siehe Landtag Mecklenburg-Vorpommern, Drs. 8/80; die Speicherung der Datensätze ist derzeit bis zum 31. Dezember 2024 befristet.

Zwar sind die Daten seit 2019 in einen zugangsbeschränkten Schutzbereich verschoben. Gleichwohl handelt es sich um eine sehr weitgehende Datenan-

Umsetzung der Löschmoratorien aus den nachstehenden Gründen nach vertretbarer Ansicht rechtskonform.

Nach dem für - im Hinblick auf Untersuchungsausschüsse angeordnete - Löschmoratorien vorgegebenen rechtlichen Rahmen dürfen Daten und Akten nur dann gelöscht bzw. vernichtet werden, wenn ein Bezug zum jeweiligen Untersuchungsgegenstand ausgeschlossen ist. Hierfür trifft die Verwaltung die Darlegungslast. Umgekehrt ist die Aufbewahrung derjenigen Daten und Akten erforderlich, bei denen ein Bezug zum jeweiligen Untersuchungsgegenstand möglich erscheint.

Mit Blick auf den Umfang der in Rede stehenden parlamentarischen Untersuchungsgegenstände und die Reichweite der Beweisbeschlüsse der noch aktiven Untersuchungsausschüsse zur rechtsextremistischen Straftatenserie in Neukölln in den Jahren 2009 bis 2021 sowie zum NSU-Komplex in Bayern und in Mecklenburg-Vorpommern, die in ihrer Gesamtheit auf eine Ausleuchtung des gesamten Umfelds, der chronologischen Entwicklung und länderübergreifender Zusammenhänge der jeweiligen Verbrechensserie zielen, lässt sich gerade ein möglicher Bezug polizeilicher Daten zu einem der in Rede stehenden Untersuchungsgegenstände eben nicht von vornherein mit der erforderlichen Sicherheit auszuschließen.

Angesichts des hohen verfassungsrechtlichen Ranges des parlamentarischen Untersuchungsrechts sieht sich die Polizei daher verpflichtet, zur Vermeidung potentiell fehlerhafter Einschätzungen, die zu schwerwiegenden, irreversiblen Beweismittelverlusten führen können, die Datenlöschung vollständig auszusetzen. Die an sich löschreifen Daten wurden in einen besonderen Schutzbereich verschoben und sind in ihrem Zugriff beschränkt. Es ist durch technische und organisatorische Maßnahmen sichergestellt, dass sie nur noch für Zwecke der Untersuchungsausschüsse, nicht aber für die operative Polizeiarbeit genutzt werden können. Hierin sieht der Senat einen hinreichenden Ausgleich zwischen der Gewährleistung einer effektiven Erfüllung des verfassungsrechtlich verbrieften Rechts des Parlaments zur Kontrolle der Exekutive einerseits und der Wahrung datenschutzrechtlicher Belange der betroffenen Personen andererseits.

sammlung von löschreifen Vorgängen. Zu berücksichtigen ist, dass die Polizei die Pflicht hat, dem Parlament Rede und Antwort über ihre Arbeit zu stehen. Auch ist grundsätzlich nachvollziehbar, dass nicht immer von vornherein feststellbar ist, ob ein Einzelvorgang für eine spätere parlamentarische Kontrolle relevant werden könnte. Gleichzeitig stellt die Vorschrift in § 20a Abs. 2 BlnDSG die Aufbewahrung der Daten unter den Vorbehalt, dass das Nichtlöschen erforderlich ist, um an der Erfüllung der Aufgaben eines Untersuchungsausschusses mitzuwirken. Es muss daher mindestens nachvollziehbar sein, nach welchen Kriterien die Polizei eine Einteilung in relevante und irrelevante Datensätze vorgenommen hat. Im Zweifel sind Kriterien in Zusammenarbeit mit den anfragenden Parlamenten festzulegen. Anders lässt sich eine unzulässige Kettenaufbewahrung der Datensätze nicht verhindern. Nach unseren Prüfungen bei der Polizei ist dies bisher nicht im ausreichenden Maß geschehen. Bereits im Februar 2022 haben wir der Polizei mitgeteilt, dass wir eine Vorauswahl der aufzubewahrenden Vorgänge anhand plausibler Kriterien für erforderlich halten, denn die Ermächtigungsnorm beschränkt den inhaltlichen und zeitlichen Umfang des Löschmoratoriums. Die Polizei hält stattdessen eine unterschiedslose Aufbewahrung für erforderlich.

Unsere Prüfungen bei den Staatsanwaltschaften haben ergeben, dass diese in der Lage waren, ihre Auswahl der aufbewahrten Akten nachvollziehbar zu begründen.[49] Die weiter aufbewahrten Vorgänge weisen einen engen persönlichen oder inhaltlichen Bezug zum Gegenstand des Untersuchungsausschusses auf. Die Zahl der nicht gelöschten Vorgänge beläuft sich nur auf einen Bruchteil der bei der Polizei für die Untersuchungsausschüsse vorgehaltenen Vorgänge.

Auch der Verfassungsschutz hat uns plausibel dargelegt, wie und welche löschreifen Akten anlässlich der Löschmoratorien ausgesondert werden. Überdies hat der Verfassungsschutz durch die Einrichtung einer personell gut ausgestatteten Projektgruppe organisatorische Maßnahmen getroffen, um sowohl die Aussonderung und Aufbewahrung der betreffenden Daten als auch deren anschließende Vernichtung und Löschung zu gewährleisten. Die Zahl der Vorgänge, die allein aufgrund der Löschmoratorien nicht vernichtet sind, war im Ergebnis nicht zu beanstanden.

Die anfragenden Parlamente müssen ebenfalls konkret prüfen, ob die angeforderten Unterlagen erforderlich

[49] Rechtsgrundlage ist hier § 9 Verordnung über die Aufbewahrung und Speicherung von Justizakten (JAktAV) auf Grundlage von § 2 Justizaktenaufbewahrungsgesetz (JAktAG).

sind. In einem Urteil[50] zum Verfahren eines vom Österreichischen Nationalrat eingesetzten Untersuchungsausschusses hat der Europäische Gerichtshof (EuGH) erst kürzlich deutlich gemacht, dass auch die Verarbeitung von personenbezogenen Daten im Rahmen von Untersuchungsausschüssen an den Anforderungen der Datenschutz-Grundverordnung (DSGVO) zu messen ist.

Parlamentarische Untersuchungsausschüsse dienen der Stärkung des Vertrauens der Bürger:innen in die Arbeit der Exekutive. Dieses Vertrauen ist gefährdet, wenn Behörden keine Rechenschaft über ihr Handeln ablegen können. Zu diesem Zweck sieht § 20a BlnDSG vor, dass auch personenbezogene Daten im Rahmen von Löschmoratorien über die gesetzlich vorgegebene Löschfrist hinaus gespeichert werden dürfen. Gleichwohl ist die Vorhaltung der Daten nicht voraussetzungslos, sondern steht unter dem Vorbehalt, dass die Daten im Rahmen der Mitwirkung an der Aufgabenerfüllung des Untersuchungsausschusses erforderlich sein müssen. Die Prüfung der Erforderlichkeit muss in den Prozessen der aufbewahrenden Behörden Niederschlag finden und nachvollziehbar sein. Im Zweifel müssen zusammen mit dem anfragenden Parlament geeignete Kriterien für die Relevanz der Daten gefunden werden, denn auch die Parlamente und ihre Untersuchungsausschüsse müssen die Vorgaben der DSGVO beachten.

2. Informationspflicht bei Zuverlässigkeitsüberprüfungen

Während der diesjährigen „Berlin Pride"-Parade anlässlich des Christopher Street Day (CSD) hat die Polizei Zuverlässigkeitsüberprüfungen bei den Fahrer:innen der Umzugswagen vorgenommen, ohne uns davon frühzeitig in Kenntnis zu setzen. Die beabsichtigte Datenübermittlung wurde uns erst zwei Tage vor der Veranstaltung mitgeteilt. Die Benachrichtigung ließ damit keinen ausreichenden Raum für die Ausübung unseres gesetzlichen Auftrags,

Im Vorfeld des 45. Christopher Street Day vereinbarte die Polizei mit dem Versammlungsleiter der Parade, Zuverlässigkeitsüberprüfungen nach § 45a Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (ASOG Bln) durch-zuführen. Diese Zuverlässigkeitsüberprüfungen betrafen etwa 75 Fahrer:innen der sog. Float-Trucks, die während der Demonstration eingesetzt werden sollten. Im Anschluss

[50] EuGH, Urteil vom 16. Januar 2024, C-33/22.

an die Zuverlässigkeitsüberprüfungen sollte eine Akkreditierung durch den Versammlungsleiter erfolgen.

Bei beabsichtigten Datenübermittlungen zum Zweck einer Zuverlässigkeitsüberprüfung ist die Benachrichtigung unserer Behörde gesetzlich vorgeschrieben.[51] Diese muss uns rechtzeitig vor der Übermittlung erreichen, andernfalls kann unser gesetzlicher Auftrag der datenschutzrechtlichen Kontrolle nicht wirksam erfüllt werden. Eine Unterrichtung erst zwei Tage vor Beginn der Veranstaltung ist nicht ausreichend. Wir müssen Zeit haben, den Sachverhalt zu prüfen und rechtlich wie technisch zu bewerten sowie etwaige Bedenken zu äußern, bevor die Datenübermittlung stattfindet. Zudem muss die faktische Möglichkeit bestehen, aufsichtsrechtlich einzuschreiten. Da die rechtzeitige Einbindung versäumt wurde, haben wir gegenüber der Polizei eine Mangelfeststellung ausgesprochen.

Die gesetzlich vorgesehene Unterrichtung unserer Behörde über geplante Datenübermittlungen im Rahmen von Zuverlässigkeitsüberprüfungen muss frühzeitig vor der beabsichtigten Datenübermittlung erfolgen, damit der Sinn einer datenschutzrechtlichen Überprüfung nicht konterkariert wird. Insbesondere bei umfangreichen Zuverlässigkeitsüberprüfungen muss der Zeitrahmen so bemessen sein, dass wir die Rechtmäßigkeit prüfen und dann ggf. noch notwendige Anpassungen vorgenommen werden können.

Die Kritik der Berliner Beauftragten für Datenschutz und Informationsfreiheit an der nicht rechtzeitig erfolgten Benachrichtigung über die Durchführung einer Zuverlässigkeitsüberprüfung anlässlich der „Berlin Pride“- Parade ist berechtigt. Es handelt sich insofern um einen bedauerlichen Einzelfall; die Polizei wird künftig darauf achten, dass die Berliner Beauftragte für Datenschutz und Informationsfreiheit fristgerecht im Vorfeld einer Zuverlässigkeitsüberprüfung über diese nach § 45a Absatz 3 ASOG informiert wird.

3. Einsatz von Bodycams in Wohnungen

Die Regierungsfraktionen haben einen Gesetzesentwurf zur Änderung des ASOG Bln ins Abgeordnetenhaus eingebracht, der u. a. die Ausweitung des Einsatzes von körpernah getragenen Kameras, sog. Bodycams, vorsieht. Im Rahmen einer Expertenanhörung haben wir Änderungen am Entwurf vorgeschlagen.

Der Einsatz von Bodycams ist Polizist:innen sowie Angehörigen von Feuerwehr und Rettungsdiensten im öffentlichen Raum bereits erlaubt.[52] Nach der bisherigen Regelung befinden sich die Kameras während des Einsatzes im ständigen Aufnahmebetrieb und überschreiben alle 30 Sekunden das Gefilmte. Dauerhaft gespeichert werden die Aufnahmen nur, wenn die Speicherung per Knopfdruck ausgelöst wird. Dann werden die letzten 30 Sekunden (sog. Pre-Recording) sowie sämtliche Aufnahmen bis zum erneuten Knopfdruck gespeichert. Dies soll nach dem Gesetz zum Schutz der eingesetzten Beamt:innen erfolgen, auf Verlangen einer betroffenen Person oder sobald Zwangsmaßnahmen

[51] Siehe § 45a Abs. 3 ASOG Bln.
[52] Siehe § 24c ASOG Bln; siehe auch JB 2020, 3.2.

angewendet werden, die unmittelbar auf Personen oder Sachen durch körperliche Gewalt, deren Hilfsmittel und durch Waffen einwirken.[53]

Mit dem eingebrachten Änderungsentwurf beabsichtigten die Regierungsfraktionen u. a., den Einsatz von Bodycams auch innerhalb von Wohnungen und an anderen nichtöffentlichen Orten zu erlauben. Darüber hinaus sollten die Dauer des Pre-Recording von 30 auf 60 Sekunden verlängert, zusätzlich Dienstkräfte der Ordnungsämter mit Kameras ausgestattet und die Fristenregelung zur Geltungsdauer der Vorschriften unter der Bedingung der wissenschaftlichen Evaluation gestrichen werden. Bisher war vorgesehen, dass die Regelungen im ASOG Bln zum 1. April 2025 außer Kraft -treten, wenn sie nicht ein Jahr zuvor wissenschaftlich evaluiert und danach durch das Abgeordnetenhaus bestätigt werden.[54]

In einem wesentlichen Kritikpunkt unserer Stellungnahme haben wir hervorgehoben, dass der Gesetzesentwurf keinen Richtervorbehalt für die Weiterverwendung der in Wohnungen angefertigten Aufnahmen vorsah. Sowohl der Einsatz von Kameras in Wohnungen als auch die Verwendung dieser Aufnahmen zu anderen Zwecken als der Eigen- bzw. Drittsicherung der Polizeibeamt:innen oder Rettungskräfte stellen für sich genommen gesonderte Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung in Art. 13 Grundgesetz (GG) dar. Ob solche Eingriffe gerechtfertigt sein können, ist abschließend in Art. 13 GG geregelt (sog. Grundrechtsschranken). Der Einsatz von Kameras in Wohnungen zur Eigensicherung von Polizei- oder Rettungskräften lässt sich verfassungsrechtlich abbilden,

Zu dem von der Berliner Beauftragten für Datenschutz und Informationsfreiheit wiedergegebenen Gesetzentwurf der Koalitionsfraktionen wurde am 13. November 2023 eine Sachverständigenanhörung im Ausschuss für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin durchgeführt, in der auch die Berliner Beauftragte für Datenschutz und Informationsfreiheit ihre Kritik und ihre Hinweise vorgebracht hat. In der Folge wurden, wie von der Berliner Beauftragten für Datenschutz und Informationsfreiheit zutreffend dargestellt, ein Richtervorbehalt für die Nutzung von Bodycam-Aufzeichnungen aus dem nicht-öffentlich zugänglichen Bereich, insbesondere aus Wohnungen, in den Gesetzentwurf ebenso aufgenommen wie eine ausdrückliche Verpflichtung zur Kennzeichnung und Verschlüsselung der Bodycam-Aufzeichnungen. Die Kritik der Berliner Beauftragten für Datenschutz und Informationsfreiheit an der Verlängerung des Pre-Recordings von 30 auf 60 Sekunden als unverhältnismäßig wurde vom Abgeordnetenhaus nicht aufgegriffen. Die Verlängerung ermöglicht es, den Vorlauf von Situationen, die zu dem Auslösen der Anfertigung von Bild- und Tonaufnahmen geführt haben, besser nachzuvollziehen. Eine Pre-Recording-Dauer von 60 Sekunden findet sich daher in den gesetzlichen Regelungen Brandenburgs, Bremens, Mecklenburg-Vorpommerns, und Sachsens, während Sachsen-Anhalt und Schleswig-Holstein eine Dauer von 120 Sekunden zulassen.

[53]Siehe § 2 Gesetz über die Anwendung unmittelbaren Zwanges bei der Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Landes Berlin (UZwG).
[54]Siehe § 24c Abs. 7 Satz 1 ASOG Bln.

auch ohne dass ein Gericht die Maßnahme zuvor angeordnet hat. Anders sieht es hingegen aus, wenn die so entstandenen Aufnahmen zu anderen Zwecken genutzt werden. Sollen die Aufnahmen zum Zweck der Straf-verfolgung oder der Gefahrenabwehr weiterverwendet werden, bedarf es wie bei anderen repressiven Ermittlungshandlungen, die in Art. 13 GG eingreifen, der richterlichen Feststellung, ob die Maßnahme rechtmäßig war (sog. Richtervorbehalt). In anderen Landesgesetzen sind solche Regelungen zum Einsatz von Bodycams in Wohn-räumen entsprechend formuliert[55] und von ersten gerichtlichen Entscheidungen bestätigt.[56] Nur so kann unabhängig überprüft werden, ob die Maßnahme des Kameraeinsatzes in Wohnungen rechtmäßig war und die Weiterverwendung der durch die Maßnahme gewonnenen Daten und Erkenntnisse unter Beachtung der Grundrechtspositionen der Betroffenen genehmigt werden kann.

Nach dem Gesetzesentwurf soll die Einsatzmöglichkeit der Bodycams nicht nur auf Wohnungen erweitert werden, sondern auch auf andere nicht-öffentliche Orte. Dies eröffnet zahlreiche Eingriffsmöglichkeiten in andere besonders grundrechtsrelevante Schutzbereiche wie Arztpraxen, Anwaltskanzleien, öffentliche Toiletten, Religionsstätten, Gerichte und das Abgeordnetenhaus. Spezielle Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten durch Polizei, Rettungsdienste oder Bezirksämter sowie entsprechende Garantien, wie sie auch europarechtlich gefordert sind, fehlen im Entwurf.[57] Zudem halten wir den zunehmenden Überwachungsdruck, wie er sich aus dem Vorschlag ergibt, das Pre-Recording der Bodycams um das Doppelte zu verlängern, für unverhältnismäßig.

In unserer Stellungnahme an das Abgeordnetenhaus haben wir daher Nachbesserungen bezüglich der geplanten Regelungen sowie deren rechtlicher Fundie-

[55]Siehe § 15c Abs. 6 Satz 1 Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW); Art. 33 Abs. 4 Satz 5 Gesetz über die Aufgaben und Befugnisse der Bayerischen Polizei (Polizeiaufgabengesetz, PAG); § 32a i. V. m. § 26a Abs. 4 Satz 1 Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (Sicherheits- und Ordnungsgesetz, SOG M-V), § 31a Abs. 3 Satz 3 Brandenburgisches Polizeigesetz (BbgPolG); § 32 Abs. 3 Satz 5 Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG); § 33 Abs. 4 Satz 4 Bremisches Polizeigesetz (BremPolG); § 44 Abs. 6 Polizeigesetz Baden-Württemberg (PolG); § 184a Abs. 1 Satz 5 Allgemeines Verwaltungs-gesetz für das Land Schleswig-Holstein (LVwG).

[56]Siehe dazu jüngst Oberlandesgericht (OLG) Karlsruhe, Beschluss vom 26. April 2023, 14 W 15/23 (Wx), Rn. 14, 20; Arbeitsgericht (ArbG) Reutlingen, Beschluss vom 10. August 2021, 5 UR II 4/21 L.

[57]Die nötigen Garantien und Voraussetzungen unterscheiden sich insoweit je nach Zweck der Datenverarbeitung und verantwortlicher Stelle im Detail, siehe u. a. § 33 Abs. 1 und 2 BlnDSG; Art. 6, Art. 10 JI-Richtlinie; Art. 9 Abs. 1, Art. 10 DSGVO.

rung angemahnt und auf die Notwendigkeit einer konkreten datenschutzkonformen technischen Ausgestaltung, wie etwa die manipulationssichere Kennzeichnung der Wohnungsaufnahmen oder deren verschlüsselte Speicherung und Weiterverarbeitung, hingewiesen. Es wäre insgesamt angezeigt gewesen, wie vom Gesetz ursprünglich vorgesehen, eine wissenschaftliche Evaluation durchzuführen und auf dieser Grundlage Änderungs-vorschläge vorzulegen.

Inzwischen ist das Gesetz mit einigen Änderungen angenommen. Wir konnten die Regierungsfraktionen gemeinsam mit anderen Sachverständigen zumindest überzeugen, den Richtervorbehalt bei der Weiterverwendung von Aufnahmen aus Wohnungen aufzunehmen. Ebenso wurden Regelungen zur Verschlüsselung und zur Kennzeichnung von Aufnahmen aus nicht-öffentlichen Bereichen konkretisiert. Andere wichtige Punkte unserer Stellungnahme wurden hingegen nicht aufgegriffen.

4. Recht auf kostenfreie Auskunft über polizeiliche Zugriffsprotokolle

Die Polizei ist gesetzlich verpflichtet, alle Zugriffe auf die bei ihr gespeicherten personenbezogenen Daten zu protokollieren und diese Protokolle zwei Jahre lang aufzubewahren.[58] Sie spielen im Rahmen unserer Aufsichtspraxis insbesondere bei Auskunftsansprüchen nach dem Berliner Informationsfreiheitsgesetz (IFG) und der DSGVO eine Rolle..

Immer häufiger beantragen betroffene Personen bei der Polizei nicht nur Auskunft über die zu ihnen gespeicherten Einträge, sondern bitten auch um Auflistung der zu ihrer Person getätigten Datenabfragen inklusive Abfragegrund, abfragender Person und zugehöriger Dienststelle. Bislang wurden diese Anfragen von der Polizei mit einem Musterschreiben unter Verweis auf das IFG beantwortet. Grund dafür könnte sein, dass der in der Rechtsprechung des Oberverwaltungsgericht Berlin-Brandenburg entschiedene Fall zur Herausgabe von Protokollbanddaten nach dem IFG entschieden wurde.[59] Nach dem IFG besteht zwar in der Regel ein Anspruch auf Herausgabe der Protokolldaten, allerdings mit dem Nachteil für die betroffene Person, dass die Bearbeitung von IFG-Anfragen grundsätzlich kostenpflichtig ist.

Es ist zutreffend, dass die Polizei Berlin in der Vergangenheit diejenigen Daten, die die Umstände von Abfragen personenbezogener Daten durch ihre Dienstkräfte protokollieren, kostenpflichtig nach dem IFG Bln an die insoweit Auskunft begehrende betroffene Person herausgegeben hat. Die Polizei ist davon ausgegangen, dass diese Protokolldaten keine bzw. allenfalls nur eine mittelbare Verarbeitung personenbezogener Daten der Betroffenen darstellen, da die Protokolle die Tätigkeit der abfragenden Dienstkräfte dokumentieren und daher in erster Linie deren personenbezogenen Daten enthalten.

Auf die Kritik der Berliner Beauftragten für Datenschutz und Informationsfreiheit und den Hinweis auf das Urteil des EuGH hin hat die Polizei ihre Verfahrensweise dahingehend geändert, dass sie nunmehr im Rahmen eines Antrags auf Auskunft über die bei der Polizei Berlin gespeicherten Daten

[58] Siehe § 62 BlnDSG.
[59] Oberverwaltungsgericht (OVG) Berlin-Brandenburg, Urteil vom 1. Dezember 2021, 12 B 23/20.

auch die Protokolldaten zu Abfragen zur Antragstellenden Person gebührenfrei gemäß § 43 BlnDSG bzw. § 50 ASOG Bln zur Verfügung stellt.

Der EuGH hat nunmehr entschieden, dass Informationen, die protokollierte Abfragen personenbezogener Daten betreffen und sich auf den Zeitpunkt und den Zweck dieser Abfragen beziehen, unter den Auskunftsanspruch nach Art. 15 DSGVO fallen.[60] Damit sind Zugriffsprotokolle herauszugeben; lediglich die schützenswerten personenbezogenen Daten der Mitarbeitenden, die die betreffenden Datensätze aufgerufen haben und deren Name und Stellung aus den Protokollen hervorgehen könnten, sind unter Umständen zu schwärzen. Der EuGH will aber auch die Herausgabe dieser Daten erlauben, wenn einerseits die Rechte und Freiheiten der Mitarbeitenden gegenüber der Herausgabe abgewogen werden und andererseits die Herausgabe unerlässlich ist, um den anfragenden Personen die wirksame Wahrnehmung ihrer Betroffenenrechte zu ermöglichen.

Der Auskunftsanspruch nach der DSGVO ist zwar auf Daten der Strafverfolgungs-behörden nicht direkt anwendbar.[61] Die Verarbeitung im Bereich der Gefahrenabwehr und der Strafverfolgung wird durch die sog. JI-Richtlinie[62] geregelt, die einen gleichgelagerten Auskunftsanspruch enthält.[63] Auch der Begriff „personenbezogene Daten“ ist in der DSGVO und JI-Richtlinie wortgleich definiert.[64] In seinem Urteil hat der EuGH festgestellt, dass Protokolldaten über Abfragen zu einer Person Informationen über diese Person enthalten und sich damit auf diese Person beziehen, also mithin selbst personenbezogene Daten der abgefragten Person sind. Auch der Auskunftsanspruch der JI-Richtlinie erstreckt sich damit auf diese Daten. Die Auskunft ist nach den Vorgaben der JI-Richtlinie bzw. der nationalen Umsetzung kostenlos zu erteilen.[65] Ebenso schreibt die Richtlinie den Behörden vor, das Auskunftsverfahren für

[60]EuGH, Urteil vom 22. Juni 2023, C-579/21.
[61]Siehe Art. 2 Abs. 2 lit. d DSGVO.
[62]Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, umgesetzt jeweils in Teil 3 des BlnDSG und des Bundesdatenschutzgesetzes (BDSG).
[63]Siehe Art. 12 Abs. 4 JI-Richtlinie, umgesetzt in §§ 43, 45 BlnDSG bzw. in §§ 57, 59 BDSG i. V. m. § 500 Abs. 1 Strafprozessordnung (StPO).
[64]Siehe Art. 4 Nr. 1 DSGVO und Art. 3 Nr. 1 JI-Richtlinie.
[65]Siehe Art. 12 Abs. 4 JI-Richtlinie.

Antragsteller:innen möglichst barrierefrei zu gestalten.[66] Wir haben die Polizei informiert und aufgefordert, die bisherige Praxis rechtskonform umzustellen.

Wenn die Polizei für eine datenschutzrechtliche Auskunft eine Gebühr erhebt, stellt dies regelmäßig einen Verstoß dar. Nach aktueller Rechtsprechung des EuGH umfasst das Auskunftsrecht im Rahmen der DSGVO auch nähere Angaben zu protokollierten Abrufen der Mitarbeitenden der verantwortlichen Stelle. Diese Klarstellung zum Umfang des Auskunftsrechts ist auch auf die Verarbeitung personenbezogener Daten nach der JI-Richtlinie übertragbar. Die Entscheidung betrifft damit alle Behörden, die personenbezogene Daten im Bereich der JI-Richtlinie verarbeiten, denn zur Protokollierung der Zugriffe sind beispielsweise auch Staatsanwaltschaften, Justizvollzugsanstalten und Ordnungsämter verpflichtet.[67]

5. Datenerhebung im aufenthaltsrechtlichen Verteilverfahren

Wenn Angehörige von Drittstaaten[68] illegal nach Deutschland einreisen, sieht das deutsche Aufenthaltsrecht eine Verteilung dieser Personen auf die Bundesländer vor. Die Voraussetzungen für die Verteilungsentscheidung sowie die organisatorischen Fragen des sog. Verteilverfahrens sind gesetzlich in § 15a Aufenthaltsgesetz (-AufenthG) geregelt. Das Landesamt für Einwanderung (LEA) erhebt diesbezüglich mithilfe mehrerer Fragebögen zahlreiche Informationen über die betroffenen Personen.

Das Landesamt für Einwanderung (LEA) wird die kritisierten Vordrucke abschaffen.

Künftig werden nur noch Daten erhoben werden und in Form einer Niederschrift zur Akte gelangen, die erforderlicherweise erhoben werden müssen bzw. die aufgrund der gesetzlichen Vorgaben wie insbesondere gemäß §§ 62 ff. AufenthV (Verpflichtung für die Ausländerbehörden, die Ausländerdateien A und B mit vorgegebenen Datensatzinhalten zu führen bzw. künftig so im Ausländerzentralregister - AZR - zu speichern) erhoben werden. Für die Änderung des Verfahrens werden die künftig zu verwendenden Vordrucke noch in die wichtigsten Sprachen übersetzt und die Mitarbeitenden, welche die Befragungen durchführen, entsprechend geschult.

Das LEA führt zunächst eine Befragung anhand von zwei Erhebungsbögen mit dem Titel „Neueinreise“ durch. In einem Bogen werden Angaben zur betroffenen Person sowie deren Ehepartner:in, Kindern und Eltern erfasst, soweit sich diese in Deutschland aufhalten, d. h. Vor- und Familiennamen, Geschlecht, Geburtsdatum, Staatsangehörigkeit und Aufenthaltsort ggf. genannter Angehöriger. Ferner wird das Datum der Einreise vermerkt sowie die Angabe gefordert, ob die Einreise zusammen mit Ehepartner:in, Kindern und/oder

[66] Siehe Art. 12 Abs. 2 JI-Richtlinie.
[67] Siehe § 30 Abs. 1 und 2 i. V. m. § 62 BlnDSG; § 500 Abs. 1 StPO i. V. m. § 76 BDSG.
[68] Dies sind alle Länder, die weder zur Europäischen Union (EU) noch zum Europäischen Wirtschaftsraum (EWR) gehören – ausgenommen die Schweiz.

Eltern erfolgt ist. Im zweiten Bogen werden Informationen zu den bisherigen Lebensverhältnissen verzeichnet, soweit diese dem LEA noch nicht vorliegen: Angaben zur Schul- und Ausbildung sowie zu Beruf und letzter bzw. letztem Arbeitgeber:in, zur Anschrift im Heimatland, zur Muttersprache und weiteren Sprachkenntnissen, zu Familienangehörigen, die sich nicht in Deutschland aufhalten, und Angehörigen im europäischen Ausland. Ferner werden Auskünfte zu Reisebeginn und -verlauf sowie zu Kosten, Finanzierung und etwaiger Unterstützung eingeholt.

Für die Ausländerbehörden hat der Gesetzgeber eine spezifische Datenverarbeitungsbefugnis erlassen, wonach diese „zum Zweck der Ausführung dieses Gesetzes und ausländerrechtlicher Bestimmungen in anderen Gesetzen personenbezogene Daten erheben [dürfen], soweit dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz und nach ausländerrechtlichen Bestimmungen in anderen Gesetzen erforderlich ist“.[69] Die Aufgabenerfüllung wird im Zusammenhang mit dem Verteilverfahren wiederum durch § 15a Abs. 1 AufenthG konkretisiert. Die Ausländerbehörde muss demnach feststellen, ob das Verteilverfahren im konkreten Fall überhaupt greift.[70] Das bedeutet, sie muss am Einzelfall prüfen, ob die drei folgenden Voraussetzungen für die Verteilung erfüllt sind: Die betroffene Person muss unerlaubt eingereist sein, sie darf kein Asylgesuch gestellt haben und sie kann nicht unmittelbar in Haft genommen oder ab- bzw. zurückgeschoben werden.[71] Darüber hinaus muss ausgeschlossen sein, dass zwingende Gründe der Verteilung an einen anderen Ort entgegenstehen.[72]

Gemessen an diesen gesetzlich definierten Aufgaben sind zahlreiche Informationen, die das LEA mithilfe ihrer Fragebögen im Rahmen des Verteilverfahrens erhebt, nicht erforderlich. Beispielsweise bedarf es nicht des konkreten Einreisedatums, um zu prüfen, ob das Verteilverfahren durchgeführt werden kann; vielmehr ist dafür die Feststellung ausreichend, ob die Einreise vor oder nach dem 1. Januar 2005 erfolgt ist. Ferner ist nicht erkennbar, inwiefern die Informationen über die schulische und berufliche Ausbildung, über Familienangehörige außerhalb des Bundesgebiets sowie über Reiseverlauf, Kosten, Finanzierung und Unterstützung zur Prüfung der Tatbestandsvoraussetzungen für das Verteilverfahren erforderlich sind.

[69] § 86 AufenthG.
[70] So darf das Verteilverfahren nach § 15a Abs. 6 AufenthG nicht auf Personen angewendet werden, die nachweislich vor dem 1. Januar 2005 eingereist sind.
[71] § 15a Abs. 1 Satz 1 AufenthG.
[72] § 15a Abs. 1 Satz 6 AufenthG.

Wir haben das LEA deshalb darauf hingewiesen, dass der Umfang der für das Verteilverfahren erhobenen Daten gegen den Grundsatz der Datenminimierung nach Art. 5 DSGVO verstößt und die Fragebögen entsprechend anzupassen sind.

Der Umfang an erlaubten Datenverarbeitungen von Behörden ist durch deren gesetzlich festgelegte Aufgaben begrenzt. Im aufenthaltsrechtlichen Verteilverfahren bedeutet dies, dass solche personenbezogenen Daten nicht erhoben werden dürfen, die zur Prüfung der gesetzlichen Voraussetzungen nicht benötigt werden. Der Grundsatz der Datenminimierung ist dabei zu jeder Zeit anzuwenden.

6. Unzulässige Verarbeitung eines Namens im standesamtlichen Verfahren

In einer Bescheinigung über die Namensführung wurde von einem Standesamt der Nachname der US-amerikanischen Leihmutter als früherer Geburtsname des -Kindes eingetragen. Die Wunscheltern des Kindes waren damit nicht einverstanden und wandten sich an uns, weil sie diese Datenverarbeitung als unzulässig ansahen.

Nach der Geburt des Kindes in den USA war den Wunscheltern vom zuständigen US-Bezirksgericht die rechtliche Elternstellung bestätigt worden. Das Recht des betreffenden US-Bundesstaates sieht vor, dass eine Leihmutter mit Geburt des Kindes auf die elterliche Sorge verzichtet und die Wunscheltern die elterliche Sorge anerkennen. Daraufhin gaben diese beim zuständigen Standesamt in Berlin eine Namenserklärung ab, mit der der Familienname des Kindes bestimmt wurde, da sie zwar verheiratet aber keinen gemeinsamen Ehenamen führten. Zur Prüfung der Wirksamkeit der Namenserklärung wandte sich das Standesamt an das zuständige Amtsgericht,[73] das die Rechtmäßigkeit der Elternstellung bestätigte, woraufhin das Standesamt die Namensbescheinigung für das Kind ausstellte. Als neuer Geburtsname wurde der von den Eltern gewünschte Nachname eingetragen, allerdings gab das Standesamt als früheren Geburtsnamen des Kindes den Nachnamen der Leihmutter an. Diese Angabe und die Verarbeitung des Nachnamens der Leihmutter sind unrechtmäßig.

Wenn Eltern zum Zeitpunkt der Geburt eines Kindes zwar miteinander verheiratet sind, aber keinen gemeinsamen Ehe- bzw. Familiennamen führen, müssen sie

[73] Siehe § 49 Abs. 2 Satz 1 PStG.

gegenüber dem Standesamt eine Namenserklärung abgeben, damit das Kind einen Geburtsnamen erhält. Nichts anderes gilt für ein im Ausland geborenes Kind.[74] Das Standesamt, das seine Vorschriften aus dem Personenstandsgesetz (PStG) und der Personenstandsverordnung (PStV) bezieht, beglaubigt mit seiner Bescheinigung die Namensbestimmung und nimmt die entsprechende Eintragung im Personenstandsregister vor.[75] Das Personenstandsrecht bezieht sich dabei allein auf die rechtliche Elternschaft[76] und ist nicht zur Information über die biologische oder genetische Elternschaft bestimmt. Der Bundesgerichtshof (BGH) hat 2014 entschieden, dass die Begründung originärer gemeinsamer Elternschaft zweier Männer möglich sei, wenn sie mittels einer Leihmutter ein Kind bekommen.[77] Nach Ansicht des BGH gehört zum Kindeswohl die verlässliche rechtliche Zuordnung zu denjenigen Personen, die für sein Wohl und Wehe kontinuierlich Verantwortung übernehmen.[78] Zwar hat das Kind ein Recht auf Kenntnis seiner Abstammung, jedoch gehört es nicht zur gesetzlichen Aufgabenerfüllung eines Standesamts, die Herkunft in einer Bescheinigung offenzulegen; ebenso wenig wie diese durch das Personenstandsregister preiszugeben ist. Die Bescheinigung über die Namensführung eines Kindes trifft damit nur eine Aussage zu der rechtlichen Elternschaft und – bei unterschiedlichen Namen der rechtlichen Eltern – dem bestimmten Familiennamen.

Die Aufnahme des Namens der Leihmutter in die Bescheinigung war daher nicht erforderlich, die Verarbeitung durch das Standesamt damit unzulässig. Dies haben wir sowohl den Wunscheltern als auch dem Standesamt mitgeteilt.

Das Personenstandsregister sowie Bescheinigungen des Standesamtes, die eine Namensbestimmung beglaubigen, bilden nicht die genetische Abstammung eines Kindes, sondern das rechtliche Eltern-Kind-Verhältnis ab. Dementsprechend dürfen das Register und die Bescheinigung nur die dafür erforderlichen Daten enthalten. Zur Berichtigung eines bereits abgeschlossenen Registereintrags muss ggf. ein Antrag auf gerichtliche Anordnung gestellt werden.

[74]Siehe Deutsche Vertretungen in den USA, Namenserklärung für ein im Ausland geborenes Kind, abrufbar unter https://www.germany.info/us-de/service/familienangelegenheiten/namensrecht/name-kind/1216876; § 1617 Abs. 1 Bürgerliches Gesetzbuch (BGB).
[75]Siehe § 45 Abs. 1 Nr. 1, Abs. 2 Satz 2, § 9 Abs. 1 PStG.
[76]Siehe Dominik Balzer, Die genetische Vaterschaft im Familien-, Familienverfahrens- und Personenstandsrecht, StAZ Das Standesamt, 12/2012, S. 368.
[77]BGH, Beschluss vom 10. Dezember 2014, XII ZB 463/13.
[78]Ebd., Rn. 57 m. w. N., sowie insbesondere Europäischer Gerichtshof für Menschenrechte (EGMR), Urteil vom 26. Juni 2014, 65192/11 (Mennesson vs. Frankreich).

7. Erforderlichkeitsgrundsatz bei der Anspruchsbegründung vor Gericht

Soweit Rechtsanwält:innen im Rahmen eines Mandatsverhältnisses in gerichtlichen bzw. außergerichtlichen Verfahren ihre eigenen Interessen oder die rechtlichen -Interessen ihrer Mandant:innen wahrnehmen und dabei personenbezogene Daten verarbeiten, entscheiden sie grundsätzlich über die Zwecke und Mittel der Verarbeitung dieser Daten und sind insofern datenschutzrechtlich Verantwortliche.[79] Dementsprechend müssen sie insbesondere dafür Sorge tragen, dass die jeweilige Daten-verarbeitung rechtmäßig erfolgt, mithin eine Rechtsgrundlage hierfür existiert. Dabei kommt dem Erforderlichkeitsgrundsatz eine besondere Bedeutung zu.

Regelmäßig erhalten wir Beschwerden von Betroffenen über die Verarbeitung nicht erforderlicher Daten durch Rechtsanwält:innen. In einem uns vorliegenden Fall befand sich die betroffene Person mit einer ehemals mandatierten Kanzlei in einem Rechtsstreit über die Höhe der anwaltlichen Kostenrechnungen. Die Kanzlei machte die Forderung gegen die betroffene Person in einer Klage geltend. Zur Begründung des Forderungsanspruchs übersandte die Kanzlei mehrere Hundert Seiten Kopien der Mandatsakte als Anlage zur Klageschrift an das zuständige Gericht. Die übermittelten Dokumente enthielten eine Vielzahl an Informationen über die betroffene Person, darunter auch besonders schutzwürdige Gesundheitsdaten wie ärztliche Gutachten, Diagnose-berichte und Versicherungsunterlagen, die die Kanzlei seinerzeit im Rahmen des Mandats zur Wahrnehmung der rechtlichen Interessen der betroffenen Person erhalten hatte.

In Art. 6 Abs. 1 Satz 1 DSGVO sind die verschiedenen Erlaubnistatbestände für eine Verarbeitung personenbezogener Daten festgelegt. Das darin zum Ausdruck kommende sog. Verbotsprinzip mit Erlaubnisvorbehalt wird durch das übergreifende Prinzip der Erforderlichkeit ergänzt. Eine Datenverarbeitung nach den Regelungen der DSGVO[80] ist nur zulässig, wenn dies im Rahmen des jeweiligen Erlaubnistatbestands erforderlich ist. Die Datenverarbeitung wird also hinsichtlich Art und Umfang durch die gesetzliche Forderung beschränkt, dass die Verarbeitung zu bestimmten legitimen Zwecken[81] erforderlich sein muss. Erforderlichkeit verlangt, dass es zur beabsichtigten Art und Weise der Datenverarbeitung keine sinnvolle oder zumutbare mildere Alternative gibt, um die jeweils verfolgte Zielsetzung zu erreichen. Nicht ausreichend ist dagegen,

[79] Siehe Art. 4 Nr. 7 DSGVO.
[80] Art. 6 Abs. 1 Satz 1 lit. b bis f, Art. 9 Abs. 2 lit. b, c, f bis j DSGVO.
[81] Zweckbindungsgrundsatz nach Art. 5 Abs. 1 lit. b DSGVO.

wenn die Verarbeitung der Daten den im Erlaubnistatbestand aufgeführten Zielsetzungen lediglich dienlich oder förderlich ist. Bei der Bewertung der Erforderlichkeit im Einzelfall ist auch der Grundsatz der Datenminimierung[82] zu beachten, der die Auslegung weiter ausschärft. Nach dem Datenminimierungsgrundsatz müssen personenbezogene Daten dem Zweck angemessen, erheblich und auf solche Daten beschränkt sein, die für die Zweckerreichung notwendig sind.

Zwar erfolgte die Übermittlung personenbezogener Daten der betroffenen Person im vorliegenden Fall zum Zweck der Wahrung der rechtlichen Interessen der verantwortlichen Kanzlei bzw. der Durchsetzung der eigenen Rechtsansprüche.[83] Nicht alle übersandten Unterlagen waren hierfür jedoch erforderlich. Zum Nachweis, dass eine Honorarforderung entstanden ist, genügt der Beleg, aus dem sich die Mandatierung ergibt. Abhängig davon, welche Gebührenart eingeklagt wird, können auch weitere Belege notwendig sein. Selbst wenn der Umfang und die Schwierigkeit der anwaltlichen Tätigkeit nachgewiesen werden sollen,[84] sind hierfür nicht sämtliche Dokumente aus der Mandatsakte erforderlich, sondern nur diejenigen, die dem Gericht die rechtliche Komplexität verdeutlichen. Es wäre folglich ausreichend gewesen, einige Seiten aus der Mandatsakte exemplarisch zu übermitteln.

Rechtsanwält:innen müssen stets prüfen, ob die Weitergabe personenbezogener Daten für die Geltendmachung eines Anspruchs vor Gericht erheblich bzw. zur Wahrung der klägerischen Darlegungslast für die anspruchsbegründenden Tatsachen notwendig ist. Nicht erforderliche Daten sind unkenntlich zu machen oder auf deren Weitergabe ist zu verzichten. Bei Zweifeln, ob ein Sachvortrag hinreichend substanziiert ist, kann um gerichtlichen Hinweis gebeten werden, ob aus Sicht des Gerichts weitere, ggf. ungeschwärzte Unterlagen erforderlich sind.

VI. Gesundheit, Arbeit und Soziales

1. Aufsichtszuständigkeit für Unternehmen zur Onlinebuchung von Arztterminen

Für Unternehmen, die Datenverarbeitungen in mehreren Mitgliedstaaten der Euro-päischen Union (EU) vornehmen, kann der in der Datenschutz-Grundverordnung (DSGVO) vorgesehene One-Stop-Shop-Mechanismus zur Anwendung gelangen. Dieser besagt, dass

[82] Siehe Art. 5 Abs. 1 lit. c DSGVO.
[83] Siehe Art. 6 Abs. 1 Satz 1 lit. f i. V. m. Art. 9 Abs. 2 lit. f DSGVO.
[84] Siehe § 14 Abs. 1 Rechtsanwaltsvergütungsgesetz (RVG).

die von einem Verantwortlichen (oder Auftragsverarbeiter) durchgeführten grenzüberschreitenden Datenverarbeitungen der Aufsicht einer federführenden Aufsichtsbehörde unterliegen, und zwar derjenigen, die für die Hauptniederlassung oder die einzige Niederlassung des Verantwortlichen (oder -Auftragsverarbeiters) zuständig ist.[85]

Auch in diesem Jahr gingen bei uns Beschwerden über ein Unternehmen ein, das eine Internetplattform zur Buchung von Arztterminen betreibt. Die Beschwerden hatten beispielsweise die Verarbeitung personenbezogener Daten zu Werbezwecken oder die Übermittlung von Daten an Dritte zum Gegenstand. Das Unternehmen mit Sitz in Berlin ist ein Tochterunternehmen einer Gesellschaft aus einem anderen EU-Mitgliedstaat. Im Rahmen unserer aufsichtsbehördlichen Verfahren wird uns entgegengehalten, dass nicht wir, sondern die Aufsichtsbehörde des Mitgliedstaats, in dem die Konzernmutter ihren Sitz hat, die zuständige Datenschutzaufsichtsbehörde sei. Gleichzeitig bezeichnet sich das Berliner Unternehmen selbst als Verantwortlicher für die beschwerdegegenständlichen Datenverarbeitungen.

Die DSGVO enthält in Kapitel VI Regelungen, anhand derer die zuständige Aufsichtsbehörde zu bestimmen ist: Nach Art. 55 Abs. 1 DSGVO ist grundsätzlich jede Aufsichtsbehörde im Hoheitsgebiet ihres eigenen Mitgliedstaats für die Erfüllung der Aufgaben und die Ausübung der Befugnisse zuständig, die ihr mit der DSGVO übertragen wurden. Nach Art. 56 Abs. 1 DSGVO ist für die von einem Verantwortlichen durchgeführten grenzüberschreitenden Verarbeitungen allerdings diejenige Aufsichtsbehörde federführend zuständig, in deren Hoheitsgebiet die Hauptniederlassung oder die einzige Niederlassung des Verantwortlichen liegt. Die Niederlassungen in diesem Sinne müssen keine unselbständigen Niederlassungen sein und können durchaus eigene Rechtspersönlichkeit besitzen.[86] Grenzüberschreitende Verarbeitungen können daher auch bei Unternehmensgruppen stattfinden. Aber, unabhängig davon, ob tatsächlich eine grenzüberschreitende Verarbeitung gegeben ist, knüpft Art. 56 Abs. 1 DSGVO die Zuständigkeit der Aufsichtsbehörde an den Sitz der Hauptniederlassung des Verantwortlichen. In unserem Fall stellt sich daher die Frage, ob die Konzernmutter eine Hauptniederlassung in diesem Sinne ist.

Nach Art. 4 Nr. 16 a DSGVO ist entscheidendes Merkmal für die Definition der Hauptniederlassung, dass

[85]Siehe Art. 56 Abs. 1 DSGVO.
[86]Erwägungsgrund (ErwGr.) 22, Satz 2 und 3 DSGVO.

diese über die Zwecke und Mittel der Datenverarbeitung entscheidet und diese Niederlassung befugt ist, diese Entscheidungen umsetzen zu lassen. Auch in der Unternehmensgruppe kann die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten, aber nur dann, wenn die Zwecke und Mittel der Verarbeitung nicht von einem anderen Unternehmen festgelegt werden.[87]

Letzteres ist vorliegend aber offenbar der Fall: Die Tochtergesellschaft mit Sitz in Berlin erklärt, dass sie Verantwortliche ist. Als Verantwortliche entscheidet sie nach Art. 4 Nr. 7 DSGVO über die Zwecke und Mittel der Datenverarbeitung, die Gegenstand unserer Beschwerden sind, und nicht die Konzernmutter. Entsprechend kann die Konzernmutter auch nicht Hauptniederlassung sein und der Anknüpfungspunkt für eine Zuständigkeit nach Art. 56 Abs. 1 DSGVO entfällt.

Auch kann nicht damit argumentiert werden, dass übergeordnete unternehmenspolitische Entscheidungen zur Verarbeitung von personenbezogenen Daten im Konzern zu einer Zuständigkeitsverteilung nach Art. 56 Abs. 1 DSGVO führen, wenn gleichzeitig so viel Entscheidungsspielraum bei der Tochtergesellschaft besteht, dass diese selbst Verantwortliche sein soll. Bereits dann, wenn die Konzernmutter befugt wäre, in der Tochtergesellschaft Entscheidungen in Bezug auf die Datenverarbeitungen umsetzen zu lassen, würde die Tochtergesellschaft nicht mehr allein über Zwecke und Mittel der Datenverarbeitung entscheiden und wäre damit nicht Verantwortliche i. S. v. Art. 4 Nr. 7 DSGVO.

Dies entspricht auch dem Sinn und Zweck der DSGVO, die darauf abzielt, eine Verantwortungsdiffusion zu vermeiden sowie Transparenz herzustellen, wer für die Datenverarbeitung verantwortlich zeichnet und daran anknüpfend haftet. Sie kennt nur einen alleinigen Verantwortlichen oder gemeinsam Verantwortliche[88]. Eine parallele Verantwortlichkeit ist der DSGVO hingegen fremd.

Die Anwendbarkeit des One-Stop-Shop-Mechanismus (OSS) setzt im Hinblick auf das Tatbestandsmerkmal der Hauptniederlassung voraus, dass in der Hauptniederlassung des Verantwortlichen – bei einer Unternehmensgruppe in der Hauptniederlassung des herrschenden Unternehmens – auch die Entscheidungen über Mittel und Zwecke der Datenverarbeitungen getroffen werden. Auf eine (Unternehmens-)Gruppe, die aus

[87] ErwGr. 36, Satz 8 DSGVO.
[88] Art. 26 DSGVO.

mehreren Verantwortlichen besteht, die i. S. d. Art. 4 Nr. 7 DSGVO jeweils allein über Zwecke und Mittel einer Verarbeitung entscheiden, ist der OSS hingegen nicht anwendbar.

2. Verarbeitung von Gesundheitsdaten durch Verantwortliche und Auftragsverarbeiter

Bei der Überprüfung eines Medizinischen Versorgungszentrums (MVZ) haben wir festgestellt, dass das Unternehmen seiner Verpflichtung nicht nachgekommen war, die Datenverarbeitungen seines zur Terminverwaltung eingesetzten Auftragsverarbeiters ausreichend zu überprüfen.

Ein Bürger hatte sich bei uns darüber beschwert, dass er von einem MVZ wiederholt per SMS an Arzttermine erinnert wurde, die andere Patient:innen betrafen. Mit dem Versand der Erinnerungen hatte das MVZ ein Terminverwaltungsunternehmen beauftragt. Wir nahmen die Beschwerde des Bürgers zum Anlass, die Einbindung des Termindienstleisters als Auftragsverarbeiter, die Buchungsmöglichkeit von Arztterminen und deren Eintragung in den Onlinekalender sowie die Rechtmäßigkeit der Datenverarbeitungen beim Versand der Erinnerungs-SMS von Amts wegen zu prüfen. Bei Redaktionsschluss war die Prüfung noch nicht abgeschlossen; es zeigte sich in den geprüften Bereichen jedoch bereits eine Reihe von datenschutzrechtlichen Mängeln.

Terminerinnerungen dürfen nur dann versendet werden, wenn die Patient:innen eingewilligt haben, dass deren Telefonnummer oder E-Mail-Adresse zu diesen Zwecken genutzt werden darf.[89] Zur Durchführung der Datenverarbeitungen, für die eine Rechtsgrundlage besteht, dürfen Verantwortliche auch Auftragsverarbeiter einsetzen, wobei die Vorgaben der Art. 28 und 29 DSGVO zu beachten sind. Die Auftragsverarbeiter dürfen personenbezogene Daten grundsätzlich ausschließlich auf Weisung der Verantwortlichen und nicht zu eigenen Zwecken verarbeiten.[90] Das bedeutet, dass Verantwortliche stets wissen müssen, welche Datenverarbeitungen von den eingesetzten Auftragsverarbeitern vorgenommen werden und ob diese sich im Rahmen ihrer Weisung bewegen. Der Auftraggeber muss insbesondere Abhilfe schaffen, wenn er Kenntnis davon erlangt, dass der von ihm eingesetzte Auftragsverarbeiter die Daten zu eigenen Zwecken nutzt.

Unternehmen, die für Datenverarbeitungen Dienstleister:innen beauftragen, müssen sicherstellen, dass die

[89] Siehe JB 2019, 6.3; JB 2021, 6.5; JB 2022, 5.3.
[90] Siehe Art. 29 DSGVO.

Datenschutzvorgaben bei der Durchführung des Auftrags eingehalten werden. Sie sind auch für die Rechtmäßigkeit der Datenverarbeitungen verantwortlich. Dementsprechend müssen die Unternehmen Kenntnis darüber haben, welche Datenverarbeitungen konkret auf welche Weise von den Auftragsverarbeitern durchgeführt werden, und regelmäßig prüfen, ob dies datenschutzkonform geschieht. Im Fall von Ärzt:innen muss zusätzlich sichergestellt sein, dass durch die Einbindung von Auftragsverarbeitern die ärztliche Schweigepflicht nicht verletzt wird.

3. Aufzeichnung von Telefonaten im Gesundheitswesen

Eine Einrichtung im Bereich der Vermittlung ärztlicher Versorgung plante, sämtliche Telefonate aufzuzeichnen, die mit medizinischem Personal geführt werden. In diesen Gesprächen teilten die Anrufenden auch Gesundheitsdaten[91] mit. Es stellte sich nicht nur die Frage, unter welchen Voraussetzungen die Aufzeichnung von Daten der Anrufenden zulässig ist, sondern auch, wie es mit dem Datenschutz der Beschäftigten steht.

Der Verantwortliche hielt die Datenverarbeitung auf Grundlage der ihm gesetzlich zugewiesenen Aufgabe für zulässig, konnte aber nicht nachweisen, inwiefern die Aufzeichnungen zur gesetzlichen Aufgabenerfüllung erforderlich sind.[92] Als Zweck der Aufzeichnungen gab er die ärztliche Dokumentationspflicht, den Schutz seiner Beschäftigten sowie die Verwendung in Schulungen und Feedbackgesprächen an. Wir haben dem Verantwortlichen mitgeteilt, dass eine Gesprächsaufzeichnung ohne ausdrückliche Einwilligung der anrufenden Personen nicht zulässig ist.

Die ärztliche Dokumentationspflicht erfordert weder nach der zivilrechtlichen Vorschrift zur Dokumentation einer Behandlung[93] noch nach der für Ärzt:innen geltenden Berufsordnung[94] die Aufzeichnung vollständiger Gespräche oder deren wortgetreue Wiedergabe. Zur Erfüllung der Dokumentationspflicht stehen weniger eingriffsintensive und datensparsamere Verfahren bereit. Ebenso wenig war diese Aufzeichnung zum Schutz der Beschäftigten und zur Verteidigung von etwaigen Rechtsansprüchen notwendig. Ein lediglich potenziell eintretendes Ereignis begründet noch keine Erforderlichkeit und ist als Rechtsgrundlage nicht ausreichend. Vielmehr müssen konkrete Anhaltspunkte zum

[91] Siehe Art. 4 Nr. 15, Art. 9 Abs. 1 DSGVO.
[92] Siehe Art. 6 Abs. 1 Satz 1 lit. c i. V. m. Art. 9 Abs. 2 lit. h DSGVO i. V. m. der jeweiligen Aufgabenzuweisungsnorm im Sozialgesetzbuch Fünftes Buch (SGB V).
[93] § 630 f. Bürgerliches Gesetzbuch (BGB).
[94] § 10 der Berufsordnung der Ärztekammer Berlin.

Eintreten dieses Ereignisses vorliegen, um die Datenverarbeitung auf die DSGVO stützen zu können. Auch für die vom Verantwortlichen herangezogenen Zwecke der Personalsteuerung bzw. -schulung lässt sich keine Rechtsvorschrift für die Verarbeitung von Gesundheitsdaten finden. Die Aufzeichnung der Daten kann folglich ausschließlich mit der ausdrücklichen Einwilligung der anrufenden Personen zulässig sein.[95]

Aus Sicht des Beschäftigtendatenschutzes ist die generelle Aufzeichnung von sämtlichen Telefongesprächen der Beschäftigten grundsätzlich nicht erlaubt, sofern das Telefonieren ihren Tätigkeitsschwerpunkt darstellt. Das Bundesarbeitsgericht (BAG) hat mehrfach darauf hingewiesen, dass eine vollständige Überwachung der Beschäftigten während der Arbeitszeit rechtswidrig ist: Anhand der für die Erforderlichkeitsprüfung notwendigen Interessenabwägung im sog. Keylogger-Urteil stellt das BAG fest, dass mit der zeitlich unbegrenzten Überwachung den Beschäftigten die Möglichkeit genommen sei, sich „dem permanenten Zugriff des Arbeitgebers zu entziehen“.[96] Am Beispiel von Kameraüberwachung führt das BAG an anderer Stelle aus, dass eine „lückenlose, dauerhafte sowie sehr detaillierte Erfassung des Verhaltens“ der Beschäftigten eine „schwerwiegende Pflichtverletzung“ darstelle, weil damit ein „psychischer Anpassungs- und Leistungsdruck“ erzeugt werde.[97]

Sollen Telefongespräche aufgezeichnet werden, müssen Verantwortliche grundsätzlich prüfen, ob für die Verarbeitung der personenbezogenen Daten sowohl der Anrufenden als auch der die Anrufe entgegennehmenden Mitarbeiter:innen eine Rechtsgrundlage besteht. Soll die Einwilligung der Anrufenden eingeholt werden, ist sicherzustellen, dass die Anrufenden vor Beginn des Gesprächs transparent und vollständig nach Art. 13 DSGVO über die Datenverarbeitung informiert werden und die Einwilligung freiwillig und in informierter Weise erteilen. Unabhängig von einer Einwilligung der Anrufenden ist die Aufzeichnung regelmäßig nicht erlaubt, wenn die Beschäftigten durch das Aufzeichnen der Telefongespräche permanent überwacht werden.

4. Gesundheitsdaten im Dienstplan

Dienstpläne sind in vielen Unternehmen für alle Beschäftigten einsehbar. Dies kann sinnvoll sein, um die An- und Abwesenheit im Betrieb sichtbar zu machen

[95] Siehe Art. 6 Abs. 1 Satz 1 lit. a i. V. m. Art. 9 Abs. 2 lit. a DSGVO.
[96] BAG, Urteil vom 27. Juli 2017, 2 AZR 681/16, Rn. 33.
[97] BAG, Urteil vom 28. März 2019, 8 AZR 421/17, Rn. 39 f.

und den Betriebsablauf zu gewährleisten. Es gibt jedoch regelmäßig keinen Grund, in den Dienstplänen Krankenstände von Beschäftigten kenntlich zu machen.

In einem uns vorliegenden Fall wurde die krankheitsbedingte Abwesenheit der Beschäftigten im Dienstplan einer Pflegeeinrichtung mit dem Großbuchstaben K vermerkt. Wir haben die Pflegeeinrichtung auf die Rechtslage hingewiesen, worauf sie uns mitteilte, dass nach Absprache mit dem beauftragten Softwareunternehmen künftig nur noch der Großbuchstabe A für alle Formen der Abwesenheit im Dienstplan vermerkt wird. In einem zweiten Fall gab es ebenso Beschwerden über die Dokumentation des Krankenstands im Dienstplan einer Pflegeeinrichtung. Auf unser Einwirken hin wurde die Datenverarbeitung angepasst und nur noch zwischen Urlaub und ungeplanter Abwesenheit unterschieden. In einem dritten Fall unterschied ein Unternehmen in seinem Dienstplan durch farbige Hervorhebung zwischen spontaner und mittelfristig angekündigter Abwesenheit, um damit auf kurzfristige Änderungen der Schichten besser reagieren zu können. Da die verantwortliche Stelle mitgeteilt hat, dass in einem beispielhaften Zeitraum nur etwas mehr als die Hälfte der kurzfristigen Abwesenheitstage auf Krankmeldungen zurückzuführen war, haben wir die Daten-verarbeitung nicht beanstandet.

Informationen über den Status der Gesundheit einer Person gehören nach Art. 9 Abs. 1 DSGVO zu den besonderen Kategorien personenbezogener Daten. Sie unterstehen einem besonderen Schutz und dürfen nur unter bestimmten Bedingungen verarbeitet werden.[98] Besonders große Rücksicht bei der Verarbeitung muss auf die Vertraulichkeit der Daten genommen werden. Die Kennzeichnung des Krankenstands von Beschäftigen ist in Dienstplänen grundsätzlich nicht notwendig. Zur Koordination der Arbeitsabläufe reicht es regelmäßig aus, die Abwesenheit an sich zu vermerken. In bestimmten Fällen kann es zur kurzfristigen Koordinierung notwendig sein, zwischen spontan auftretender Abwesenheit, auf die bei der Planung aktueller Schichten möglicherweise gesondert Rücksicht genommen werden muss, und längerer, vorherseh-barer Abwesenheit zu unterscheiden. Unzulässig sind selbstverständlich auch Vermerke wie „Kind krank“, „Kur“ usw., die ebenfalls Informationen zum Gesundheitsstatus transportieren. Im Zusammenhang mit einer Dienstplanung sind solche Daten in der Regel nicht relevant und dürfen folglich nicht verarbeitet werden. Zusätzlich ist immer darauf zu achten, dass Dienstpläne – selbst, wenn

[98] Siehe Art. 9 Abs. 2 DSGVO.

sie keine Gesundheitsdaten enthalten – keinen unbeteiligten Dritten oder Beschäftigten, sondern ausschließlich denjenigen Beschäftigten zugänglich sind, die auf die Informationen des Dienstplans angewiesen sind.

Es ist regelmäßig ausreichend, in Dienstplänen die Abwesenheit der Beschäftigten zu vermerken, ohne deren konkreten Grund festzuhalten. Die Verarbeitung von Gesundheitsdaten in Dienstplänen ist in aller Regel nicht zulässig.

5. Nutzung privater Telefonnummern von Beschäftigten

Die Nutzung von privaten Mobilfunknummern von Beschäftigten kann einen unzulässigen Eingriff in deren Privatsphäre darstellen. Die Kontaktaufnahme über eine solche Nummer kann jedenfalls ein Diensttelefon nicht ersetzen und ist damit nicht zulässig, wenn eine Kontaktaufnahme mit den Beschäftigten zum Betriebsablauf gehört bzw. zur Verrichtung der Arbeitstätigkeit notwendig ist.

In einem uns vorliegenden Fall wurde ein Beschäftigter, der im Bereich des Objektschutzes tätig ist, von seiner Dienststelle mehr als 70-mal über seine private Mobilfunknummer kontaktiert, obwohl er der Nutzung seiner Nummer ausdrücklich widersprochen hatte. Vonseiten der Dienststelle konnten keine überzeugenden Gründe für die Kontaktaufnahme vorgebracht werden, weshalb wir eine Verwarnung gegen die Verantwortliche ausgesprochen haben.

Oft übermitteln Beschäftigte im Rahmen der Bewerbung oder zur Kontaktaufnahme in Notfällen ihre private Telefonnummer an die Arbeitgeber:innen. Das bedeutet jedoch nicht, dass die Beschäftigten auch im laufenden Beschäftigungsverhältnis darüber kontaktiert werden dürfen, um etwa das dienstliche Geschäft zu organisieren. So geht das Landesarbeitsgericht (LAG) Thüringen etwa davon aus, dass die Freizeit unzumutbar beeinträchtigt werden würde, wenn Beschäftigte damit rechnen müssen, von ihren Arbeitgeber:innen über ihr privates Mobiltelefon kontaktiert zu werden.[99]

Laut Sachverhalt, der dem Urteil des LAG Thüringen zugrunde lag, wurden die Beschäftigten eines kommunalen Arbeitgebers nach Abschaffung der Rufbereitschaft bei Notfällen über ihre Privatnummer gefragt, ob sie Arbeitsschichten übernehmen könnten. Das Gericht problematisierte das Abhängigkeitsverhältnis der Beschäftigten und stellte heraus, dass sich Freizeit gerade dadurch auszeichne, den Arbeitgeber:innen nicht zur

[99] LAG Thüringen, Urteil vom 16. Mai 2018, 6 Sa 442/17.

Verfügung stehen zu müssen. Den Anrufen seitens der Arbeitgeber:innen könne sich nur dann entzogen werden, wenn das eigene Mobilfunkgerät während der Freizeit nicht genutzt werde. Dies widerspreche aber dem Prinzip, selbstbestimmt über die Gestaltung der freien Zeit verfügen zu können. Da Mobiltelefone in der alltäglichen Lebensgestaltung von großer Bedeutung sind, sei ein solcher Eingriff schwerwiegend.[100]

Natürlich stellt die Nutzung der privaten Telefonnummer nicht in jedem Fall einen Datenschutzverstoß dar. Entscheidend ist, aus welchen Gründen die Beschäftigten kontaktiert werden: So kann beispielsweise die Annahme eines Notfalls bei den Beschäftigten, der Hinweis auf Gefahren in den Betriebsräumen, der kurzfristige Dienstausfall usw. aufgrund der Fürsorgepflicht der Arbeitgeber:innen einen Anruf begründen. Die Anhaltspunkte für einen solchen Notfall müssen aber im Zweifelsfall dargelegt werden.

Arbeitgeber:innen können nicht das Diensttelefon einsparen, indem sie Beschäftigte zur Durchführung des Betriebsablaufs standardmäßig privat kontaktieren. Die Einwilligung der Beschäftigten in die Nutzung der privaten Mobilfunknummer zu dienstlichen Zwecken kann regelmäßig nur dann eine wirksame Rechtsgrundlage sein, wenn den Beschäftigten hieraus ein wirtschaftlicher oder rechtlicher Vorteil entsteht.[101] Aufgrund der Freiwilligkeit kann die einmal erteilte Einwilligung jederzeit zurückgezogen werden.

6. Berechtigungsnachweis für Empfänger:innen von Sozialleistungen

Nach einer Entscheidung des Rats der Bürgermeister (RdB) vom Juli 2020[102] wurden die bislang von den Bürgerämtern ausgestellten Berlinpässe zu Beginn dieses Jahres durch Berechtigungsnachweise ersetzt, die direkt von den leistungsgewährenden Sozialbehörden ausgestellt werden.[103] Wie die ehemaligen Berlinpässe ermöglichen die Berechtigungsnachweise Empfänger:innen von Sozialleistungen den vergünstigten Zugang zu Bildung, Sport und Kultur und insbesondere den Erwerb eines ermäßigten Tickets für den öffentlichen Nahverkehr. Die Umstellung auf das neue Verfahren stellt die Behörden allerdings vor erhebliche Herausforderungen.

Umstellung auf den Berechtigungsnachweis

Nach Beschluss des Rates der Bürgermeister (RdB) vom Juli 2020 wurden die bisher von den Bürgerämtern ausgestellten Berlinpässe zu Beginn des Jahres 2021 durch Berechtigungsnachweise ersetzt, welche fortan direkt von den zuständigen leistungsgewährenden Behörden ausgestellt wurden. Diese Berechtigungsnachweise ermöglichten den Empfängerinnen und Empfängern von Sozialleistungen – wie zuvor der Berlinpass – den vergünstigten Zugang zu Angeboten in den Bereichen Bildung, Sport, Freizeit und Kultur sowie insbesondere den Erwerb eines ermäßigten Tickets für den öffentlichen Nahverkehr.

[100] Ebd., Rn. 45.
[101] Siehe § 26 Abs. 2 Satz 2 Bundesdatenschutzgesetz (BDSG).
[102] RdB, Beschluss vom 23. Juli 2020, Nr. R-880/2020.
[103] Siehe JB 2020, 12.1; JB 2022, 6.2.

Bereits zu Beginn der Einführung kam es zu Engpässen und Verzögerungen bei der Ausstellung der Berechtigungsnachweise sowie der VBB-Kundenkarte Berlin S, die zur Gültigkeit des ermäßigten Nahverkehrstickets erforderlich ist. Aus diesem Grund wurde die seit der Corona-Pandemie bestehende „Übergangslösung" bis in die ersten Monate dieses Jahres hinein verlängert, d. h. die Anspruchsberechtigten waren gezwungen, ihren Vergünstigungsanspruch im öffentlichen Nahverkehr anhand ihrer originalen Leistungsbescheide gegenüber den Fahrkartenkontrolleur:innen nachzuweisen. Diese Situation ist für die betroffenen Personen häufig sehr unangenehm, da diese Form des Nachweises beispielsweise auch anderen Fahrgästen nicht verborgen bleibt. Wir haben gegenüber der Senatsverwaltung deutlich gemacht, dass die Verwendung der originalen Leistungsbescheide beendet werden muss. Zugleich haben wir uns für die Entwicklung eines datenschutzkonformen Verfahrens beim Berechtigungsnachweis eingesetzt.

Die ersten Überlegungen zur Weiterentwicklung des Projekts Berechtigungsnachweis waren mit den datenschutzrechtlichen Grenzen bei der Weitergabe besonders schützenswerter Daten, zu denen auch die Sozialdaten zählen, nicht vereinbar. Sie sahen eine Weitergabe der personenbezogenen Daten der Anspruchsberechtigten durch die Sozialleistungsträger und andere Behörden direkt an die Berliner Verkehrsbetriebe (BVG) oder externe Dienstleister vor. Wir haben den Projektverantwortlichen den datenschutzrechtlichen Rahmen für eine Weiterentwicklung des Verfahrens skizziert und unsere Positionen zu den datenschutzrechtlich nicht tragfähigen Lösungsvorschlägen verdeutlicht.

Bereits vor Beginn der Umstellung ergaben sich jedoch verschiedene Herausforderungen, die von der für Soziales zuständigen Senatsverwaltung in Zusammenarbeit mit weiteren beteiligten Stellen adressiert werden mussten, weshalb das neue Verfahren zunächst als Interimsverfahren galt. Da die Berliner Jobcenter, die nicht in Landesverantwortung stehen, aufgrund der bundesweit eingesetzten Fachprogramme keine Möglichkeit hatten, die Berechtigungsnachweise zusammen mit dem Leistungsbescheid zu versenden, wurde eine Vereinbarung mit der Regionaldirektion Berlin-Brandenburg getroffen. Diese ermöglichte die regelmäßige, jedoch zeitversetzte Zustellung der Berechtigungsnachweise an die Leistungsempfangenden.

Eine weitere Herausforderung stellte die mangelnde Fälschungssicherheit der neuen Berechtigungsnachweise dar, weswegen der zuständige ÖPNV-Betreiber diese nicht als alleinigen Nachweis für den Erhalt von Ermäßigungen im öffentlichen Nahverkehr akzeptierte. Leistungsempfangende waren daher verpflichtet, zusätzlich eine Kundenkarte („VBB-Kundenkarte Berlin S") bei der BVG zu beantragen, die sie als Berechtigungsnachweis für die ermäßigte Nutzung des ÖPNV nutzen konnten. Diese Umstände erschwerten die Implementierung des neuen Verfahrens erheblich.

In Anbetracht dieser Sachlage wurde entschieden, eine „Übergangsregelung" einzuführen. Diese Übergangsregelung ermöglichte es den Leistungsempfangenden, mittels ihres Leistungsbescheides weiterhin sämtliche Vergünstigungen im Land Berlin in Anspruch zu nehmen, sollte der Berechtigungsnachweis oder die VBB-Kundenkarte Berlin S noch nicht zugestellt worden sein. Im Hinblick auf datenschutzrechtliche Bedenken wurde mehrfach darauf hingewiesen, dass eine Kopie des Leistungsbescheides zu verwenden sei und nicht relevante Angaben im Bescheid (z. B. Leistungsbeträge oder Kontodaten) nach Möglichkeit zu schwärzen sind.

Nach dem anfänglich holprigen Start des Verfahrens wurden zusätzliche Maßnahmen ergriffen, um dieses Verfahren sowohl effizienter als auch datenschutzkonformer für die Leistungsempfangenden zu gestalten. Unter anderem wurde ergänzend zur regulären Ausstellung des Berechtigungsnachweises durch die Berliner Jobcenter die Möglichkeit einer Ersatzausstellung im Falle von Nichtzugang oder Verlust des Nachweises implementiert.

Da dieses Verfahren von Beginn an als Interimslösung vorgesehen war, wurde stetig im Hintergrund in enger Zusammenarbeit mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit sowie weiteren Beteiligten gearbeitet.

Es ist notwendig, das aktuelle Verfahren der Ausstellung der Berechtigungsnachweise durch die Sozialleistungsträger, wie Grundsicherungsämter, Jobcenter und weitere Behörden, zu optimieren und ein tragfähiges digitales Verfahren einzuführen. Allerdings ist es ebenso notwendig, die Persönlichkeitsrechte der Betroffenen angesichts der besonders schützenswerten Daten im Blick zu behalten. Dies ist kein Widerspruch, da durchaus datenschutzkonforme Lösungsansätze denkbar sind.

Lösungsvorschläge zur Digitalisierung des Verfahrens

Seit Einführung des neuen Verfahrens zur Ausstellung des Berechtigungsnachweises sowie der VBB-Kundenkarte Berlin S, welches von Beginn an als Übergangslösung gedacht war, arbeiten die Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung, die Berliner Beauftragte für Datenschutz und Informationsfreiheit sowie die weiteren beteiligten Institutionen kontinuierlich an der Entwicklung einer langfristig tragfähigen, digitalen Lösung für die Bürger:innen. Ziel war und ist es, ein benutzerfreundliches und sicheres Verfahren zu etablieren, das den Anforderungen an Datenschutz und Effizienz gerecht wird. Verschiedene Lösungsansätze wurden geprüft, jedoch erwiesen sich diese aus datenschutzrechtlicher Sicht als nicht umsetzbar.

Der zuletzt vorgeschlagene Ansatz sah vor, dass Leistungsempfangende nach Erhalt ihres Leistungsbescheids an Automaten der BVG direkt ihr vergünstigtes Ticket für den ÖPNV erwerben können. Hierzu wäre durch die leistungsgewährenden Stellen im Hintergrund eine Datenbank bereitgestellt worden, die nur die notwendigsten Informationen – wie Name, Vorname, Geburtsdatum, Kundennummer/Geschäftszeichen und Leistungszeitraum – enthält. Nach Eingabe dieser Daten durch die Leistungsempfangenden an den Verkaufsautomaten der BVG erfolgt durch diese ein Abgleich mit der Datenbank der leistungsgewährenden Stellen. Anschließend gibt der Verkaufsautomat entweder ein Ticket für die vergünstigte Nutzung aus oder zeigt, bei fehlender Berechtigung, eine entsprechende Fehlermeldung an.

Auch dieser Vorschlag wurde jedoch von der Berliner Beauftragten für Datenschutz und Informationsfreiheit aus datenschutzrechtlichen Gründen als nicht konform eingestuft und konnte daher nicht weiterverfolgt werden.

Das Projekt Berechtigungsnachweis ist seit Beginn an von Umsetzungsproblemen geprägt. Es stellt sich die Frage, warum das bewährte Verfahren zum Berlinpass überhaupt aufgegeben wurde. Die Pläne für die Fortentwicklung und Digitalisierung des Verfahrens werfen nun viele zum Teil komplexe datenschutzrechtliche

Zusammenfassung

Zusammenfassend lässt sich feststellen, dass die Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung tets in engem Austausch mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit

Fragen auf. Wir haben der Senatsverwaltung angeboten, uns auch in Zukunft mit konkreten Lösungsvorschlägen in die Weiterentwicklung des Berechtigungsnachweises für Empfänger:innen von Sozialleistungen einzubringen. Wir halten es für dringend erforderlich, dass zeitnah ein Zustand geschaffen wird, der allen Beteiligten gerecht wird und zugleich die datenschutzrechtlichen Anforderungen erfüllt.

stand und kontinuierlich daran gearbeitet hat, deren Anforderungen umzusetzen. Ein umsetzbares, benutzerfreundliches und sicheres Verfahren zum Erhalt der Vergünstigungen für die berechtigten Bürger:innen, das auch den datenschutzrechtlichen Anforderungen gerecht wird, konnte bisher nicht gefunden werden.

Vor diesem Hintergrund wurde das Interimsverfahren der Ausstellung der Berechtigungsnachweise sowie der VBB-Kundenkarte Berlin S zum 1. Januar 2025 eingestellt. Die bereits und bis zum Ende des Jahres 2024 ausgegebenen VBB-Kundenkarten Berlin S behalten bis zum Ablauf ihrer jeweiligen Gültigkeitsdauer ihre Wirksamkeit.

Der Senat sowie die weiteren beteiligten Institutionen arbeiten weiterhin intensiv an einer optimierten, datenschutzkonformen Lösung für ein zukünftiges Verfahren. Ziel ist es, den Prozess effizienter und bürgerfreundlicher zu gestalten. Der Senat hofft auf eine weiterhin enge Zusammenarbeit mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit, um bestehende Herausforderungen von Beginn an lösungsorientiert und im gegenseitigen Einvernehmen anzugehen.

7. Datenschutzrechtliche Anforderungen an Vor-Ort-Beratungen in Sozialämtern

Um Sozialleistungen zu beantragen, ist es häufig notwendig, einen Vor-Ort-Termin in einem der Sozialämter wahrzunehmen. Aufgrund eines Hinweises haben wir uns in einem Amt für Soziales die örtlichen Gegebenheiten angesehen und dies zum Anlass genommen, datenschutzrechtliche Mindestanforderungen an die Ausgestaltung solcher Räume zu erarbeiten.

Vor dem Hintergrund der Corona-Pandemie waren Beratungsgespräche in einem Amt für Soziales auf dem Flur der Behörde abgehalten worden. Bei unserem Besuch konnten wir uns allerdings davon überzeugen, dass diese Form der Beratung inzwischen eingestellt worden war. Die Beratungsgespräche finden wieder innerhalb der Doppelbüros zwischen den Sachbearbeiter:innen und ihren Klient:innen statt. Wir haben jedoch festgestellt, dass die Zwischentüren zu den angrenzenden Räumen offen gehalten werden und dementsprechend Gespräche innerhalb der nebenliegenden Büros mitgehört werden können. Auf Nachfrage hat das Amt für Soziales für uns nachvollziehbar darlegt, dass dieses Verfahren aus einer Abwägung der verschiedenen Interessen resultiert: auf der einen Seite die

Vertraulichkeit der Gespräche zu wahren, auf der anderen Seite die Sicherheit der Beschäftigten zu gewährleisten. Regelmäßige verbale und physische Angriffe auf die Sachbearbeiter:innen machten es notwendig, Maßnahmen zu ergreifen, die eine schnelle Hilfe durch die Kolleg:innen und das Wachpersonal ermöglichen. Das Offenhalten der Bürotüren habe sich bewährt, um diesem Anliegen nachzukommen.

Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind bzw. nur an diese weitergegeben werden.[104] Eine unrechtmäßige Verarbeitung von personenbezogenen Daten liegt somit vor, sobald Sozialdaten dritten Personen, etwa anderen Klient:innen, oder aber auch unbefugten Beschäftigten, die für andere Bereiche des Sozialleistungsträgers zuständig sind, offenbart werden, beispielsweise dadurch, dass Beratungsgespräche mitgehört werden können. Um unbefugte Offenlegungen von Sozialdaten zu verhindern, ist der Sozialleistungsträger als Verantwortlicher der Datenverarbeitung verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten der Klient:innen zu ergreifen.[105] Gleichzeitig ist der Sozialleistungsträger als Verantwortlicher in der Pflicht, die Sicherheit seiner Beschäftigten zu gewährleisten.[106] Die Maßnahmen zum Schutz der Persönlichkeitsrechte der Klient:innen müssen folglich mit den Maßnahmen zum Schutz der Beschäftigten abgestimmt werden.

Wir haben mit dem Amt für Soziales erörtert, welche Maßnahmen zu ergreifen sind, um sowohl den Persönlichkeitsrechten der Klient:innen als auch dem Schutz der Beschäftigten gerecht zu werden. Insbesondere bei Vor-Ort-Beratungen müssen die eingesetzten technisch-organisatorischen Maßnahmen sicherstellen, dass Sozialdaten weder Dritten noch unzuständigen Beschäftigten offenbart werden.

VII. Wohnen, öffentlicher Raum und Videoüberwachung

1. Datenerhebung für den Mietspiegel 2024

Für das kommende Jahr plant die Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen (SenStadt) die Erstellung eines neuen qualifizierten Mietspiegels. Bei

[104] Siehe § 35 Abs. 1 Satz 2 SGB I.
[105] Siehe Art. 32 Abs. 1 Satz 1 DSGVO.
[106] Siehe u. a. § 618 Abs. 1 BGB.

den dafür erforderlichen Umfragen, die für die ausgewählten Mieter:innen verpflichtend sind, wird eine Vielzahl personenbezogener Daten erhoben. Wir erklären die rechtlichen Grundlagen für die Erhebung und Verarbeitung der teils sehr detaillierten Datensätze.

Für die Erstellung eines qualifizierten Mietspiegels sind konkrete Angaben zu Miethöhe, Wohnumfeld, Größe und Ausstattung der Mietwohnungen notwendig. Diese Angaben müssen in ausreichender Zahl vorliegen, um repräsentativ zu sein. Dementsprechend wurden zwischen September und Dezember dieses Jahres zufällig ausgewählte Mieter:innen mit einem Kurzfragebogen angeschrieben und um Auskunft gebeten. Sofern deren Wohnungen den gesetzlichen Rahmenbedingungen für den qualifizierten Mietspiegel entsprachen, folgte der Umfrage noch eine zusätzliche persönliche Befragung. Aus den gewonnenen Daten wird dann die ortsübliche Vergleichsmiete berechnet, die Mieter:innen und Vermieter:innen als Einordnung dienen soll, ob die von ihnen verlangte bzw. bezahlte Miete angesichts der Lage, Größe und Ausstattung des Wohnraums angemessen ist.

Die Datenerhebung und -verarbeitung stützt sich auf Art. 238 Einführungsgesetz zum Bürgerlichen Gesetzbuch (EGBGB), der die Datenverarbeitung für qualifizierte Mietspiegel regelt und zudem eine Auskunftspflicht für alle befragten Mieter:innen und Vermieter:innen vorsieht.[107] Die versendeten Umfragebögen sind zwar umfangreich und sehr detailliert, die Beantwortung ist aber zur Erstellung der qualifizierten Mietspiegel erforderlich und rechtlich zulässig. So setzt sich der Mietspiegel aus einer Vielzahl von Elementen zusammen. Ein Teil davon muss bei Mieter:innen und Vermieter:innen erhoben werden; bestimmte Angaben können nur die Mieter:innen machen, wie etwa über den aktuellen Zustand von Bad und WC oder die derzeitige Ausstattung von Küche und Wohnung. Die erhobenen Daten müssen unverzüglich gelöscht werden, wenn ihre Verarbeitung für die Erstellung des Mietspiegels nicht mehr erforderlich ist. Sollten die Daten für eine Anpassung des Mietspiegels benötigt werden, sind sie spätestens drei Jahre nach ihrer Erhebung zu löschen.[108]

Die verpflichtende Angabe vieler Details zu den eigenen Wohnverhältnissen, die für die Erstellung des qualifizierten Mietspiegels abgefragt werden, führt bei ei-

[107] Art. 238 § 2 EGBGB.
[108] Art. 238 § 3 Abs. 2 Satz 2 EGBGB.

nigen Bürger:innen verständlicherweise zu Verunsicherung. Die rechtlichen Grundlagen für die Erhebung und Verarbeitung der Daten sind aber datenschutzrechtlich nicht zu beanstanden. Dennoch müssen sich die Auskünfte zur Umfrage auf die tatsächlich notwendigen Angaben beschränken. Bei Zweifeln am Umgang mit den eigenen Daten können Umfrageteilnehmer:innen ihr Auskunftsrecht gegenüber der Senatsverwaltung sowie dem durchführenden Institut geltend machen.

2. Wissenschaftliche Auswertung als Rechtsgrundlage für die Erprobung von Lärmblitzern

Die Senatsverwaltung für Mobilität, Verkehr, Klimaschutz und Umwelt (SenMVKU) hat ein Projekt zur Erprobung eines Lärmblitzersystems am Kurfürstendamm durchgeführt. Dieses wird derzeit von der Technischen Universität (TU) Berlin im Rahmen eines Forschungsprojekts ausgewertet. Wir haben die Senatsverwaltung im Vorfeld des Projekts ausführlich beraten und die einzuhaltenden Datenschutzanforderungen definiert.

Das Lärmblitzersystem erfasst mittels Mikrofone und Kameras Kraftfahrzeuge, die einen bestimmten Dezibel-Grenzwert überschreiten. In Frankreich werden mithilfe solcher Systeme Bußgelder gegen Halter:innen zu lauter Kraftfahrzeuge erlassen. In Deutschland fehlt es für die Erfassung von Kennzeichen zu lauter Kraftfahrzeuge zum Zweck, Bußgelder zu verhängen, an einer Rechtsgrundlage. Die Senatsverwaltung wollte zunächst die Funktionsfähigkeit des Systems erproben, um auf Basis der Ergebnisse den gesetzgeberischen Handlungsbedarf hinsichtlich der die Grenzwerte überschreitenden Kraftfahrzeuge festzustellen.

Um das Projekt durchführen zu können, musste die Senatsverwaltung zunächst die Kennzeichen der erfassten Kraftfahrzeuge an das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) und das Kraftfahrt-Bundesamt (KBA) übermitteln. Diese haben der Senatsverwaltung wiederum einige technische Daten zu den Kraftfahrzeugen übersendet, etwa die Fahrzeugklasse, den benötigten Kraftstoff oder die Motorleistung. Die Senatsverwaltung hat die Kennzeichen sodann aus den Datensätzen entfernt und diese mit den durch das System aufgenommenen Videos an die TU Berlin weitergegeben. Dort sollen die technische Zuverlässigkeit des Systems und die erfassten Grenzwertüberschreitungen im Rahmen einer Masterarbeit ausgewertet und das Potenzial der Verringerung von Lärmbelästigungen durch den Einsatz von Lärmblitzersystemen geprüft werden.

Die mit dem System erhobenen Kraftfahrzeug-Kennzeichen sind personenbezogene Daten der Halter:innen. Da die Erhebung der Daten nicht zur Erfüllung der gesetzlich der Senatsverwaltung zugewiesenen Aufgaben erforderlich war, kam § 3 Berliner Datenschutzgesetz (BlnDSG) als Verarbeitungsgrundlage nicht in Betracht. Die Senatsverwaltung führte daher zusätzlich die Forschungsvorschrift in § 17 Abs. 1 Satz 1 BlnDSG[109] an, nach der die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken unter bestimmten Voraussetzungen zulässig sein kann.

Auch wenn die Senatsverwaltung nicht darlegen konnte, inwieweit der bloße Funktionstest der technischen Anlage sowie die Erhebung und Auswertung der durch diese gewonnenen Daten als wissenschaftliche Forschung anzusehen sind, so erhebt sie die personenbezogenen Daten trotzdem nur deshalb, um sie dem Forschungsprojekt an der TU Berlin zur Verfügung zu stellen. Dass die Senatsverwaltung dabei nicht selbst als Forschungseinrichtung fungiert, halten wir für hinnehmbar. Wir haben allerdings gegenüber der Senatsverwaltung deutlich gemacht, dass sie keine eigenen Auswertungen oder über die Datenübermittlung an die TU Berlin hinausgehenden Datenverarbeitungen durchführen darf. Zudem haben wir von der Senatsverwaltung flankierende Maßnahmen, wie etwa die Einhaltung ihrer datenschutzrechtlichen Informationspflichten[110] durch die Aufstellung von Hinweisschildern im Bereich der Datenerhebung, gefordert und darauf gedrängt, neben der unverzüglichen Löschung der erhobenen Datensätze von allen Beteiligten (Senatsverwaltung, LABO und KBA) auch die Löschung damit einhergehender E-Mails sowie auf Datenträgern gespeicherter Inhalte vorzunehmen.

Öffentliche Stellen können die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken auf § 17 Abs. 1 Satz 1 BlnDSG stützen, auch wenn sie die Forschung nicht selbst durchführen, sondern die Daten an Forschungseinrichtungen weiterleiten. Auf § 3 BlnDSG können Verarbeitungen personenbezogener Daten nur dann gestützt werden, wenn diese eine sehr geringe Eingriffsintensität haben. Zudem sind strenge Maßstäbe an die Erforderlichkeit im Sinne des § 3 BlnDSG anzulegen: Datenverarbeitungen müssen zur Erfüllung der gesetzlich zugewiesenen Aufgaben erforderlich, d. h. zwingend notwendig sein.

[109] I. V. m. Art. 6 Abs. 1 Satz 1 lit. e Alt. 1 Datenschutz-Grundverordnung (DSGVO).
[110] Siehe Art. 13 Abs. 1 und 2 DSGVO.

3. Ausweiskontrollen und Videoüberwachung in Freibädern

Im Sommer dieses Jahres kam es in einigen Freibädern zu gewalttätigen Vorfällen. Die Berliner Bäder-Betriebe machten daraufhin den Zutritt zu sämtlichen von ihnen betriebenen Freibädern von der Vorlage eines Ausweisdokuments abhängig und führten in einigen davon eine Videoüberwachung der Ein- und Ausgangsbereiche ein. Nach Anfragen betroffener Personen und Pressevertreter:innen haben wir die Berliner Bäder-Betriebe um Erläuterung gebeten.

Infolge von Gewaltvorfällen in der Sommerbadesaison 2023 wurde die Arbeitsgruppe Sicherheit in Freibädern (AG Sichere Freibäder), u.a. bestehend aus Vertreterinnen und Vertretern der Senatsverwaltung für Inneres und Sport, der Polizei Berlin, der Berliner Bäder-Betriebe (BBB) und der Senatsverwaltung für Bildung, Jugend und Familie gegründet. Unter der Federführung der Senatsverwaltung für Inneres und Sport erarbeitete die AG Sichere Freibäder einen ganzheitlichen Maßnahmenkatalog aus Service, Prävention und Sicherheit zur Bewältigung der Lage.

Der Maßnahmenkatalog umfasst neben einer Reihe von Maßnahmen, u.a. die Pflicht zum Mitführen von Identitätsnachweisen (Ausweiskontrolle) und den Einsatz von Kamera-überwachungsanlagen in Ein- und Ausgangsbereichen (Videoüberwachung).

Die Berliner Bäder-Betriebe führten eine Sichtkontrolle der Ausweisdokumente sämtlicher Badegäste durch. Die bloße Sichtung und damit Wahrnehmung personenbezogener Daten ohne anschließende Weiterverarbeitung ist zwar aufgrund der geringen Eingriffstiefe ein Grenzfall der Anwendbarkeit des Datenschutzrechts. Dennoch lassen sich Datenschutzrisiken für die betroffenen Personen nicht ausschließen. So lässt etwa bereits ein zugeklappter Reisepass die Staatsangehörigkeit der betroffenen Person erkennen. Dies gilt nicht nur gegenüber dem Sicherheitspersonal, sondern auch gegenüber anderen in der Warteschlange stehenden Badegästen. Der Begriff der Verarbeitung ist weit auszulegen. Er erfasst jeden Vorgang im Zusammenhang mit personenbezogenen Daten.[111] Es kommt weder darauf an, ob automatisierte Verfahren eingesetzt werden, noch ob die Daten nach der Erhebung gespeichert werden. Vor dem Hintergrund der möglichen Diskriminierungsrisiken liegt bereits in der bloßen Wahrnehmung der personenbezogenen Daten eine Verarbeitung dieser Daten mit der Folge eines nicht nur unerheblichen Eingriffs vor.

Seit Juli 2023 ist der Zutritt in die Sommerbäder nur bei Mitführen eines amtlichen Lichtbildausweises für alle Besuchenden ab 14 Jahren möglich.

Nach Auffassung des Senats ist die Maßnahme, den Zutritt zu den Freibädern der BBB nur bei Mitführen und nach Sichtkontrolle eines Identitätsnachweises zu ermöglichen, zur Aufgabenerfüllung der BBB erforderlich. Rechtsgrundlage der Maßnahme ist Art. 6 Abs. 1 Satz 1 lit. e) DSGVO i.V.m. § 23 Bäder-Anstaltsgesetz (BBBG). Gemäß § 23 BBBG ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur Erfüllung der im BBBG genannten Aufgaben erforderlich ist.

Die Berliner Bäder-Betriebe dürfen personenbezogene Daten verarbeiten, allerdings muss dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sein.[112] Es gehört zu den Aufgaben der Berliner Bäder-Betriebe, die

Aufgabe der BBB ist nach § 3 Abs. 1 BBBG unter anderem der Betrieb der Schwimmbäder. Dazu gehören sowohl die Sicherstellung der Einhaltung eines reibungslosen Betriebes als auch die Gewährleistung der Sicherheit der Mitarbeitenden und der

[111] Siehe Art. 4 Nr. 2 DSGVO.
[112] Siehe § 23 Gesetz über die Anstalt öffentlichen Rechts Berliner Bäder-Betriebe (Bäder-Anstaltsgesetz, BBBG).

Sicherheit ihrer Gäste und ihrer Beschäftigten zu gewährleisten. Die Sichtung der Ausweisdokumente sämtlicher Badegäste ist jedoch zur Erfüllung dieses Zwecks weder geeignet noch erforderlich. Die Maßnahme hilft nämlich nicht dabei, Personen, für die ein Hausverbot besteht, zu identifizieren und Ihnen den Zutritt zu verwehren, denn ein Abgleich mit der Hausverbotsliste erfolgt gerade nicht. Auch ist nicht erkennbar, wie das Sicherheitspersonal nach Sichtung eines Ausweises auf einen Verdachtsfall schließen soll. Ein Konzept hierfür haben die Berliner Bäder-Betriebe nicht vorgelegt. Im Übrigen muss berücksichtigt werden, dass die Berliner Bäder-Betriebe auch in der Vergangenheit bei Vorliegen eines konkreten Verdachtsfalls die Badegäste bereits auffordern konnten, sich zu identifizieren, und ihnen bei Weigerung ggf. den Zutritt verweigern konnten.

Letztlich konnten die Ausweiskontrollen lediglich sicherstellen, dass Personen bei ihrem Badebesuch Ausweise bei sich führen. Nach einem Vorfall wäre es dann möglich gewesen, die Identität festzustellen und ein Hausverbot zu verhängen. Hierbei ist allerdings zu berücksichtigen, dass gerade keine gesetzliche Verpflichtung für die Badegäste besteht, ihre Ausweisdokumente – in diesem Fall dem Sicherheitspersonal – auch

Besuchenden. Durch die beschriebene Verfahrensweise besteht die Möglichkeit, Personen, die in der Vergangenheit die Sicherheit der Badegäste und Beschäftigten gefährdeten, als solche zu identifizieren und ihnen den Zutritt zu verwehren.

Im Rahmen einer Interessenabwägung des Grundrechts auf informationelle Selbstbestimmung der von der Vorlage eines Identitätsnachweises betroffenen Besuchenden nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gegenüber dem Recht auf körperliche Unversehrtheit aller Mitarbeitenden und Besuchenden nach Art. 2 Abs. 2 GG fällt die Abwägung zugunsten der Sicherheit von Mitarbeitenden bzw. Besuchenden aus. Dies liegt insbesondere an der geringen Eingriffsintensität, die mit der Vorlage eines Identitätsnachweises einhergeht.

Die Ausweispflicht ermöglicht es den BBB, bei Verstößen gegen die Haus- und Badeordnung die Erteilung und Einhaltung von Hausverboten sicherzustellen. Die Hausverbote werden in einer digitalen Liste erfasst. Verstößt jemand gegen die Haus- und Badeordnung, kann anhand des Ausweises geprüft werden, ob bereits ein Hausverbot vorliegt. In diesen Fällen kann somit konsequent Anzeige wegen Hausfriedensbruchs erstattet werden. Ein regelhafter Abgleich persönlicher Daten vor Eintritt ins Bad findet hingegen nicht statt, die BBB behalten sich eine anlassbezogene Kontrolle der Ausweise vor, bspw. bei begründetem Verdacht durch Sicherheitskräfte, Mitarbeitende und/ oder Badbesuchende aufgrund persönlichen Wiedererkennens, dass gegen eine den Einlass suchende Person ein Hausverbot besteht. Es wird jedoch das Mitführen eines Identitätsnachweises durch Sichtkontrolle kontrolliert.

Darüber hinaus dient die Ausweispflicht dem Zweck der Kontrolle bei begründetem Verdacht der Erschleichung von Leistungen bzw. der Überprüfung der Rechtmäßigkeit zur Gewährung von Ermäßigungstarifen an Schülerinnen und Schüler, Studierende, Auszubildende und/oder Empfängerinnen und Empfänger von Bürgergeld oder Sozialleistungen.

Im Ergebnis ist die Maßnahme verhältnismäßig und erforderlich, da kein milderes gleichgeeignetes Mittel erkennbar ist, um das Ziel zu erreichen. Sie ist ein wichtiger Baustein, um der Gewalt in den Sommerbädern vorzubeugen und die Sicherheit aller im Bad Anwesenden zu gewährleisten. Die Betroffenen werden durch das Mitführen eines Iden-

vorzuzeigen. Weigerte sich eine betroffene Person, musste auch nach Einführung der Ausweiskontrollen die Polizei zur Identitätsfeststellung hinzugezogen werden. Die Maßnahme und die damit verbundene Verarbeitung personenbezogener Daten erschien daher zur Gewährleistung der Sicherheit in den Bädern nicht als geeignet und erforderlich.

Für die Erforderlichkeit der zeitgleich mit den Ausweiskontrollen eingeführten Videoüberwachung der Ein- und Ausgangsbereiche bei einigen Freibädern haben die Berliner Bäder-Betriebe den Nachweis ebenfalls nicht erbracht. Die Videoüberwachung diente im Wesentlichen dem Zweck, die Aufnahmen bei erfolgten Straftaten den Strafverfolgungsbehörden zur Verfügung stellen zu können. Begeht eine Person mutmaßlich eine Straftat und verlässt das jeweilige Freibad ohne vorherige Identifizierung durch das Sicherheitspersonal oder die hinzugerufene Polizei, wäre eine Identifizierung ohne die Kameraaufnahmen zwar tatsächlich nur schwer möglich. Die Erforderlichkeit für eine dauerhafte Überwachung der öffentlich zugänglichen Eingangsbereiche muss vom Verantwortlichen allerdings nachgewiesen werden, etwa durch Zahlen, wie viele Straftaten in der Vergangenheit verübt wurden und Verdächtige aufgrund fehlender Videoüberwachung nicht identifiziert werden konnten. Einen Nachweis legten uns die Berliner Bäder-Betriebe trotz Nachfrage jedoch nicht vor.

Wir haben den Berliner Bäder-Betrieben in Bezug auf die Sommersaison 2023 unsere datenschutzrechtliche

titätsnachweises und die Sichtkontrolle nicht gezwungen, ihre Identität preis zu geben. Ihnen wird jedoch der Zugang zum Freibad verwehrt, wenn sie grundsätzlich anonym bleiben und keinen Ausweis mitführen wollen. Dies ist hinnehmbar, da es für die BBB keinen Kontrahierungszwang gibt, den Zugang zum Schwimmbad zu gewährleisten. Zudem wiegen die Gefahren, dass gewaltbereite Besuchende die Rechte anderer Besuchenden stören, deutlich schwerer.

Seit August 2023 sind die Ein- und Ausgangsbereiche der Sommerbäder Neukölln, Pankow, Am Insulaner und Kreuzberg durch Videokameras überwacht. In der Badesaison 2024 wurde die Videoüberwachung der Ein- und Ausgangsbereich auf das Kombibad Gropiusstadt ausgeweitet.

Auch die Videoüberwachung hält der Berliner Senat gemäß § 20 BlnDSG für zulässig, weil sie zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe und zur Wahrnehmung des Hausrechts in den Sommerbädern erforderlich ist.

Die Videoüberwachung ist auf die Ein- und Ausgangsbereiche von den fünf Bädern beschränkt, in denen es in der Vergangenheit immer wieder zu sicherheitskritischen Vorfällen und der Gefährdung der körperlichen Unversehrtheit von Besuchenden und Beschäftigten kam. In allen fünf Bädern wird ausschließlich während der Öffnungszeiten der Ein-/Ausgansbereich des Schwimmbades von der Videoüberwachung erfasst.

Analog zu der Ausweispflicht hat die Videoüberwachung in erster Linie einen präventiven Charakter und dient der Vorbeugung von Straftaten im Vorfeld und ermöglicht zudem die Identifizierung von Tatverdächtigen im Nachgang. Sie leistet somit - unabhängig von der Anzahl angeforderter Bilder durch die Berliner Strafverfolgungsbehörden - einen wichtigen Beitrag zur Sicherheit in den Bädern und trägt dazu bei, das Sicherheitsniveau und -gefühl der Mitarbeitenden sowie der Besucherinnen und Besucher im Hinblick auf etwaige Übergriffe zu erhöhen. Allein das Vorhandensein einer Videoüberwachung und das damit einhergehende Abschreckungspotential kann dazu führen, dass potentielle Tatpersonen vom Besuch bzw. Eintritt in einem Sommerbad abgehalten werden.

Bewertung mitgeteilt und Beratung zur Evaluation der Maßnahmen sowie ihrer etwaigen Fortführung angeboten.

Allein die Sichtung von Ausweisdokumenten kann bereits eine Verarbeitung personenbezogener Daten darstellen, unabhängig davon, ob die Daten auch gespeichert werden. Auch wenn die Eingriffstiefe zunächst gering erscheint, birgt die Datenverarbeitung Diskriminierungsrisiken für die betroffenen Personen. Die Ausweiskontrolle kann nur dann rechtmäßig sein, wenn sie zur Gewährleistung der Sicherheit in den Bädern geeignet und erforderlich ist. Wird zusätzlich eine Videoüberwachung eingesetzt, muss diese einen durch Nachweise erbrachten messbaren Mehrwert für die Identifizierung von Straftäter:innen aufweisen, um datenschutzrechtlich zulässig zu sein. Erfüllt sie diese Anforderung nicht, ist von ihrem Einsatz abzusehen.

Die Vorlagepflicht eines Identitätsnachweises (Ausweiskontrolle) und der Einsatz von Videoüberwachung sind Teile des ganzheitlichen Konzeptes aus Service, Prävention und Sicherheit, bestehend aus verschiedenen Maßnahmen (u.a. Verstärkung der Zaunanlagen, Deeskalationstraining, Steuerung von Besucherströmen durch Ampelsystem, betreute Sportangebote „SpOrt im Freibad“). Alle Maßnahmen können hiernach nur in ihrer Gesamtheit und in der Gesamtwirkung betrachtet werden.

In der Vergangenheit kam es in den betroffenen Bädern mehrfach zu sicherheitsrelevanten Vorfällen. Nach Einführung des Maßnahmenbündels im vergangenen Jahr 2023/2024 ist eine deutliche Beruhigung der Situation zu verzeichnen, welche sich in der statistischen Erfassung widerspiegelt:

- Im Vergleich zur Freibadsaison 2023 mit drei Badräumungen sowie einer vorzeitigen Badschließung aufgrund von Gewaltvorfällen, kam es im Jahr 2024 lediglich zu einer vorzeitigen Badschließung aufgrund gewalttätiger Auseinandersetzungen unter Gästen sowie gegen BBB-Mitarbeitende und Sicherheitskräfte.
- Im Jahr 2023 wurden insgesamt 310 Straftaten mit der Tatörtlichkeit „Freibad“ erfasst, im Jahr 2024 waren es bis zum 30. September hingegen insgesamt nur noch 254 Fälle.
- In Bezug auf die „Gewaltdelikte“ (Straftatengruppen mit Straftaten gegen das Leben, Straftaten gegen die sexuelle Selbstbestimmung, Straftaten gegen die persönliche Freiheit sowie Rohheitsdelikte) wurden im Jahr 2023 87 Fälle registriert. Im Jahr 2024 wurden hingegen 61 Gewaltdelikte verzeichnet.
- Insgesamt wurden durch die Polizei Berlin im Jahr 2023 7.473,02h Einsatzkräftestunden geleistet, im Jahr 2024 sank der Wert hingegen auf 5.809,37h.
- Bis Mitte September 2024 erteilten die BBB insgesamt 254 schriftliche Hausverbote im Vergleich zum Vorjahr mit 163 Hausverboten. Der Anstieg ist dabei auf die Ausweispflicht und die damit verbun-

dene konsequentere Ahndung von Verstößen gegen die Haus- und Badeordnung zurückzuführen.

- Nach der Einschätzung der Beschäftigten und der Polizei Berlin sowie anhand der Rückmeldungen von Besuchenden tragen die Service-, Präventions- und Sicherheitsmaßnahmen wesentlich zu der friedlicheren Freibadsaison in 2024 bei. Die BBB erzielten in diesem Zusammenhang einen Rekordwert an 1,965 Mio. Besuchenden in den Sommerbändern (Vorjahr: ca. 1,7 Mio.).
- Die Vielfalt und der Mix der unterschiedlichen Maßnahmen haben im Ergebnis aus Sicht aller Beteiligten insgesamt zu einer Befriedung der Sommerbäder sowie zu einer Steigerung des subjektiven Sicherheitsgefühls sowie der objektiven Sicherheit der Besuchenden und Mitarbeitenden der BBB geführt und sich bewährt.

Aus Sicht des Senats ist der im Jahresbericht 2023 der Berliner Beauftragten für Datenschutz und lnformationsfreiheit geforderte (statistische) Nachweis eines messbaren Mehrwerts, aufgrund der eingeführten Sicherheits-, Service- und Präventionsmaßnahmen gegeben. Eine eindeutige (statistische) Zuordnung des messbaren Mehrwerts ausschließlich zu den beiden im Fokus stehenden Maßnahmen (Ausweiskontrolle und Videoüberwachung) - wie im Bericht darüber hinaus gefordert - um datenschutzrechtlich zulässig zu sein, ist einerseits aufgrund des Präventionscharakters der beiden Maßnahmen nicht zielführend und andererseits aufgrund ihrer Eigenschaft als Bestandteile eines ganzheitlichen Gesamtkonzeptes nicht möglich.

Vor diesem Hintergrund vertritt der Senat hinsichtlich der Identitäts- bzw. Ausweiskontrolle und Videoüberwachung die Auffassung, dass es sich bei beiden Einzelmaßnahmen im Gesamtkontext um erforderliche und verhältnismäßige Bausteine zur Steuerung und Sicherung des Badebetriebes, Gefahrenabwehr, Durchsetzung des Hausrechts und Erfüllung der Betreiberpflichten handelt.

Ausweiskontrolle und punktuelle Videoüberwachung sind nach der gemeinsamen Rechtsauffassung des Senats und der BBB hiernach datenschutzrechtlich nicht zu beanstanden.

Die bisherigen umgesetzten Service-, Sicherheits- und Präventionsmaßnahmen, darunter die Aus-

weispflicht und Kameraüberwachung in den Sommerbädern, sollen daher auch in der kommenden Freibadsaison in 2025 fortgeführt werden. Dabei soll das Beratungsangebot seitens der Berliner Beauftragten für Datenschutz und lnformationsfreiheit zur gemeinsamen Evaluation der Maßnahmen sowie ihrer beabsichtigen Fortführung in Anspruch genommen werden.

4. Kennzeichenerfassung zur Ermittlung der Parkdauer

Regelmäßig erhalten wir Beschwerden über Parkhäuser und Parkplätze, die ticket- und teilweise schrankenlos betrieben werden und die Kennzeichen ein- und ausfahrender Kraftfahrzeuge zur Ermittlung der Parkdauer erfassen. Betroffene Fahrzeughalter:innen stellen oftmals die Frage, ob solche Systeme überhaupt rechtmäßig sind. Sie bemängeln, dass sich am Kassenautomaten die Parkdauer anderer in der Parkanlage befindlicher Kraftfahrzeuge anzeigen lässt.

Die Systeme erfassen per Kamera die Kennzeichen der ein- und ausfahrenden Kraftfahrzeuge und speichern diese samt Datum und Uhrzeit als Textdatei ab. Am Kassenautomaten muss dann nur das Kennzeichen eingegeben sowie die erhobene Parkgebühr entrichtet werden. Über Kennzeichen-Erfassungssysteme kann die Parkdauer beweissicher bestimmt und aufgrund des Verzichts auf Papiertickets zudem die Gefahr eines Parkscheinverlusts mit erhöhten Folgekosten vermieden werden.

Die mit der Kennzeichenerfassung verbundene Verarbeitung personenbezogener Daten kann zulässig sein, wenn ausreichende Schutzmaßnahmen ergriffen werden. Es dürfen beispielsweise keine Aufnahmen von Personen angefertigt werden und das erfasste Kennzeichen ist innerhalb weniger Tage nach Bezahlung zu löschen. Auf die Kennzeichenerfassung muss hingewiesen[113] und die Hinweisschilder müssen so positioniert werden, dass Personen, die die Parkanlage potenziell nutzen möchten, diese noch vor Kennzeichenerfassung wieder verlassen können. Sollte dies im Einzelfall aus baulichen Gründen nicht möglich sein, muss ein Zeitfenster eingeräumt werden, in dem betroffene Personen die Parkanlage wieder verlassen können, ohne dass Parkgebühren erhoben werden. Die Fahrzeugkennzeichen müssen in diesem Fall unverzüglich wieder gelöscht werden.

[113] Siehe Art. 13 Abs. 1 und 2 DSGVO.

Beim Bezahlvorgang lässt es sich nicht vermeiden, dass neben den Daten zum eigenen Fahrzeug auch die Anzeige der Parkdauer anderer auf der Parkanlage befindlicher Kraftfahrzeuge möglich ist, wenn deren Kennzeichen in den Kassenautomaten eingegeben werden. Vor dem Hintergrund, dass dies zum einen technisch nicht zu vermeiden ist und zum anderen nur die Parkdauer anderer Kraftfahrzeuge preisgegeben wird, die ohne Zusatzwissen keine Rückschlüsse auf deren Halter:innen zulassen, halten wir dies für rechtlich hinnehmbar.

Kennzeichen-Erfassungssysteme in ticket- und schrankenlosen Parkanlagen sind unter Einhaltung bestimmter Voraussetzungen grundsätzlich zulässig. Allerdings müssen Betreiber:innen dieser Parkanlagen ein besonderes Augenmerk auf die Einhaltung der Datenschutzanforderungen richten, insbesondere ist die Kenn-zeichenerfassung transparent zu machen und die Pflicht zur zeitnahen Löschung der erfassten Daten zu beachten.

5. Luftaufnahmen von Privatgrundstücken per Drohne

Im Rahmen einer beantragten Zwangsversteigerung zum Zweck der Aufhebung einer Eigentümergemeinschaft nahm ein Immobilienunternehmen im Auftrag des zuständigen Amtsgerichts eine Verkehrswertermittlung des betroffenen Grundstücks vor. Zur besseren Begutachtung und Beschreibung des Grundstücks fertigte das Unternehmen Luftbildaufnahmen mit einer Drohne an, ohne zuvor die Einwilligung der betroffenen Grundstücksbesitzer:innen eingeholt zu haben.

Die Rechtmäßigkeit, Luftbilder per Drohne aufzunehmen, ist an den Vorgaben der DSGVO zu messen, wenn die Aufnahmen personenbezogene Daten enthalten. Dies ist bei Luftaufnahmen, die mit einer Adresse referenziert sind, immer der Fall. Aber auch ohne Angabe der konkreten Lage einer Liegenschaft können Luftbilder zumindest personenbeziehbar sein und damit dem Schutzbereich der DSGVO unterliegen, wenn durch sie eine Zuordnung zu einer konkreten Person hergestellt werden kann. Da die Datenverarbeitung im vorliegenden Fall auch nicht ausschließlich im Rahmen persönlicher oder familiärer Tätigkeiten erfolgte, sondern zu gewerblichen Zwecken und zum Zweck der Veröffentlichung stattfand, kommt die DSGVO vollumfänglich zur Anwendung.

Obwohl das Unternehmen vom Gericht beauftragt worden ist, bleibt es für die Erhebung, Verarbeitung und Weitergabe der personenbezogenen Daten bei der Fertigung der Drohnenaufnahmen selbst verantwortlich.

Als Rechtsgrundlage für die Datenverarbeitung des Unternehmens kommt ein berechtigtes Interesse an der Erfüllung der von ihm eingegangenen Verpflichtung zur Erstellung der Grundstücksbewertung in Betracht. Die Verarbeitung zur Wahrung berechtigter Interessen der Verantwortlichen oder Dritten muss auch erforderlich sein.[114] Zudem muss das Interesse des Unternehmens mit den schutzbedürftigen Interessen der betroffenen Personen abgewogen werden. Überwiegt das Interesse der Betroffenen am Schutz ihrer personenbezogenen Daten, kann die Datenverarbeitung nicht auf Art. 6 Abs. 1 Satz 1 lit. f DSGVO gestützt werden.

Zweck der Anfertigung der Luftaufnahmen war, dem zuständigen Gericht aussagekräftige Bilder für Aushänge oder Veröffentlichungen vorzulegen. Auch wenn die Drohnenaufnahmen zum Erreichen dieses Zwecks hilfreich waren, waren sie zur Beschreibung des Grundstücks nicht erforderlich. Es hätten dafür weniger eingriffsintensive Alternativen zur Verfügung gestanden, beispielsweise hätten sich Bilder aus dem Geoportal der Liegenschaftsverwaltung verwenden lassen, die einen ausreichenden Informationswert, wenn auch nicht den gleichen Detailgrad, wie die angefertigten Luftaufnahmen, gehabt hätten. Die Verwendung von Bildern aus dem Geoportal der Liegenschaftsverwaltung wäre in gleicher Weise geeignet gewesen, um einen äußeren Eindruck vom betreffenden Grundstück zu erhalten. Wir haben dies dem Unternehmen mitgeteilt und eine Verwarnung ausgesprochen.[115]

Für die Verwendung von Drohnen, die Bilder mit personenbezogenen Daten anfertigen, ist die DSGVO zu beachten. Sollen Luftaufnahmen eines Privatgrundstücks zu gewerblichen Zwecken erstellt werden, ist in der Regel die zuvor eingeholte Einwilligung der betroffenen Grundstücksbewohner:innen erforderlich.

6. Rechtmäßigkeit der Veröffentlichung umweltbezogener Daten

Die SenMVKU hatte uns 2021 Pläne zu einer Veröffentlichung von grundstücks-genauen Starkregenhinweis- und -gefahrenkarten vorgestellt. Nach erneuter -Prüfung sind wir zum Ergebnis gelangt, dass die unbeschränkte Veröffentlichung solcher -Karten abweichend von unserer bisherigen Bewertung unter bestimmten Voraussetzungen rechtmäßig ist.

[114] Siehe Art. 6 Abs. 1 Satz 1 lit. f DSGVO.
[115] Siehe Art. 58 Abs. 2 lit. b DSGVO.

Die von der Senatsverwaltung vorgestellten Starkregenhinweis- und -gefahrenkarten enthalten personenbezogene Daten.[116] Es handelt sich zwar in erster Linie um umweltbezogene Informationen wie sog. Sach- oder Geodaten, diese können gleichwohl, beispielsweise wenn sie die Überflutungsgefahren einzelner Grundstücke aufzeigen, personenbeziehbar sein. Dies ist dann der Fall, wenn sie grundstücks- oder gebäudegenau sind und das jeweils betroffene Grundstück oder Gebäude im Eigentum einer natürlichen Person steht. Nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) handelt es sich um Informationen über natürliche Personen bzw. die Informationen beziehen sich auf natürliche Personen, wenn sie aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft sind.[117] Die Überflutungsgefahr von Grundstücken hat ebenso wie viele andere umweltbezogene Informationen Auswirkungen auf den Wert der Grundstücke und damit auf die wirtschaftliche Identität der Eigentümer:innen. Insbesondere da die Karten explizit dafür erstellt sind, diese zu präventiven Maßnahmen anzuhalten, sollte eine besondere Gefährdung der Grundstücke vorliegen. Über das Grundbuch oder das Liegenschaftskataster sind die Eigentümer:innen zudem identifizierbar. Das für eine Einsichtnahme regelmäßig erforderliche berechtigte Interesse liegt bei einer erheblichen Anzahl von Personen (etwa Journalist:innen) vor; die Identifizierung ist insoweit einem weiten Personenkreis möglich.

Starkregengefahren- und -hinweiskarten enthalten wichtige Informationen über Gefahren und Gefährdungen bei Starkregen, die für eine wirksame private und öffentliche Vorsorge gegenüber Extremwetterereignissen unerlässlich sind. Damit sind sie nach ihrem Inhalt, ihrem Zweck oder ihren Auswirkungen aber nicht mit einer bestimmten Person verknüpft und geben keine Auskunft über die persönlichen oder sachlichen Verhältnisse einer Person. Auf die Starkregengefahren- und -hinweiskarten bezogen ist zu berücksichtigen, dass diese allein Auskunft über den möglichen Abfluss von Regenmengen auf eine bestimmte Bodenfläche geben. Auskünfte über das Verhalten oder die Verhältnisse einer Person sind damit jedoch weder unmittelbar noch mittelbar verbunden (vgl. Callies/Schumacher, NVwZ 2023, S. 1361, 1365).

Mittelbar können Informationen über die Starkregengefährdung zwar Rückschlüsse auf den wirtschaftlichen Wert eines Grundstücks oder dessen Versicherbarkeit gegenüber extremen Naturereignissen zulassen. Damit bilden sie jedoch einen Teil der Gesamtheit der dem jeweiligen Grundstück anhaftenden Sacheigenschaften, zu der eine Person erst in einen bestimmten rechtlichen oder tatsächlichen Bezug treten muss. Sollten im Einzelfall dennoch personenbezogene Daten offenbart werden, ist dieser Eingriff in das Recht auf Datenschutz mit den privaten und öffentlichen Interessen an einer wirksamen Gefahrenvorsorge abzuwägen. Dabei ist zu berücksichtigen, dass einer nach Ausmaß und Intensität relativ geringen Beeinträchtigung der informationellen Selbstbestimmung das grundrechtlich geschützte Interesse an der Vorsorge vor Beeinträchtigungen von Leib, Leben und Eigentum bei Extremereignissen und das öffentliche Interesse an der Anpassung urbaner Lebensräume an Starkregenereignisse gegenüberstehen. Im Übrigen ist die öffentliche Verbreitung von Informationen über örtliche Starkregengefahren das mildere Mittel gegenüber Eingriffen in das Sach- und Grundeigentum durch verpflichtende Maßnahmen der Starkregenanpassung (vgl. Callies/Schumacher, NVwZ 2023, S. 1361, 1367).

Für die Veröffentlichung solcher Karten benötigen öffentliche Stellen dementsprechend eine spezifische Rechtsgrundlage.[118] Bei unserer datenschutzrechtlichen Neubewertung sind wir zum Ergebnis gekommen, dass § 10 Abs. 1 Umweltinformationsgesetz (UIG) und

Zum Erfordernis einer Drittbeteiligung bleibt anzumerken, dass die Drittbeteiligung bereits tatbestandlich voraussetzt, dass durch die Bekanntgabe der in Rede stehenden Information Interessen der Betroffenen erheblich beeinträchtigt werden. Dies

[116] Siehe Art. 4 Nr. 1 DSGVO.
[117] EuGH, Urteil vom 20. Dezember 2017, C-434/16, Rn. 35.
[118] Siehe Art. 6 Abs. 1 Satz 1 lit. c oder e i. V. m. Art. 6 Abs. 2 und 3 DSGVO.

§ 11 Abs. 1 Gesetz über den Zugang zu digitalen Geodaten im Land Berlin (Geodatenzugangsgesetz Berlin, GeoZG Bln) als Rechtsgrundlagen in Betracht kommen.[119] Hiernach sind öffentliche Stellen dem Grunde nach verpflichtet, Umweltinformationen[120] und Geodaten[121] der Öffentlichkeit zur Verfügung zu stellen. Dies kann auch eine unbeschränkte Veröffentlichung personenbezogener Daten einschließen, an die allerdings weitere Voraussetzungen geknüpft sind: So muss die veröffentlichende Stelle zum Schutz personenbezogener Daten entweder die Einwilligung der betroffenen Personen einholen oder im Einzelfall, bezogen auf die jeweiligen Grundstücke, eine Interessenabwägung zwischen dem öffentlichen Interesse am Informationszugang und dem Interesse der Grundstückseigentümer:innen an einer Nichtveröffentlichung ihrer Daten vornehmen. Auch bedarf es einer vorherigen Anhörung sämtlicher betroffener Personen.[122] Zwar gilt im allgemeinen Verwaltungsverfahrensrecht, dass Behörden auf Anhörungen verzichten können, falls sie gleichartige Regelungen in größerer Zahl erlassen möchten.[123] Der Gesetzgeber hat hier jedoch ein spezifisches Anhörungsverfahren geregelt, das den allgemeinen Bestimmungen vorgeht und keine Ausnahmen enthält. Die zu treffenden Entscheidungen dürften zudem nicht in jedem Fall gleichartig sein.

ist jedoch im Falle einer Veröffentlichung – wie vorgenannt erläutert - von Starkregengefahren- und -hinweiskarten nicht anzunehmen. In Massenverfahren ist die Anhörung überdies nach § 28 Absatz 2 Nr. 4 VwVfG entbehrlich. Die Bestimmung wird als verfassungsrechtlich unbedenklich angesehen (vgl. VGH München, BayVBl. 1988, 496 (497)) und entspringt ebenfalls dem Gedanken der Verfahrensökonomie. Die Vorschrift will insbesondere den besonderen Schwierigkeiten und Problemen begegnen, die in Verfahren mit einer Vielzahl von Beteiligten bei der Gewährung rechtlichen Gehörs auftreten können (vgl. VGH Mannheim, NVwZ 1989, S. 978, 981).

Zudem wurde die verpflichtende Drittbeteiligung des § 9 Absatz 1 Satz 3 UIG im Gesetzgebungsverfahren zum UIG erst auf Vorschlag des Bundesrates neu eingeführt; die UIRL sieht ein solches Verfahren nicht vor. Insoweit ist die Annahme nicht haltbar, die Drittbeteiligung sei für die unionsrechtlich vorgezeichnete Interessenabwägung unabdingbar. Eine Auslegung des § 9 Absatz 1 Satz 3 UIG, die mittels eines unverhältnismäßigen Drittbeteiligungsaufwands die allgemeine Informationspflicht gegenüber der Öffentlichkeit nach Art. 7 Absatz 1, Absatz 4UIRL praktisch vereiteln würde, liefe vielmehr dem unionsrechtlichen Effektivitätsgrundsatz zuwider und würde zur Unionsrechtswidrigkeit des § 9 Absatz 1 Satz 3 UIG führen (vgl. Callies/Schumacher, NVwZ 2023, S. 1361, 1367).

Darüber hinaus ist die Unterlassung einer aktiven Information über örtliche Starkregengefahren eine nicht zu rechtfertigende Einschränkung des effektiven Zugangs zu Umweltinformationen nach Art. 5 der Aarhus-Konvention, § 10 Absatz 1, Absatz 5 UIG und der positiven Schutzpflicht des Staates vor Extremereignissen nach Art. 2 Absatz 2 Satz 1 GG, da die unterlassene Veröffentlichung der Starkregengefahren- und -hinweiskarten urbane Gefahren durch Starkregenereignisse verstärkt und eine effektive Risikovorsorge verhindert (vgl. Callies/Schumacher, NVwZ 2023, S. 1361, 1367).

[119]Konkret Art. 6 Abs. 1 Satz 1 lit. c DSGVO i. V. m. § 18a Abs. 1 Informationsfreiheitsgesetz (IFG) i. V. m. § 10 Abs. 1 UIG bzw. § 11 Abs. 1 GeoZG Bln.
[120]Siehe § 2 Abs. 3 UIG.
[121]Siehe § 3 Abs. 1 GeoZG Bln.
[122]Siehe § 10 Abs. 6 UIG i. V. m. § 9 Abs. 1 Satz 1 Nr. 1, Satz 3 UIG bzw. § 12 Abs. 2 Satz 2 Nr. 1, Satz 3 GeoZG Bln.
[123]§ 28 Abs. 2 Nr. 4 Verwaltungsverfahrensgesetz (VwVfG).

Umweltbezogene Informationen, die grundstücks- und gebäudegenaue Daten beinhalten, können personenbezogene Daten der Grundstückseigentümer:innen darstellen. Beabsichtigt eine öffentliche Stelle, diese Daten zu veröffentlichen, benötigt sie eine spezifische Rechtsgrundlage. Entsprechende Rechtsgrundlagen sind im UIG und im GeoZG enthalten. Allerdings bedarf es vor Veröffentlichung der Anhörung aller betroffenen Personen.

7. Videoüberwachung öffentlichen Raums durch diplomatische Einrichtungen

Regelmäßig machen uns Bürger:innen auf Videokameras aufmerksam, die an den Außenfassaden und Grundstücksgrenzen von Botschaftsgebäuden und diplomatischen Einrichtungen angebracht und auf die Straße, also auf öffentlich zugänglichen Raum, ausgerichtet sind.

Auch Botschaften und diplomatische Einrichtungen sind nach dem Wiener Übereinkommen über diplomatische Beziehungen (WÜD) grundsätzlich an das Recht des Empfangsstaats gebunden. Da für uns allerdings keine aufsichtsrechtlichen Befugnisse bestehen, die Videoüberwachung der diplomatischen Vertretungen zu überprüfen und datenschutzrechtlich auszuwerten, können wir die Verantwortlichen nur auf dem dafür vorgesehenen diplomatischen Weg auf die Rechtslage hinweisen.

Auch Botschaften und diplomatische Einrichtungen dürfen den öffentlichen Straßenraum außerhalb des Botschaftsgrundstückes nicht einfach überwachen. Sie sind an das Recht des Empfangsstaats gebunden und müssen sich entsprechend auch an die Vorgaben der DSGVO halten.

VIII. Wirtschaft und internationaler Datenverkehr

1. Personenbezogene Daten aus dem Internet

Die Bundesrechtsanwaltskammer (BRAK) ist nach den gesetzlichen Vorschriften verpflichtet, bestimmte Daten von allen in Deutschland zugelassenen Rechtswält:innen im Internet zu veröffentlichen. Ein Dienstleistungsunternehmen hat dieser Datenbank die Stamm- und Kontaktdaten der Rechtsanwält:innen entnommen, um aus den insgesamt etwa 113.000 Datensätzen eine eigene Suchmaschine aufzubauen.

Per E-Mail wurden die betroffenen Rechtsanwält:innen, wie gesetzlich gefordert,[124] über ihre Aufnahme in

[124]Siehe Art. 14 Datenschutz-Grundverordnung (DSGVO).

die Suchmaschine informiert und der Abschluss eines kostenpflichtigen Accounts empfohlen, mit dem sie ihr Ranking bei der Ergebnisanzeige der Suchmaschine verbessern konnten.

Bereits die Erhebung der Daten durch das Unternehmen war rechtswidrig. Personenbezogene Daten dürfen nur erhoben und verarbeitet werden, wenn es hierfür eine gesetzliche Grundlage gibt. Allein die Tatsache, dass die Informationen bereits rechtmäßig im Internet veröffentlicht sind, erlaubt nicht, dass sie für beliebige Zwecke weiterverwendet werden dürfen.[125] Uns gegenüber hat das Unternehmen angegeben, ihr berechtigtes Interesse bestünde im Zweck der Direktwerbung und Kundenanwerbung. Nach den Vorschriften des Gesetzes über den unlauteren Wettbewerb (UWG) stellt die Neukundenwerbung per E-Mail ohne Einwilligung der betroffenen Personen jedoch eine unzumutbare Belästigung dar und ist deswegen unzulässig.[126] Insofern fehlte es bereits an einem berechtigten Interesse.

Zudem stehen die Interessen der Rechtsanwält:innen der Verarbeitung entgegen: Rechtsanwält:innen sind gesetzlich verpflichtet, ihre Daten der BRAK zur Veröffentlichung zu übermitteln. Damit geht nicht automatisch einher, dass sie die übermittelten Daten auch für andere als die gesetzlichen Zwecke freigeben.[127] Das Unternehmen hat die Daten bereits infolge unserer ersten Ansprache wieder gelöscht. Daher haben wir eine Verwarnung ausgesprochen; weitere Maßnahmen waren nicht erforderlich.

Auch wenn personenbezogene Daten bereits im Internet veröffentlicht sind, muss vor jeder weiteren Verarbeitung geprüft werden, ob eine Rechtsgrundlage für deren Weiterverarbeitung vorliegt. Sind personenbezogene Daten aufgrund einer gesetzlichen Verpflichtung im Internet veröffentlicht, besteht seitens der betroffenen Personen in aller Regel ein Interesse, dass diese nicht zu anderen als den gesetzlich vorgesehenen Zwecken weiterverarbeitet werden.

2. Informationspflicht über das berechtigte Interesse bei Bonitätsabfragen

Wer bei Wirtschaftsauskunfteien Bonitätsauskünfte über eine Person einholen möchte, benötigt dafür ein berechtigtes Interesse. Das berechtigte Interesse müssen abfragende Dritte den Auskunfteien, von denen sie

[125] Grundsatz der Zweckbindung nach Art. 5 lit. b DSGVO.
[126] § 7 UWG.
[127] Dies gilt im Übrigen auch für die gesetzlich vorgeschriebene Veröffentlichung der Daten im Impressum.

Informationen erhalten möchten, mitteilen. Wirtschaftsauskunfteien sind gehalten, diesbezüglich auch verifizierende Stichproben durchzuführen. Die betroffenen Personen, deren Daten abgefragt und übermittelt werden, sind von den Auskunfteien darüber zu informieren, welches berechtigte Interesse an der Übermittlung vorliegt.

Im Rahmen eines Beschwerdeverfahrens informierte uns eine betroffene Person darüber, ein Datenschutzinformationsschreiben von einer Wirtschaftsauskunftei erhalten zu haben, in dem diese ihm mitteilte, erstmals personenbezogene Daten zu seiner Person an Dritte übermittelt zu haben. Welches berechtigte Interesse der abfragende Dritte an der Übermittlung geltend gemacht hatte, teilte die Wirtschaftsauskunftei in ihrem Schreiben nicht mit. Stattdessen zählte sie die möglichen berechtigten Interessen Dritter in Form von Stichwörtern auf. Wir haben der Auskunftei mitgeteilt, dass diese Praxis nicht den Vorgaben der DSGVO entspricht, woraufhin die Auskunftei ihre Praxis angepasst hat.

Auskunfteien dürfen personenbezogene Daten an abfragende Dritte übermitteln, wenn diese ein berechtigtes Interesse an der Datenübermittlung haben, ihr berechtigtes Interesse gegenüber der Auskunftei benennen und sofern nicht die Interessen, Recht und Freiheiten der betroffenen Person, die den Schutz der Daten erfordern, überwiegen.[128] Ein berechtigtes Interesse kann dann gegeben sein, wenn ein finanzielles Ausfallrisiko bei den abfragenden Dritten besteht, etwa wenn ein Unternehmen erheblich in Vorleistung gehen muss.

Wenn personenbezogene Daten nicht bei den betroffenen Personen erhoben werden und die Verarbeitung der Daten auf Art. 6 Abs. 1 Satz 1 lit. f DSGVO beruht, müssen die Verantwortlichen die betroffenen Personen über die berechtigten Interessen informieren, die von dem Verantwortlichen oder einem Dritten verfolgt werden.[129] Die Verantwortlichen, etwa Auskunfteien, müssen diese Informationen spätestens zum Zeitpunkt der ersten Offenlegung erteilen, wenn die Offenlegung an einen anderen Empfänger beabsichtigt ist.[130] Damit müssen Auskunfteien bei Erteilung der datenschutzrechtlichen Information die betroffene Person über das konkrete von einem abfragenden Dritten angegebene berechtigte Interesse informieren, falls sie bereits personenbezogene Daten an den Dritten übermittelt haben. Die Informationspflichten aus Art. 13 und 14 DSGVO

[128] Art. 6 Abs. 1 Satz 1 lit. f DSGVO
[129] Art. 14 Abs. 2 lit. b DSGVO.
[130] Art. 14 Abs. 3 lit. c DSGVO.

sollen in Verbindung mit dem Auskunftsrecht der betroffenen Personen[131] gewährleisten, dass diese die Rechtmäßigkeit der Verarbeitung ihrer personenbezogenen Daten überprüfen und ggf. Folgemaßnahmen ergreifen können.

Wirtschaftsauskunfteien müssen Personen, deren Daten sie an Dritte übermitteln, das konkrete berechtigte Interesse der Dritten an den Daten zum Zeitpunkt der ersten Offenlegung zusammen mit anderen Informationen im Rahmen ihrer gesetzlichen Informationspflichten mitteilen.

3. Löschung der Daten vs. Nachweis von Einwilligungen

Verantwortliche tragen immer wieder vor, sie könnten den Nachweis für die Rechtmäßigkeit einer Datenverarbeitung nicht mehr erbringen, da die betroffene Person die Löschung ihrer Daten verlangt habe und sämtliche Nachweise für die Rechtmäßigkeit antragsgemäß gelöscht worden seien. In unserer Praxis betrifft dies häufig den Nachweis einer Einwilligung in die Datenverarbeitung zu Werbezwecken.

Die Verantwortlichen tragen die Beweislast dafür, dass die betroffene Person in die Datenverarbeitung zu Werbezwecken eingewilligt hat.[132] Dasselbe gilt für das Vorliegen der Voraussetzungen einer anderen Rechtsgrundlage, auf die sich Verantwortliche zur Begründung einer Verarbeitung personenbezogener Daten berufen.[133] Unabhängig von einem Löschverlangen der betroffenen Person sind Verantwortliche gesetzlich verpflichtet, die rechtmäßige Datenverarbeitung nachzuweisen, beispielsweise indem sie nachweisen, dass eine Person in die Verwendung ihrer Daten zu Werbezwecken eingewilligt hat. Die Datenverarbeitung zum Zweck des Nachweises verfolgt einen anderen Verarbeitungszweck als der Versand der E-Mail zu Werbezwecken; die Verarbeitung der personenbezogenen Daten zum Zweck des Nachweises erfolgt zur Erfüllung einer rechtlichen Verpflichtung.[134]

Eine Verpflichtung zur Löschung dieses Nachweises besteht während der Dauer der Nachweispflicht nicht – auch nicht, wenn die betroffene Person dies verlangt – , da die Datenverarbeitung notwendig ist, um eine

[131] Siehe Art. 15 DSGVO.
[132] Siehe Art. 7 Abs. 1, Art. 6 Abs. 1, Art. 5 Abs. 2 i. V. m. Abs. 1 lit. a DSGVO; Europäischer Gerichtshof (EuGH), Urteil vom 11. November 2020, C-61/19, Rn. 42.
[133] EuGH, Urteil vom 24. Februar 2022, C-175/20, Rn. 77 und 81; Urteil vom 4. Mai 2023, C-60/22, Rn. 53; Urteil vom 4. Juli 2023, C-252/21, Rn. 95; Urteil vom 14. Dezember 2023, C-340/21, Rn. 52 ff.; Bundesverwaltungsgericht (BVerwG), Urteil vom 2. März 2022, 6 C 7.20, Rn. 50; Oberlandesgericht (OLG) Hamm, Urteil vom 15. August 2023, 7 U 19/23, Ls. 1; OLG Stuttgart, Urteil vom 22. November 2023, 4 U 20/23, Rn. 401 ff.
[134] Siehe Art. 6 Abs. 1 Satz 1 lit. c i. V. m. Art. 7 Abs. 1, Art. 5 Abs. 2 DSGVO.

rechtliche Verpflichtung zu erfüllen. Insofern sind die erforderlichen Daten von der Löschpflicht ausgenommen[135] bzw. es liegt bei ordnungsgemäßer Festlegung der Zwecke der Verarbeitung auch kein Fall des Art. 17 Abs. 1 lit. a DSGVO vor.

Betroffene Personen sind schon bei der Erhebung der Daten darauf hinzuweisen, welche Daten wie lange zu Nachweiszwecken gespeichert werden,[136] um die Grundsätze des Art. 5 Abs. 1 lit. a DSGVO, insbesondere den Grundsatz der Transparenz, zu erfüllen.

Ein Löschungsersuchen verpflichtet Verantwortliche nicht dazu, etwaige Nachweise für eine erteilte Einwilligung oder für das Vorliegen einer anderen Rechtsgrundlage zu löschen. Bei der Speicherung des Nachweises handelt es sich um einen eigenständigen Verarbeitungszweck. Verantwortliche sind nach der DSGVO verpflichtet, die Rechtmäßigkeit einer Verarbeitung nachweisen zu können. Können sie den Nachweis nicht erbringen, müssen sie damit rechnen, dass ein datenschutzrechtlicher Verstoß festgestellt wird.

4. Onlinezugriff auf Konten anderer Personen durch Kontovollmachten

Mit einer Kontovollmacht dürfen nicht nur Bankgeschäfte in Vertretung der kontoführenden Person durchgeführt, sondern jederzeit auch Einsicht in das betreffende Konto genommen werden. Viele Personen erteilen ihnen nahestehenden Menschen umfassende Kontovollmachten für unvorhersehbare Notfälle, erwarten aber nicht, dass diese im regulären Alltag zur Anwendung kommen. Durch das Onlinebanking ist der Zugriff auf diese Konten wesentlich vereinfacht, da die Vollmacht der Bank nicht jedes Mal erneut vorgezeigt werden muss. Im vorliegenden Fall reichte sogar ein Klick auf der Startseite des eigenen Kontos, um auf das bei derselben Bank geführte Konto der vollmachtgebenden Person zugreifen zu können.

Eine Bank hatte das Startportal der Onlinekonten ihrer Kund:innen neu gestaltet. Daraufhin haben uns Beschwerden von zwei betroffenen Personen erreicht, die überrascht waren, dass es ihnen nach der Umgestaltung möglich war, das Konto einer jeweils anderen Person einzusehen. Es stellte sich heraus, dass für beide beschwerdeführenden Personen jeweils Kontovollmachten vorlagen, die ihnen vor etlichen Jahren erteilt worden, aber offenbar nie zur Anwendung gekommen und damit aus dem Blick geraten waren.

[135] Art. 17 Abs. 3 lit. b DSGVO.
[136] Siehe Art. 13 Abs. 1 lit. c, Abs. 2 lit. a DSGVO.

Die Erteilung einer umfassenden Kontovollmacht räumt der bevollmächtigten Person nahezu alle Befugnisse im Umgang mit dem Konto ein, wie diese auch der kontoführenden Person zur Verfügung stehen.[137] Insbesondere darf die bevollmächtigte Person sämtliche Bankgeschäfte wie Abhebungen und Transaktionen durchführen, den Kontostand sowie die Kontoauszüge aufrufen und die Kommunikation mit der Bank übernehmen. Bis zu ihrem Widerruf bleibt eine einmal ausgestellte Vollmacht unbeschränkt wirksam.[138] Dementsprechend stehen auch die beiden Beschwerdeführer:innen im vorliegenden Fall bis auf Widerruf mit den vollmachtgebenden Personen in einem Verhältnis, das ihnen unbeschränkten Zugriff auf deren Konten gewährt. Aufgrund des durch die Vollmachtserteilung bestehenden Vertrags darf und muss die Bank den Bevollmächtigten die Kontodaten der anderen Personen anzeigen.

In unseren Fällen waren die Konten der vollmachtgebenden Person nach der Umstellung für die Bevollmächtigten nun auf der Startseite ihres eigenen Kontos zu sehen. Wie die Bank mitgeteilt hat, kann die Ansicht dieser Konten ausgeblendet oder auch gänzlich ausgeschaltet werden. Ebenso lässt sich die Vollmacht jederzeit von der vollmachtgebenden Person widerrufen.

Mit einer umfassenden Kontovollmacht werden der Person, der die Vollmacht erteilt wird, weitreichende Rechte eingeräumt: Sie kann nicht nur in sämtliche Kontobewegungen Einsicht nehmen, sondern ebenso über das Guthaben auf dem Konto verfügen. Es ist grundsätzlich auch möglich, eine eingeschränkte Kontovollmacht zu erteilen, soll diese nur für einen bestimmten Bedarfsfall gelten. Für eine Vollmacht ist grundsätzlich kein Ablaufdatum vorgesehen. Einer einmal erteilten Vollmacht kann allerdings jederzeit widersprochen werden. Es empfiehlt sich, regelmäßig zu prüfen, ob die Vollmacht noch erforderlich ist.

5. Veröffentlichung der Kontaktdaten von betrieblichen Datenschutzbeauftragten

Datenschutzbeauftragte von Unternehmen und Betrieben haben eine besondere unabhängige Stellung. Dazu gehört auch, dass sich betroffene Personen vertraulich an sie wenden können. Ebenso muss die zuständige Aufsichtsbehörde mit ihnen in Kontakt treten können. Die DSGVO sieht daher die Veröffentlichung der Kontaktdaten der betrieblichen Datenschutzbeauftragten

[137] Siehe §§ 164 ff. Bürgerliches Gesetzbuch (BGB).
[138] Siehe § 171 Abs. 2 BGB.

vor, damit diese persönlich und ohne Umwege erreichbar sind.[139]

Immer wieder beschweren sich betroffene Personen bei uns darüber, dass sie mit betrieblichen Datenschutzbeauftragten vertraulich Kontakt aufnehmen wollten, stattdessen aber eine Antwort von den Verantwortlichen bzw. deren Auftragsverarbeitern erhalten haben oder keine eigenständigen Kontaktdaten zu den Datenschutzbeauftragten finden konnten. In einigen Fällen wurde bemängelt, dass die Namen, Telefonnummern oder E-Mail-Adressen der Datenschutzbeauftragten weder auf der Website der Unternehmen noch an anderer Stelle angegeben sind.

Nach Art. 37 Abs. 7 DSGVO sind Verantwortliche verpflichtet, die Kontaktdaten der von ihnen benannten Datenschutzbeauftragten zu veröffentlichen. Sie sind in den Datenschutzerklärungen bekannt zu geben[140] und der zuständigen Aufsichtsbehörde mitzuteilen.[141] In den Datenschutzerklärungen muss der Name der Datenschutzbeauftragten nicht unbedingt aufgeführt werden.[142] Was aber als Angabe grundsätzlich veröffentlicht werden muss, ist neben einer gültigen Postanschrift eine ausschließlich den Datenschutzbeauftragten zugewiesene E-Mail-Adresse und je nach Tätigkeit der Unternehmen ggf. auch eine telefonische Kontaktmöglichkeit. Letzteres gilt insbesondere dann, wenn die Kommunikation mit den Kund:innen auch sonst per Telefon erfolgt.

Die Datenschutzbeauftragten sind zur Verschwiegenheit verpflichtet, und dies insbesondere gegenüber der sie benennenden Stelle.[143] Bei allen Angaben muss daher stets sichergestellt sein, dass die Möglichkeit einer vertraulichen Kontaktaufnahme durch die betroffenen Personen gewahrt bleibt. Dazu gehört es auch, dass die Verantwortlichen konsequent darauf zu achten haben, die an die Datenschutzbeauftragten adressierte Briefpost nur diesen ungeöffnet vorzulegen. Auch etwaige bei der Zentrale oder anderen Stellen eingehende, aber für die Datenschutzbeauftragten bestimmte Telefonanrufe müssen umgehend an diese weitergeleitet werden,

[139]Die hier aufgeführten Anforderungen bestehen natürlich in gleicher Weise für behördliche Datenschutzbeauftragte.
[140]Siehe Art. 13 Abs. 1 lit. b, Art. 14 Abs. 1 lit. b DSGVO.
[141]Siehe Art. 37 Abs. 7 DSGVO.
[142]In Art. 13, Art. 14, Art. 37 DSGVO wird nur die Angabe der Kontaktdaten, nicht allerdings des Namens der Datenschutzbeauftragten gefordert. Wie sich aus den verschiedenen Entwürfen der DSGVO ergibt, ist dies eine bewusste Entscheidung des Gesetzgebers, sodass der Name nur den Aufsichtsbehörden bekannt gegeben werden muss.
[143]Siehe Art. 38 Abs. 5 DSGVO sowie § 38 Abs. 2 i. V. m. § 6 Abs. 5 Satz 2 BDSG.

ohne die Daten der anrufenden Person oder deren konkretes Anliegen zu erfragen. Die Postanschrift muss daher so gestaltet sein, dass aus ihr unmissverständlich die ausschließliche Adressierung an die betrieblichen Datenschutzbeauftragten hervorgeht. Die E-Mail-Adresse sowie etwaige weitere Kontaktmöglichkeiten per Telefon, Fax, Kontaktformular oder Messenger müssen deutlich erkennbar den Datenschutzbeauftragten zugewiesen und nur diesen oder ggf. dem ihnen unterstehenden Hilfspersonal zugänglich sein. Gemeinsame Kontaktdaten für Datenschutzbeauftragte und das Datenschutzteam des Unternehmens sind daher unzulässig.

Die Kontaktdaten der betrieblichen Datenschutzbeauftragten müssen veröffentlicht und in den Datenschutzerklärungen bekannt gegeben werden. Den Datenschutzbeauftragten sind eigenständige und unmissverständliche Kontaktdaten zuzuweisen, die sicherstellen, dass über sie nur die Datenschutzbeauftragten selbst erreicht werden und weder Verantwortliche noch unbefugte Dritte Zugriff darauf haben. Betroffenen Personen muss garantiert sein, dass ihr Kontakt zu den Datenschutzbeauftragten sowie die dabei ausgetauschten Inhalte vertraulich bleiben und jede Kenntnisnahme durch Verantwortliche oder unbefugte Dritte ausgeschlossen ist.

6. Pflicht zur Vollständigkeit der Angaben in Datenschutzerklärungen

In unserer Beratungs- und Prüfungspraxis stellen wir immer fest, dass in Datenschutzerklärungen nicht immer die in Art. 13 und 14 DSGVO geforderten Informationspflichten eingehalten werden. Die folgenden Hinweise sollen Verantwortlichen helfen, ihre Datenschutzerklärungen den rechtlichen Vorgaben getreu zu erstellen und die Vollständigkeit ihrer Angaben zu überprüfen.

Die Informationspflichten nach Art. 13 und 14 DSGVO beruhen auf dem Grundsatz der Transparenz:[144] Betroffene Personen sollen wissen, welche ihrer Daten von wem, wie, warum, auf welcher Rechtsgrundlage und wie lange verarbeitet und an wen sie weitergegeben werden. Dies soll die betroffenen Personen in die Lage versetzen, selbst überprüfen zu können, ob ihre Daten rechtmäßig verarbeitet werden.

Um die Rechtmäßigkeit der erfolgenden Datenverarbeitungen überprüfen zu können, ist die Angabe der

[144] Siehe Art. 5 Abs. 1 lit. a DSGVO.

Zwecke und Rechtsgrundlagen[145] sowie ggf. der verfolgten berechtigten Interessen[146] notwendig. Dies erfordert, dass diese vollständig – und nicht nur beispielhaft – angegeben und den konkreten Datenverarbeitungen zugeordnet werden. Eine allgemeine Darstellung, welche Rechtsgrundlagen existieren, ohne Zuordnung zu den konkreten Verarbeitungen, genügt nicht. Bei Datenverarbeitungen auf Grundlage einer rechtlichen Verpflichtung oder Wahrnehmung öffentlicher Aufgaben[147] muss zudem auch die Verpflichtungs- oder Aufgabennorm angegeben werden, denn nur diese legt letztlich die Rechtsgrundlage fest.[148] Ebenso müssen berechtigte Interessen hinreichend konkret benannt werden. Verantwortliche sollten hier besondere Sorgfalt walten lassen, weil nur die angegebenen Interessen bei der Rechtmäßigkeitsprüfung berücksichtigt werden können und sie zudem nachweisen müssen, dass die in Rede stehenden Verarbeitungen zur Wahrung der angegebenen Interessen erforderlich sind.

Zudem müssen etwaige Empfänger oder Kategorien von Empfängern der personenbezogenen Daten aufgeführt werden:[149] Ist den Verantwortlichen bekannt, an welche Empfänger oder Kategorien von Empfängern personenbezogene weitergegeben werden, müssen diese konkret benannt werden.[150] Dazu gehören sämtliche Auftragsverarbeiter und auch Unterauftragsverarbeiter. Kommt es dabei zu Datenexporten, zu denen auch Fernzugriffe aus Drittländern und die technisch gegebene Möglichkeit hierzu etwa zu Administrations- oder Supportzwecken gehören, sind diese ebenso in der Datenschutzerklärung anzugeben. Dies gilt insbesondere bei der Nutzung von Cloud- oder US-Diensten und beim Einsatz von Unterauftragsverarbeitern. Sämtliche betroffenen Drittländer müssen dementsprechend zusammen mit den von den Verantwortlichen vorgesehenen geeigneten Garantien[151] der Rechtmäßigkeit der Datenverarbeitung genannt werden. Auch die konkreten Aufbewahrungs- und Löschfristen der erhobenen Daten inklusive Fristbeginn und Fristdauer sind anzugeben.[152] Ein pauschaler Verweis auf nicht näher benannte gesetzliche Vorschriften zur Aufbewahrungspflicht ist nicht ausreichend. Es sind die Aufbewahrungs- und Löschfristen für sämtliche Datenverarbeitungen, die sich in Art und Zweck unterscheiden, differenziert zu benennen.

[145] Art. 13 Abs. 1 lit. c, Art. 14 Abs. 1 lit. c DSGVO.
[146] Sofern als Rechtsgrundlage die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO dienen soll.
[147] Siehe Art. 6 Abs. 1 UAbs. 1 lit. c oder e DSGVO.
[148] Siehe Art. 6 Abs. 3 Satz 1 DSGVO.
[149] Siehe Art. 13 Abs. 1 lit. e, Art. 14 Abs. 1 lit. e DSGVO.
[150] Zur Parallelnorm Art. 15 Abs. 1 lit. c DSGVO; EuGH, Urteil vom 12. Januar 2023, C-154/21, Leitsatz.
[151] Art. 46, Art. 47, Art. 49 Abs. 1 Satz 2 DSGVO.
[152] Art. 13 Abs. 2 lit. a, Art. 14 Abs. 2 lit. a DSGVO.

Datenschutzerklärungen sind ein wichtiges Mittel, um Transparenz über beabsichtigte oder erfolgende Datenverarbeitungen herzustellen und nachvollziehbar zu machen. Insbesondere bei der Angabe der Zwecke und Rechtsgrundlagen[153] sowie ggf. der verfolgten berechtigten Interessen[154] ist es notwendig, dass diese vollständig – und nicht nur beispielhaft – angegeben und den konkreten Datenverarbeitungen zugeordnet werden. Auch müssen die konkreten Aufbewahrungs- und Löschfristen für die jeweiligen Datenverarbeitungen benannt werden. Darüber hinaus sind die konkreten Empfänger (und nicht nur die Kategorien) aufzuführen, wenn diese bekannt sind.

7. Transparenz- und Informationspflichten bei Datenübermittlungen an Drittländer

Bei nicht weiter eingegrenzten Auskunftsersuchen nach Art. 15 DSGVO wird oft übersehen, dass Verantwortliche die Betroffenen auch über die geeigneten Garantien einer Datenübermittlung an ein Drittland unterrichten müssen, sofern dies nicht auf Grundlage eines Angemessenheitsbeschlusses erfolgt. Darüber hinaus sind Übermittlungen auch im Rahmen der sonstigen Transparenzpflichten[155] abzubilden.

Im vorliegenden Beschwerdefall rügte eine betroffene Person eine ihrer Ansicht nach unvollständige Auskunftserteilung. Sie bemängelte, dass die erforderliche Unterrichtung über die geeigneten Garantien im Zusammenhang mit der Übermittlung personenbezogener Daten an ein Drittland nicht ausreichend gewesen sei.

Nach Art. 15 Abs. 2 DSGVO hat die betroffene Person das Recht, über die geeigneten Garantien[156] im Zusammenhang mit der Übermittlung der Daten unterrichtet zu werden. Solche Garantien können aus den Standardvertragsklauseln (SCC) und ggf. den ergänzenden Maßnahmen bestehen. Auch die SCC sehen die Herausgabe einer Kopie an die betroffenen Personen vor, bei der jedoch bestimmte Geschäftsgeheimnisse durch eine Zusammenfassung ersetzt werden dürfen.[157]

Nach dem Schrems II-Urteil[158] genügt es nicht mehr, die SCC einfach nur abzuschließen, um die geforderten

[153] Art. 13 Abs. 1 lit. c, Art. 14 Abs. 1 lit. c DSGVO.
[154] Sofern als Rechtsgrundlage die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO dienen soll.
[155] Siehe Art. 13, Art. 14 DSGVO.
[156] Art. 46 DSGVO.
[157] Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 4. Juni 2021, Klauseln 8.2.c bzw. 8.3.
[158] EuGH, Urteil vom 16. Juli 2020, C-311/18.

geeigneten Garantien[159] herzustellen. Vielmehr umfassen die geeigneten Garantien alles, was notwendig ist, um das nach Art. 46 DSGVO erforderliche Schutzniveau tatsächlich herzustellen. Dies betrifft neben dem vom EuGH angemahnten sog. Transfer Impact Assessment (TIA)[160] auch etwaige „zusätzliche Maßnahmen“[161] sowie die Angaben darüber, in welcher Form, mit welchen Modulen und mit welchen Eintragungen im Text und in den Anlagen die SCC konkret ausgefüllt sind. Erst in ihrer Gesamtheit bilden diese Informationen und Maßnahmen geeignete Garantien nach Art. 46 DSGVO.

In der Gesamtschau sind daher jedenfalls die folgenden Angaben nach Art. 15 Abs. 2 DSGVO an die betroffene Person zu beauskunften:

- Angabe, welche Garantien nach Art. 46 Abs. 2 DSGVO im Zusammenhang mit der Übermittlung der personenbezogenen Daten der betroffenen Person zum -Einsatz kommen;
- Nennung der im konkreten Fall abgeschlossenen Module;
- Nennung der ausgewählten Optionen, Wahlmöglichkeiten oder Eintragungen innerhalb der SCC;
- Zusammenfassung der technisch-organisatorischen Maßnahmen nach Anhang II der SCC;
- Zusammenfassung bzw. Ergebnis des TIA;
- Zusammenfassung der ergriffenen zusätzlichen Maßnahmen.

Daneben müssen Verantwortliche Übermittlungen personenbezogener Daten an Drittländer außerhalb des Europäischen Wirtschaftsraums (EWR) nach Art. 44 DSGVO auch in den Datenschutzinformationen nach Art. 13 und 14 DSGVO – beispielsweise in Form der Datenschutzerklärung – abbilden. In jedem Fall ist darauf zu achten, dass die konkreten[162] Empfänger:innen[163] und ggf. die Absicht[164], personenbezogene Daten an ein Drittland zu übermitteln, angegeben werden.

Wir haben daraufhin die Verantwortlichen darauf aufmerksam gemacht, welche Informationen den Betroffenen im Fall eines nicht weiter eingegrenzten Auskunftsersuchens zusätzlich mitgeteilt werden müssen.

[159] Siehe Art. 46 DSGVO.
[160] EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 142.
[161] Ebd., Rn. 133.
[162] Siehe hierzu EuGH, Urteil vom 12. Januar 2023, C154/21, Rn. 39.
[163] Art. 13 Abs. 1 lit. e, Art. 14 Abs. 1 lit. e bzw. Art. 15 Abs. 1 lit. c DSGVO.
[164] Art. 13 Abs. 1 lit. f bzw. Art. 14 Abs. 1 lit. f DSGVO.

Sofern personenbezogene Daten an Drittländer außerhalb des EWR übermittelt werden, müssen Verantwortliche dies im Rahmen ihrer sonstigen Pflichten und bei der Gewährung von Betroffenenrechten abbilden. Bei der Beantwortung von nicht weiter eingeschränkten Auskunftsersuchen nach Art. 15 DSGVO muss daher insbesondere darauf geachtet werden, dass Betroffene über die geeigneten Garantien nach Art. 15 Abs. 2 DSGVO unterrichtet werden. Darüber hinaus sind Übermittlungen an Drittländer und die entsprechenden Empfänger:innen der personenbezogenen Daten auch im Rahmen der sonstigen Transparenzpflichten nach Art. 13 und 14 DSGVO anzugeben.

IX. Technischer Datenschutz

1. Datenschutzfreundliche Technikgestaltung bei webbasierten Gesundheitsanwendungen

Webanwendungen, mit denen Patient:innen mit medizinischen Einrichtungen und niedergelassenen Ärzt:innen kommunizieren, Termine vereinbaren und behandlungsrelevante Daten austauschen, treten mit dem Versprechen an, die Kommunikation und Organisation für Ärzt:innen und medizinische Fachkräfte komfortabel und medienbruchfrei zu gestalten. Da es sich bei Gesundheitsdaten um besonders schützenswerte Daten handelt, müssen diese Software-as-a-Service- oder kurz: SaaS-Lösungen erhöhte Anforderungen an die technische Gestaltung der Systeme sowie die technischen und organisatorischen Maßnahmen zu deren Absicherung erfüllen.

Wir erhielten im Jahr 2022 Hinweise von unabhängigen Sicherheitsforscher:innen, die uns über Schwachstellen in webbasierten Anwendungen im Gesundheitsbereich unterrichteten. Die Schwachstellen betrafen insbesondere fehlende Sicherheitsmaßnahmen wie Berechtigungsprüfungen, technische Mängel wie vergessener Testcode in Produktivsystemen und unzureichend umgesetzte Kontrollmechanismen. Diese ermöglichten es unberechtigten Dritten potenziell, auf die Daten von mehreren zehntausend Patient:innen zuzugreifen und die medizinischen Unterlagen von mehr als einer Million Betroffener über die an die Systeme angebundenen Arztpraxen und medizinischen Einrichtungen abzurufen. Bei der Entwicklung der Webanwendungen wurden – anders als in Art. 32 Abs. 1 Datenschutz-Grundverordnung (DSGVO) gefordert – keine ausreichenden technischen und organisatorischen Maßnahmen[165] umgesetzt. Dies stellt einen Verstoß gegen das Datenschutzrecht dar, das die Gewährleistung eines dem Risiko angemessenen Schutzniveaus bei der

[165] Siehe ergänzend auch Erwägungsgrund (ErwGr.) 78 DSGVO.

Verarbeitung personenbezogener Daten vorschreibt. Die Einleitung eines Sanktionsverfahrens war daher angezeigt.

Auch wenn die Webanwendungen im Rahmen von Auftragsverarbeitungen von den Ärzt:innen und medizinischen Einrichtungen eingebunden werden, haften die Betreiber der Anwendungen für die Sicherheit der Verarbeitung nach Art. 32 DSGVO. Sie -müssen nicht nur selbst geeignete Garantien dafür vorweisen, dass geeignete technisch-organisatorischen Maßnahmen zur Absicherung der Verarbeitung im Einklang mit der DSGVO umgesetzt werden, sondern dies ebenso von ihren Auftragsverarbeitern einfordern. Zur Verhinderung von Schwachstellen und zur Minimierung späterer Sicherheits-risiken sind grundsätzlich schon in der Planungsphase Maßnahmen, wie die Entwicklung anhand von Coding Guidelines, die Umsetzung des Vier-Augen--Prinzips durch Code Reviews, die konsequente Durchführung von Unit- und Integrationstests sowie mehrstufige Freigabeprozesse zur Qualitätssicherung, zu berücksichtigen. -Weitere Hinweise zur sicheren und datenschutzfreundlichen Technikgestaltung finden sich in den Veröffentlichungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).[166]

Die Orientierung an Empfehlungen und Leitfäden kann helfen, Webanwendungen nach den rechtlichen Vorgaben und bereits in der Konzeptionsphase sicher zu gestalten. Gerade in modernen IT-Systemen, in denen die Funktionalität durch verschiedene Teams hergestellt und aufrechterhalten wird, sind Sicherheitsmechanismen und Kontrollstrukturen zu etablieren, die der Charakteristik dieser Systeme Rechnung tragen. Dies kann beispielsweise durch die strikte Trennung von Ent-wicklungs-, Test- und Produktivumgebungen sowie obligatorische Berechtigungsprüfungen bei jedem Zugriff auf ein Objekt oder eine Ressource erreicht werden. Ebenso sind bei Webanwendungen sämtliche Ein- und Ausgaben zwingend zu validieren und zu filtern.

[166]BSI, Entwicklung sicherer Webanwendungen v2.0 vom 11. Juli 2018, abrufbar unter https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_022.html; Standards zur Internet-Sicherheit. Sicheres Bereitstellen von Web-Angeboten vom 23. Oktober 2017, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_web_server_studie.pdf?__blob=publicationFile&v=1; Leitfaden zur Entwicklung sicherer Webanwendungen, Empfehlungen und Anforderungen an die Auftragnehmer vom 3. September 2013, abrufbar unter https://www.bsi.bund.de/SharedDocs/ Downloads/DE/BSI/Publikationen/Studien/Webanwendungen/Webanw_Auftragnehmer.html; Sicherheit von Webanwendungen, Maßnahmenkatalog und Best Practices vom 1. August 2006, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/WebSec/WebSec.pdf.

2. Anforderungen an Authentifizierungsverfahren zur Identitätsfeststellung

Die Identifizierung und Authentifizierung von Nutzer:innen gehören zu den Grundbausteinen eines modernen Informationssystems, das individualisierte Dienste anbietet. Für diese Datenverarbeitungen gilt im Hinblick auf die Sicherheit der Verarbeitung nach Art. 32 DSGVO: Je höher der Schutzbedarf, desto höher muss das Schutzniveau der getroffenen Maßnahmen sein. An einem uns vorliegenden Fall wird deutlich, worin die Anforderungen an die Identifizierung und Authentifizierung bei erhöhtem Schutzbedarf bestehen.

Wir haben ein Unternehmen geprüft, das zwischen verschiedenen Vertragsparteien als Informationsvermittler tätig ist. Aufgrund des hohen Schutzbedarfs der ausgetauschten Informationen hat das Unternehmen die Nutzung des Informationsdienstes an die Bedingung geknüpft, dass die Nutzer:innen zuvor sicher identifiziert werden müssen. Das Unternehmen bietet im Rahmen der Registrierung zwei Optionen zur Identitätsfeststellung an – via Ausweisfoto oder Onlinebanking. Diese beiden Identifizierungsmethoden werden dem hohen Schutzbedarf der Daten jedoch nicht ohne Weiteres gerecht.

Tatsächlich gelang es einer Sicherheitsforscherin, eine Sicherheitslücke aufzudecken, die kurzzeitig das unbefugte Abrufen und Verändern von Daten erlaubt hätte. Unsere Prüfung hinsichtlich der Sicherheit der Verarbeitung nach Art. 32 DSGVO ergab, dass kein angemessenes Schutzniveau zum Zeitpunkt der Prüfung gewährleistet war. Nach Art. 32 DSGVO müssen Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein angemessenes Schutzniveau zu gewährleisten.

Die erste Option, die das Unternehmen im Rahmen der Registrierung anbot, beinhaltete die Identifizierung mittels eines Dienstleisters anhand eines Abgleichs des Personalausweisfotos mit einem Gesichtsfoto. Dieses Verfahren kann bereits mit relativ überschaubaren Mitteln überlistet werden und bietet daher kein angemessenes Sicherheitsniveau. Wir haben folglich auf die Funktion des elektronischen Personalausweises, sich per Chip und über ein Berechtigungszertifikat auch online ausweisen zu können, als alternatives Identifizierungsmittel hingewiesen.

Die zweite Option zur Identifizierung erfolgt über den Abgleich mit den Bankkontodaten. Hierbei werden die Nutzer:innen aufgefordert, ihre Namen und Angaben zu ihrer kontoführenden Bank anzugeben, um sich anschließend über eine Weiterleitung beim Onlinebankingdienst anzumelden. Bei erfolgter Anmeldung erhält das Unternehmen einen lesenden Zugriff auf die Stammdaten, um die Namen der Nutzer:innen mit denen der Kontoinhaber:innen zu vergleichen und auf diese Weise die Identität zu bestätigen. Allerdings ist ein Abgleich allein der Namen aufgrund von möglichen Namensgleichheiten für daran anschließende personenbezogene Verarbeitungen in der Regel nicht ausreichend. Hier müssen weitere Informationen über die Nutzer:innen, wie etwa Geburtsdatum, Adresse und Kontonummer, abgeglichen werden, um die Richtigkeit der Verarbeitung zu gewährleisten. Ein weiteres Problem der Identifizierung über Onlinebanking ist die unzureichende Datensparsamkeit: Das Unternehmen erhält zusätzlich Zugriff auf Kontoumsatzdaten eines langen Zeitraums.

Unabhängig von der gewählten Authentifizierungsmethode sind automatisierte Tests als Teil einer guten Softwareentwicklungspraxis bei kritischen Funktionen wie der Zugriffskontrolle unerlässlich. Die nachträgliche Veränderung von Daten, die als nicht veränderbar gelten, ist ein typisches Problem im Kontext von Identifizierungs- und Authentifizierungsdiensten und muss durch geeignete Schutzmaßnahmen nachweisbar verhindert werden. Wir haben festgestellt, dass bei der Gestaltung des Identifizierungsvorgangs mittels eines Bankkontos grundlegende Anforderungen an ein sicheres Systemdesign nicht erfüllt waren. Zudem halten wir in Anbetracht des erhöhten Schutzbedarfs eine Absicherung der Konten allein über Name und Passwort der Nutzer:innen für nicht ausreichend. Hier müsste zumindest eine Zwei-Faktor-Authentifizierung (2FA) über die Kombination eines Passworts mit einer TAN oder eines Ausweisdokuments mit der zugehörigen PIN erfolgen.[167]

Verantwortliche müssen bei Datenverarbeitungen, die mit erhöhten Risiken für die Rechte und Freiheiten betroffener Personen verbunden sind, geeignete technische und organisatorische Maßnahmen treffen, die ein entsprechend hohes Schutzniveau gewährleisten. Hierzu gehört die Auswahl starker, aber datensparsamer Identifizierungsmittel, wie etwa der Einsatz eines Ausweisdokuments mit der zugehörigen PIN. Eine

[167] Siehe auch A.IX.4.

Identifizierung über ein Bankkonto ist so zu gestalten, dass nicht mehr als die erforderlichen Daten für den Zweck der eindeutigen Identifizierung erhoben werden. Das schließt in der Regel einen unbeschränkten Zugriff auf das Bankkonto über das Onlinebanking aus.

3. Zugriffsschutz durch Passwörter

Per E-Mail mit Unternehmen zu kommunizieren, ist Standard. Die Korrespondenz häuft sich in den Postfächern der Unternehmen an und muss adäquat geschützt werden. Ein Zugriffsschutz allein über Benutzername und Passwort ist dafür grundsätzlich nicht mehr ausreichend.

Ein Unternehmen meldete uns eine Datenpanne im Zusammenhang mit einem E-Mail-Postfach, das der Kommunikation mit dessen Kund:innen diente. Im Zuge unserer Prüfung stellte sich heraus, dass das für das Postfach verwendete Passwort aufgrund seiner unzureichenden Komplexität erraten werden konnte. Als direkte Maßnahme nach der Datenpanne hatte das Unternehmen seine Passwortrichtlinien überarbeitet und die Möglichkeit zum Fernzugriff auf das betroffene Postfach sowie ähnlich verwendete Postfächer deaktiviert. Mit unserer Prüfung wollten wir sicherstellen, dass die nun getroffenen Sicherheitsvorkehrungen ausreichend sind und längerfristig ein angemessenes Schutzniveau eingehalten werden kann.

Wer personenbezogene Daten verarbeitet, muss nach Art. 32 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen treffen, die ein dem Risiko angemessenes Schutzniveau gewährleisten. Hierbei sind immer der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und der Zweck der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten etwaig betroffener Personen zu berücksichtigen. Verantwortliche müssen dementsprechend abwägen, auf welche Teile ihrer Datenverarbeitung Zugriff aus dem Internet und auf welche Teile nur Zugriff aus dem internen Netzwerk gewährt werden soll. Betreiben Verantwortliche – wie im vorliegenden Fall – selbst einen E-Mail-Server, empfiehlt sich die Prüfung, ob nicht der E-Mail-Abruf über das interne Netzwerk ausreicht. Wird ein externer E-Mail-Dienstleister genutzt, ist sicherzustellen, dass der Zugriff auf die Postfächer ausschließlich über eine sichere Authentisierung[168] erfolgt. Die bloße Verwendung von Benutzername und Passwort entspricht dabei nicht mehr dem

[168]Im allgemeinen Sprachgebrauch werden die Begriffe „Authentisierung“ und „Authentifi-zierung“ oft synonym verwendet, sie beschreiben jedoch unterschiedliche Teilprozesse des Anmeldevorgangs: Eine Person authentisiert sich an einem System mittels eindeutiger Anmeldedaten. Das System überprüft daraufhin deren Gültigkeit und authentifiziert die betroffene Person; siehe JB 2022, 10.5, S. 93.

Stand der Technik und ist deshalb durch mindestens einen zweiten Faktor zu ergänzen.[169] Noch besser wäre es, ganz auf die Verwendung von nutzergenerierten Passwörtern zu verzichten und stattdessen sog. Passkeys[170] einzusetzen, die als in den Endgeräten der Nutzer:innen gespeicherte kryptografische Schlüssel die vollständig passwortlose Anmeldung erlauben.

Zugriffskontrolle ist ein wichtiger Bestandteil des technischen Datenschutzes. Der Zugriff auf IT-Systeme ist immer auf das notwendige Minimum zu beschränken. Je weniger Zugänge vergeben werden, desto besser ist der Schutz der Systeme und der darauf befindlichen Daten gewährleistet. Sind bestimmte Bereiche, wie etwa E-Mail-Postfächer, über das Internet zugänglich, ist die Zugriffskontrolle durch eine sichere Authentisierung der berechtigten Personen unabdingbar. Mindestanfor-derung ist hier die Verwendung zweier oder mehrerer Faktoren; wenn durchführbar, empfiehlt sich der Wechsel auf passwortlose Methoden.

4. Schutz vor Phishing und Ransomware

Innerhalb der letzten zwei Jahre hat sich die Zahl der uns als Datenpannen[171] gemeldeten Angriffe durch Datendiebstahl und Schadsoftware nahezu verdoppelt. Für Verantwortliche wie betroffene Personen ist es daher wesentlich, die Maßnahmen zu kennen, die ergriffen werden können und auch ergriffen werden sollten, um die Angriffsmöglichkeiten einzuschränken und die Auswirkungen dennoch erfolgter Angriffe zu begrenzen.

Das BSI übertitelt die Web-Ankündigung seines aktuellen Reports zur IT-Sicherheitslage in Deutschland mit dem Hinweis: „Ransomware ist und bleibt die größte Bedrohung“.[172] Auch die Presse berichtet zunehmend häufiger über Unternehmen und Behörden, deren Daten – darunter oft auch die personenbezogenen Daten ihrer Kund:innen – unrechtmäßig abgegriffen wurden. Ermöglicht werden diese Angriffe regelmäßig über den Einsatz von Phishing-E-Mails oder unter Verwendung von Ransomware. Während -Phishing-E-Mails betroffene Personen dazu verleiten sollen, Schadsoftware herunterzuladen oder vertrauliche Informationen wie Anmeldedaten oder Kontonummern preiszugeben, sind Ransomware Schadprogramme, die

[169]Siehe BSI, Zwei-Faktor-Authentisierung, abrufbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html.
[170]Siehe auch A.IX.2.
[171]Siehe Art. 33 DSGVO.
[172]BSI, Die Lage der IT-Sicherheit in Deutschland 2023 vom 2. November 2023, abrufbar unter https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

entweder durch Sicherheitslücken oder anhand erworbener Daten zugriffsberechtigter Nutzer:innen in fremde Systeme gelangen und hierdurch weitgehende Zugriffsrechte gewähren bzw. erhalten.

Bis vor einigen Jahren war das primäre und oft einzige Ziel der Ransomware, die Daten angegriffener Organisationen oder Einrichtungen zu verschlüsseln und für die Entschlüsselung Lösegeld (engl. ransom) zu fordern. Mittlerweise sind die Angreifenden allerdings dazu übergegangen, die Daten zusätzlich auf eigene Server zu übertragen. Der Zweck: Wenn die Verantwortlichen nicht willens sind, für die Entschlüsselung der Daten zu bezahlen – beispielsweise weil diese bereits eine funktionierende -Back-up-Strategie umgesetzt haben und ein Großteil der Daten auch ohne Zahlung des Lösegelds wiederherstellbar ist –, so werden diese nun auch damit erpresst, dass die Daten im Falle einer Nichtzahlung veröffentlicht werden. Dies wäre für die betroffenen Unternehmen und Einrichtungen mindestens rufschädigend und könnte zusätzlich – je nachdem, welche Daten auf diese Weise zugänglich werden würden – erhebliche Schadensersatzforderungen oder auch Sanktionen einschließlich der Verhängung von Bußgeldern nach sich ziehen.

Auch bei Phishing-E-Mails ist eine Professionalisierung des Vorgehens zu beobachten: Wurden vor Jahren noch fehlerhaft formulierte Standard-E-Mails mit Schadsoftware im Anhang verschickt, werden nun Inhalte bereits bestehender E-Mails aus gehackten Postfächern übernommen, um realistische Phishing-E-Mails etwa als Antwort auf vorher versendete E-Mails zu simulieren.

Zumeist erfolgt der Versand der Phishing-E-Mails automatisiert. Wenn allerdings bestimmte Unternehmen oder Behörden gezielt angegriffen werden, werden durchaus auch manuell erstellte und dem Einzelfall angepasste Phishing-E-Mails eingesetzt, die ggf. zusätzlich durch Anrufe, Kurznachrichten oder andere Mitteilungen unterstützt werden. Im Zuge der aktuellen KI-Entwicklung ist zu erwarten, dass diese individualisierten Angriffe künftig häufig halb- oder gar vollautomatisch durchgeführt werden und trotz Erhöhung der Sicherheitsmaßnahmen ein Anstieg der Betroffenenzahlen zu verzeichnen ist.

In diesem Jahr erreichten uns beispielsweise vermehrt Eingaben zu Phishing-Vorfällen im Zusammenhang mit einer Hotel- und Ferienunterkünfte-Onlineplattform. Die Beschwerdeführer:innen teilten mit, dass sie verdächtige Nachrichten von der Buchungsplattform erhalten hätten, die dem Anschein nach von der von

ihnen gebuchten Ferienunterkunft stammen. Sie würden dazu aufgefordert, Reservierungen über einen mitgesendeten Link zu bestätigen oder Kreditkartendetails über den Link einzugeben. Die Nachrichten machten einen täuschend echten Eindruck, da sie Details, wie etwa konkrete Buchungszeiträume, enthielten. Einige der Beschwerdeführer:innen hatten die gebuchten Hotels und Ferienunterkünfte nach Erhalt der Nachricht direkt kontaktiert, die ihnen daraufhin bestätigten, dass die Nachricht nicht von ihnen stamme. Es handelte sich offenbar um Betrugsfälle mittels sog. Spear-Phishing[173], bei denen kriminelle Dritte an die Buchungsdaten der Beschwerdeführer:innen gelangt sind und versuchten, mit einer vertrauenserweckenden E-Mail die Preisgabe von vertraulichen Zugangsinformationen zu erwirken.

Eine technische Maßnahme zur Verringerung des Angriffsrisikos durch Phishing oder Ransomware ist die Einführung einer 2FA oder Mehrfaktor-Authentifizierung (MFA).[174] Diese ergänzt die zur Anmeldung notwendige Eingabe eines Benutzernamens und eines Passworts um mindestens einen zusätzlichen Faktor, beispielsweise eine Transaktionsnummer (TAN). Trotz Warnungen wird nach wie vor oft dieselbe Kombination aus Kennung und Passwort für verschiedene Onlinedienste verwendet. Die Erfolgsquote ist daher vergleichsweise hoch, wenn einmal abgegriffene oder bekannt gewordene Zugangsdaten bei populären Onlinediensten ausprobiert werden. Die Kombination mit einer zeitlich befristeten TAN kann das Risiko verringern, da sie nur über einen kurzen Zeitraum gültig ist und unverzüglich eingegeben werden muss. Der zweite Faktor kann aber auch in einer passwortlosen Anmeldung mittels sog. Passkey bestehen, der von gängigen Webbrowsern, mobilen Betriebssystemen und immer mehr Onlinediensten unterstützt wird. Ein Passkey ist ein im Endgerät der Nutzer:innen gespeicherter kryptografischer Schlüssel, mit dem sich das Endgerät gegenüber der authentifizierenden Stelle ausweisen kann. Der Zugriff auf den Schlüssel wird zusätzlich durch die Abfrage eines Masterpassworts oder durch biometrische Bestätigung per Fingerabdruck oder Gesicht geschützt. Entscheidend für die Wirksamkeit der eingesetzten Faktoren ist, dass diese verschiedenen Kategorien entstammen und eine Kombination aus Wissensdaten (Passwort), automatisiert generierten Daten (TAN) und biometrischem Daten (Fingerabdruck) darstellen.

[173]Spear-Phishing ist eine verfeinerte Variante des Phishings und richtet sich gezielt gegen bestimmte Organisationen oder Individuen. Spear-Phishing-E-Mails werden oft mit hohem Aufwand und viel Akribie auf konkrete Empfänger:innen zugeschnitten, um eine vertrauenswürdige Quelle nachzuahmen. Neuere Technologien wie etwa FraudGPT erleichtern die Erstellung solcher E-Mails.

[174]Letztere wird auch Multifaktor-Authentifizierung genannt.

Zusätzliche technische Maßnahmen zur Sicherung der eigenen Infrastruktur und der IT-Systeme führt das BSI an:[175] Updates und Patches müssen zeitnah eingespielt werden, um Sicherheitslücken umgehend zu schließen. Zudem sollten die Ausführung von Makros in E-Mails und die Darstellung von HTML-E-Mails unterbunden werden. Zusätzlich sind Netzwerke zu segmentieren und sämtliche Zugriffsrechte auf das Minimum zu beschränken, um Angriffserfolge räumlich und logisch zu begrenzen. Bei Überlegungen, Monitoringmaßnahmen mit Anomalieerkennung zumindest für sicherheitsrelevante Zugänge einzuführen, sollte berücksichtigt werden, dass die Speicherung beträchtlicher Datenmengen über längere Zeiträume mit den Datenschutzanforderungen häufig nicht zu vereinbaren ist. Außerdem handelt es sich hierbei um Maßnahmen, die Angriffe nur mit einer gewissen Wahrscheinlichkeit erkennen und den Erfolg schneller Reaktion begrenzen können. Unsichere Authentifizierungssysteme und Sicherheitslücken in der Software sind durch diese Maßnahmen nur unzureichend zu beheben. Daher muss vorab abgewogen werden, in welchem Umfang, über welche Zeiträume und durch welche Systeme Daten erhoben werden. Ziel muss es sein, einen hohen Grad an IT-Sicherheit bei gleichzeitiger geringer Verarbeitung personenbezogener Daten zu gewährleisten.

Neben diesen technischen Maßnahmen tragen auch regelmäßige Schulungen der Mitarbeitenden zur IT-Sicherheit bei. Zu Trainingszwecken kann auch der gelegentliche Versand von Pseudo-Phishing-E-Mails dienlich sein, deren Link auf eine Hinweisseite zum Schutz vor Datendiebstahl und Systemangriffen führt. Die Mitarbeitenden sind vorab über die Maßnahme zu informieren.

Kommt es durch Datendiebstahl oder Angriffe auf das IT-System zu einer Datenpanne, bei der personenbezogene Daten betroffen sind, ist dies nach Art. 33 DSGVO der zuständigen Aufsichtsbehörde zu melden.[176] Es können im Vorfeld allerdings Maßnahmen ergriffen werden, um Angriffe durch Phishing und Ransomware zu erschweren und dessen Auswirkungen zu begrenzen. Sichere Authentifizierungsverfahren leisten hier einen Hauptanteil, ebenso kann die Auftei-

[175]BSI, Top 10 Ransomware-Maßnahmen, abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/Top-10-Ransomware-Massnahmen/top-10-ransomware-massnahmen_node.html.

[176]Zusätzlich sind weitere Maßnahmen durchzuführen, siehe BSI, Ich habe einen Vorfall – Was soll ich tun?, abrufbar unter https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Kritische-Infrastrukturen-und-meldepflichtige-Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Was-soll-ich-tun/ich-habe-einen-it-sicherheitsvorfall-was-soll-ich-tun_node.html.

lung des IT-Systems in kleinere Einheiten das Schadenspotenzial eines Angriffs verringern. Zudem ließe sich die Qualität der Software durch stärkere vertragliche Haftungsbedingungen der Hersteller:innen verbessern, um Sicherheitslücken möglichst von vorherein zu vermeiden.

5. Internationale Arbeitsgruppe für Datenschutz in der Technologie

Die International Working Group on Data Protection in Technology (IWGDPT), auch Berlin Group genannt, trat in diesem Jahr zweimal unter dem Vorsitz des Bundes-beauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und unserer Beteiligung zusammen. In der internationalen Arbeitsgruppe beraten Datenschutzaufsichtsbehörden und -expert:innen aus vielen Ländern darüber, wie der Datenschutz bei der Anwendung moderner Technologien gewährleistet werden kann.

Die erste Sitzung der IWGDPT fand vom 7. bis 8. Juni dieses Jahres in Rom statt. Dabei wurden Arbeitspapiere, sog. Working Papers, zu Smart Cities und zur Verarbeitung von Telemetrie- und diagnostischen Daten verabschiedet.

Das Arbeitspapier zu Smart Cities analysiert die Datenverarbeitungsvorgänge, die Grundlage der intelligenten städtischen Dienste bilden.[177] Diese fangen bei der Datenerhebung durch Sensornetzwerke, durch Videoüberwachung, aus der Bereitstellung öffentlicher Kommunikationsdienste und der Nutzung von städtischen Diensten an.

Sie setzen sich mit der Analyse der erhobenen Daten fort, die die Zusammenführung mit anderen Datenbeständen, das Training und die Anwendung von künstlicher Intelligenz, die Profilbildung zur Vorhersage zukünftiger Ereignisse und die Simulation von städtischen Prozessen umfassen kann. Schließlich werden durch die anwendende Stadt auf der Basis der Analyseergebnisse Entscheidungen über die Erbringung von Diensten, die Kontrolle des Verkehrs und städtischer Ereignisse und politische Maßnahmen getroffen.

Ausgehend von dieser Beschreibung analysiert das Papier die Risiken, die für die Bewohner:innen der Stadt aus dieser Datenverarbeitung erwachsen können, und gibt Empfehlungen zu ihrer Minderung. Es geht darauf ein, dass die städtische Verwaltung und die eingesetz-

[177] IWGDPT, Working Paper on „Smart Cities“ vom 8. Juni 2023, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Smart-Cities.html.

ten Dienstleister:innen Rechenschaft über ihre Tätigkeit abzulegen haben, wozu gehört, dass sie die Zwecke der Verarbeitung im Voraus festlegen und die verarbeiteten Daten davon ausgehend auf das erforderliche Maß reduzieren. Eine Verwendung der Daten in einer Weise, die nicht vereinbar mit dem Erhebungszweck ist, sollte die Stadt unterlassen und bei ihren Auftragsverarbeitern unterbinden, die -Inte-grität und Vertraulichkeit der personenbezogenen Daten garantieren und Transparenz über die Verarbeitung schaffen, kurz: die Datenschutzgrundsätze durch Technikgestaltung implementieren. Für jede der dabei zu lösenden Aufgaben gibt das Papier ein praktisches Beispiel aus einer Stadt, die Smart-City-Technologien bereits jetzt einsetzt.

Das Arbeitspapier zur Verarbeitung von Telemetrie- und diagnostischen Daten[178] beschreibt die Praktiken und damit verbundenen Risiken bei der Erhebung und Verarbeitung von Daten über den Einsatz von Produkten der Informationstechnik (Telemetriedaten) und von Daten über Fehlerzustände der Produkte (diagnostische Daten) durch Hersteller:innen dieser technischen Komponenten. Relevante Produkte sind Betriebssysteme für IT-Systeme im Allgemeinen und insbesondere für Geräte, die wie Smartphones unmittelbar durch die Nutzenden bedient werden; des Weiteren mobile Anwendungen und Anwendungen, die von Clouddienstleister:innen bereitgestellt werden. Telemetrie- und diagnostische Daten sind vielfach personenbezogen und enthalten Angaben über die Nutzung der IT-Systeme durch die Nutzenden, möglicherweise aber auch Daten, die mit den überwachten Geräten verarbeitet wurden, und weitere Angaben über den Kontext der Verarbeitung.

Die Risiken werden dadurch verstärkt, dass die Hersteller:innen nicht selten weit mehr Daten erheben, als für die von ihnen verfolgten Zwecke erforderlich ist. Sie erstrecken sich auf

- fehlende Transparenz der Verarbeitung,
- unzureichende Datenminimierung,
- fehlende Zweckbindung bei der Verarbeitung,
- Zusammenführung mit anderen personenbezogenen Daten (womöglich gar zum Zweck ihrer Monetarisierung),
- fehlende oder unzureichende Einwirkungsmöglichkeiten für die Nutzenden,
- unzureichende Gewährung von Betroffenenrechten und schließlich

[178]IWGDPT, Working Paper on Telemetry and Diagnostic Data vom 8. Juni 2023, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Telemetry-Diagnostic-Data.html.

- mangelhaften Schutz der Vertraulichkeit der Daten, die durchaus zu den besonderen Kategorien personenbezogener Daten zählen und folglich besonders schützens-wert sein können, etwa wenn sie Schlussfolgerungen über die Aufenthaltsorte oder den Gesundheitszustand von Nutzenden zulassen.

Die zweite Sitzung der IWGDPT fand vom 7. bis 8. Dezember in Ottawa statt. Es wurden Arbeitspapiere zur Datenweitergabe, zur Neurotechnologie sowie zur generativen künstlichen Intelligenz und großen Sprachmodellen diskutiert. Das Arbeitspapier zum digitalen Zentralbankgeld[179] greift die Überlegungen und Pläne zu einem staatlich bereitgestellten digitalen Äquivalent zum Bargeld auf und erörtert die Datenschutzherausforderungen bei verschiedenen Umsetzungsalternativen und Einsatzszenarien. Gerichtet an den Gesetzgeber und an Entscheider:innen im Finanzsektor wird im Arbeitspapier angemerkt, dass bei einer Einführung eines Digitalen Euro die Vorteile die Datenschutz- und Grundrechtsrisiken bei einer Folgenabschätzung überwiegen müssen. Insbesondere sollten im Zuge einer gründlichen Planung datenschutzfördernde Techniken (Privacy Enhancing Technologies) eingesetzt werden, um bei Transaktionen über die Zentralbanken die Anforderungen an Geldwäsche- und Terrorismusfinanzierungsbekämpfung datensparsam umzusetzen. Ohne die Zentralbank als Intermediär kann bei direkten Peer-to-Peer-Transaktionen das Auflaufen von großen Mengen an Transaktionsdaten an zentraler Stelle vermieden werden. Neben der Europäischen Zentralbank (EZB) erwägen z. B. auch Uruguay mit der Einführung eines E-Peso und Schweden mit der E-Krone eine Möglichkeit für Peer-to-Peer-Zahlungen.

Die international breit abgestimmten Papiere der IWGDPT geben den Anwender:innen und Hersteller:innen von Technologien zur Verarbeitung personenbezogener Daten wertvolle Hinweise zur Ausgestaltung und zum Betrieb informationstechnischer Produkte. Darüber hinaus enthalten sie auf fachlich belastbarer Grundlage Empfehlungen für die Gesetzgeber zur Regelung der mit den Technologien verbundenen Datenverarbeitung.

6. Datensichere Umsetzung digitaler Archivierungsprozesse

Eine landeseigene Bildungseinrichtung hatte uns Ende des vergangenen Jahres eine Datenpanne gemeldet,

[179] Siehe auch C.I.2.

weil eine Festplatte mit einem für die Archivierung bestimmten Abbild von personenbezogenen Daten nicht mehr auffindbar war. Das Abbild war unverschlüsselt auf einer Festplatte gespeichert, die ungesichert in einem Büro verwahrt worden war.

Wir haben die Bildungseinrichtung aufgefordert, alle betroffenen Personen zu benachrichtigen und den rechtlichen Anforderungen an einen digitalen Archivierungsprozess nachzukommen. Der Archivierungsprozess muss nach Art. 32 Abs. 1 DSGVO ein geeignetes Management zur Pseudonymisierung und Verschlüsselung der verarbeiteten Daten aufweisen und über eine Review-Strategie verfügen, die die Wirksamkeit der zum Schutz der Daten vorgenommenen technischen und organisatorischen Maßnahmen regelmäßig überprüft. Dabei sind der Stand der Technik und die Implementierungskosten sowie die Art, der Umfang, die Umstände und die Zwecke der Datenverarbeitung zu berücksichtigen. Die Gewährleistung der Sicherheit der Daten erstreckt sich auch immer auf die Aufbewahrung und Archivierung sowie etwaige Transportwege von Daten, gleich ob sie auf Papier festgehalten, in öffentlichen Netzwerken oder unternehmensinternen Systemen abgelegt oder – wie in dem uns vorliegenden Fall – auf mobilen Datenträgern gespeichert sind.

Verantwortliche müssen sicherstellen, dass zu jedem Zeitpunkt nur berechtigte Personen auf diese Daten zugreifen können. Im Fall der Sicherung der Daten auf einem mobilen Datenträger muss dieser folglich so aufbewahrt oder transportiert werden, dass die auf ihm gespeicherten Daten für unberechtigte Personen unzugänglich sind. Eine Verschlüsselung der Daten nach dem Stand der Technik ist auch hier unabdingbar. Ob dabei eine Verschlüsselung des gesamten Datenträgers vorgenommen wird oder dessen Inhalte einzeln verschlüsselt werden,[180] ist im Einzelfall auf Grundlage der jeweiligen Datenverarbeitung zu entscheiden. Zwischenzeitlich konnte uns die -Bildungseinrichtung ein zufriedenstellendes Konzept zur Verbesserung ihres Archivierungsprozesses vorstellen.

Verantwortliche müssen bei jedweder Aufbewahrung und jedwedem Transport die Sicherheit der Daten gewährleisten. Auf digitaler Ebene leistet dies deren Verschlüsselung; auf physischer Ebene sind Vorkehrungen zu treffen, die geeignet sind, unrechtmäßigen Zugriff zu jeder Zeit zu verhindern.

[180]Siehe BSI, Verschlüsselung mit Software & Hardware, abrufbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datenverschluesselung/Soft-und-hardwaregestuetzte-Verschluesselung/soft-und-hardwaregestuetzte-verschluesselung.html.

X. Informationsfreiheit

1. Fehlerhafte Rechtsbehelfsbelehrungen

In diesem Jahr mussten wir häufig feststellen, dass die Rechtsbehelfsbelehrungen von Behörden bei (Teil-)Ablehnungen des Informationszugangs fehlerhaft waren. Zwar wiesen die entsprechenden Bescheide auf die Zulässigkeit eines Widerspruchs hin, der innerhalb eines Monats nach Bekanntgabe „schriftlich oder zur Niederschrift" bei der jeweiligen Behörde eingegangen sein muss. Es fehlte jedoch der Hinweis, dass der Widerspruch auch „in elektronischer Form" eingelegt werden kann.

Bei (Teil-)Ablehnungen von Anträgen nach dem Berliner Informationsfreiheitsgesetz (IFG) ist ein Widerspruchsverfahren durchzuführen.[181] Der Widerspruch ist innerhalb eines Monats nach Bekanntgabe schriftlich, in elektronischer Form[182] oder zur Niederschrift bei derjenigen Behörde einzulegen, die den Verwaltungsakt erlassen hat.[183] Die Widerspruchsfrist beginnt, sobald über den Rechtsbehelf, die Verwaltungsbehörde, den Sitz und die einzuhaltende Frist schriftlich oder elektronisch belehrt worden ist. Ist die Belehrung unterblieben oder unrichtig erteilt, verlängert sich die Frist: Die Einlegung des Widerspruchs ist dann grundsätzlich innerhalb eines Jahres ab Bekanntgabe des Verwaltungsakts zulässig.[184]

Zwar bedarf es grundsätzlich keiner Belehrung über die Art und Weise, wie ein Rechtsbehelf einzulegen ist. Wenn aber mit „schriftlich oder zur Niederschrift" schon Angaben über die Form des Widerspruchs gemacht werden, müssen diese vollständig sein. Dies ist nicht der Fall, wenn in der Rechtsbehelfsbelehrung die Möglichkeit der Erhebung des Widerspruchs in elektronischer Form nicht erwähnt wird.[185]

Die Polizei Berlin ist von der Kritik der Berliner Beauftragten für Datenschutz und Informationsfreiheit, Rechtsbehelfsbelehrungen der Behörden seien häufig unvollständig, weil der Hinweis fehle, dass der Widerspruch auch in elektronischer Form eingelegt werden könne, nicht betroffen.
Ein entsprechender Hinweis auf die Erhebung des Widerspruchs in elektronischer Form muss nach § 58 Abs. 2 VwGO i. V. m. § 3a VwVfG nur dann in die Rechtsbehelfsbelehrung mit aufgenommen werden, wenn der Empfänger, mithin also die Behörde, einen Zugang für die Übermittlung elektronischer Dokumente eröffnet hat. Einen solchen Zugang hat die Polizei Berlin jedoch bislang aus technischen Gründen nicht einrichten können. Folglich kann sie keine elektronischen Dokumente im Sinne des § 3a Abs. 1 VwVfG empfangen, sodass es sogar fehlerhaft wäre, die Rechtsbehelfsbelehrung um den Hinweis der Möglichkeit einer elektronischen Einlegung des Rechtsbehelfes zu ergänzen.

[181] Siehe § 14 Abs. 3 IFG, § 68 Verwaltungsgerichtsordnung (VwGO).
[182] § 3a Verwaltungsverfahrensgesetz (VwVfG).
[183] § 70 Abs. 1 Satz 1 VwGO.
[184] Siehe § 70 Abs. 2, § 58 Abs. 2 Satz 1 Hs. 1 VwGO.
[185] Verwaltungsgericht (VG) Berlin, Urteil vom 20. Oktober 2016, 2 K 568.15, sowie Urteil vom 28. September 2022, 2 K 88/21.

Rechtsbehelfsbelehrungen sorgen bei allen Beteiligten nur dann für Rechtssicherheit, wenn richtig belehrt wurde. Die Behörden müssen die Formulierungen überarbeiten, den Hinweis auf einen elektronischen Widerspruch entweder ergänzen oder alternativ ganz auf derartige Angaben verzichten.

2. Offenlegung des Verzeichnisses der Verarbeitungstätigkeiten

In diesem Jahr haben uns mehrere Beschwerden erreicht, weil Behörden sich geweigert haben, das datenschutzrechtlich erforderliche Verzeichnis der Verarbeitungstätigkeiten auf Anfrage offenzulegen. Diese Verweigerung findet in der Regel keine rechtliche Grundlage, vielmehr ist eine teilweise Freigabe unter Schwärzung der sicherheitsrelevanten und geheimhaltungswürdigen Informationen zu gewähren.

Nach Art. 30 Abs. 4 Datenschutz-Grundverordnung (DSGVO) müssen Verantwortliche und Auftragsverarbeiter das Verzeichnis der Verarbeitungstätigkeiten auf Anfrage der Aufsichtsbehörde zur Verfügung stellen. Ein Einsichtsrecht für „jedermann“ – wie noch in der Datenschutzrichtlinie 95/46/EG vorgesehen – findet sich in der DSGVO nicht. Insofern ist das IFG für den Zugangsanspruch anwendbar und der Umfang des Informationszugangs nur bei Vorliegen eines gesetzlichen Ausschlussgrunds ganz oder teilweise beschränkt.

Die DSGVO sieht die Verpflichtung vor, angemessene technisch-organisatorische Maßnahmen zu ergreifen, um ein dem Risiko der Verarbeitung von Daten angemessenes Schutzniveau bei der Verarbeitung zu erreichen. Solchen Sicherheitsmaßnahmen kann es immanent sein, dass sie geheim gehalten werden, da eine Offenbarung die Eignung der Maßnahme vereitelt. Vor diesem Hintergrund wären §§ 7 und 11 IFG als Ausschlussgründe denkbar, die aber – wie alle Ausnahmevorschriften – eng auszulegen sind. Danach ist der Informationszugang zu verneinen, wenn ein Betriebsgeheimnis offenbart wird bzw. das Bekanntwerden der Information eine schwerwiegende Gefährdung des Gemeinwohls zur Folge hätte. Im Fall von Verarbeitungsverzeichnissen kann dies für sicherheitskritische Informationen über technische und organisatorische Maßnahmen zutreffen. Dass ein Verarbeitungsverzeichnis allerdings in Gänze geheimhaltungsbedürftig ist, ist regelmäßig nicht anzunehmen. Die Behörden haben daher zu begründen, warum auch eine teilweise und um die betreffenden Stellen geschwärzte Offenlegung der Verarbeitungsverzeichnisse nicht in Betracht kommt.[186]

Dem für Grundsatzangelegenheiten des allgemeinen Datenschutzrechts sowie des Informationsfreiheitsrechts zuständigen Referat bei der Senatsverwaltung für Inneres und Sport sind derartige Fälle nicht bekannt geworden.

[186] § 15 Abs. 3, § 12 IFG.

Das von der DSGVO geforderte Verzeichnis der Verarbeitungstätigkeiten ist nur in den wenigsten Fällen von vornherein und in Gänze als schutzbedürftig anzusehen. Bei Anfragen nach dem IFG sind die Verzeichnisse auf sicherheitskritische und geheim zu haltende Informationen zu überprüfen und die betreffenden Stellen ggf. zu schwärzen.

3. Aktenprüfungen vor Ort

Wird ein Antrag auf Akteneinsicht von der aktenführenden Stelle (vollständig oder teilweise) abgelehnt und werden wir daraufhin von der antragstellenden Person wegen der Verweigerung des Informationszugangs angerufen, erfordert unsere Schieds-stellenfunktion es manchmal, dass wir uns vor Ort ein eigenes Bild von der streitbefangenen Akte machen. Dieses Jahr haben wir eine solche Vor-Ort-Prüfung in zwei Fällen durchgeführt, nämlich bei einem bezirklichen Veterinäramt sowie bei den -Berliner Wasserbetrieben (BWB).

Im bezirklichen Veterinäramt ging es um die Ablehnung eines Antrags auf Akteneinsicht zum Fall der Tötung eines Hundes. Es stellte sich heraus, dass die fast 90 Seiten umfassende Akte zusätzlich in einem vierseitigen Vermerk zusammengefasst war, dem sich die von der antragstellenden Person gewünschten Informationen entnehmen ließen. So konnte umgehend ein Kompromissvorschlag an die antragstellende Person verfasst werden, der die Einsicht in den Vermerk gegen eine relativ geringe Gebühr anbot. Aus rechtlichen Gründen verweigerte sich das Veterinäramt zunächst dem Wunsch der antragstellenden Person auf postalische Zusendung einer Kopie des Vermerks, revidierte diese Haltung aber nach unserem Hinweis, dass ein Wahlrecht zwischen der Einsicht vor Ort und der Übersendung von Kopien besteht.[187]

In einem weiteren Fall ging es um die Beseitigung einer Grünanlage im Zuständigkeitsbereich der BWB. Der Petent hatte bereits Unterlagen eingesehen, rügte aber, dass die ihm vorlegten Akten unvollständig seien, da sie seine Korrespondenz mit den BWB nicht enthielten. Wie sich bei unserer Vor-Ort-Prüfung herausstellte, war diese nicht den Akten beigefügt worden, da sie für die Bearbeitung des Falls nicht erforderlich war. Der Petent hatte dementsprechend bereits vollständige Akteneinsicht erhalten.

[187]Siehe VG Berlin, Urteil vom 9. November 2022, 2 K 268/21, S. 4 m. w. N.

Obwohl wir nur die Funktion einer Schiedsstelle innehaben und für die Überprüfung der Einhaltung des IFG auf die Mitarbeit der betreffenden Behörden und öffentlichen Stellen angewiesen sind, hat sich unsere Aktenprüfung vor Ort für unsere Fälle als hilfreich erwiesen. Zur Vorbereitung bitten wir die aktenführende Stelle regelmäßig, uns den in Rede stehenden Originalvorgang sowie die zur Einsicht durch die antragstellende Person vorbereitete und mit Schwärzungen versehene Kopie vorzulegen, sofern diese bereits erstellt wurde. Zudem bitten wir um die Anwesenheit einer entscheidungsbefugten Person für den Fall, dass im Laufe der Aktenprüfung eine Änderung der Ablehnungsentscheidung herbeigeführt werden kann. So bleiben wir in engem Austausch mit der Verwaltung und können auf kurzem Dienstweg gemeinsam Lösungen im Sinne des IFG für alle Beteiligten herbeiführen.

4. Recht auf Akteneinsicht in Senatsbeschlüsse

Eine Antragstellerin wollte sich über die politischen Entscheidungen zur Berliner Ernährungsstrategie informieren und begehrte von der Senatskanzlei Einsicht in die entsprechenden Beschlüsse des Rats der Bürgermeister (RdB) sowie des Senats. Die Senatskanzlei lehnte den Antrag unter Hinweis auf den Schutz des behördlichen Entscheidungsprozesses ab, woraufhin sich die Bürgerin an uns wandte und Widerspruch gegen den Ablehnungsbescheid einlegte.

Wir machten die Senatskanzlei darauf aufmerksam, dass die Ablehnung des Antrags unter Berufung auf § 10 Abs. 3 Nr. 1 IFG in Bezug auf den Senatsbeschluss und auf § 10 Abs. 4 IFG in Bezug auf den RdB-Beschluss zu Unrecht erfolgt war. Wir beriefen uns dabei auf die verwaltungsgerichtliche Rechtsprechung. Danach schützen beide Vorschriften nur die Beratung bzw. den Willensbildungsprozess im engeren Sinne, d. h. die Besprechung, Beratschlagung und Abwägung, mithin den eigentlichen Vorgang des Überlegens bzw. der behördlichen Entscheidungsfindung. Nicht geschützt sind dagegen die Tatsachengrundlagen und das Ergebnis der Willensbildung.[188] Unserer Bitte, dem Widerspruch der Bürgerin entsprechend abzuhelfen und Akteneinsicht zu gewähren, kam die Senatskanzlei erst nach weiterer Überzeugungsarbeit nach, allerdings ausdrücklich ohne Anerkennung einer Rechtspflicht.

Offenbar geht die Senatskanzlei immer noch von einer grundsätzlichen Vertraulichkeit von Senatsbeschlüssen aus, wie die Antwort auf eine Schriftliche Anfrage vom

[188] Siehe Oberverwaltungsgericht (OVG) Berlin-Brandenburg, Urteil vom 20. Dezember 2017, 12 B 12.16; VG Berlin, Urteil vom 25. August 2016, 2 K 92.15.

23. Januar 2023 vermuten lässt.[189] Die Vertraulichkeitsregelung in § 14 Abs. 2 Geschäftsordnung des Senats (GOSen) kann aber die Vorschriften eines förmlichen Gesetzes, hier des IFG, nicht aushebeln. Die in der Verfassung von Berlin (VvB) vorgesehene Ermächtigungsgrundlage für die GOSen beinhaltet nur die Aussage, dass der Senat sich eine Geschäftsordnung gibt, nicht aber mit welchem Inhalt.[190] Damit sind für die Reichweite der Zugangsbeschränkungen allein die Ausnahmevorschriften des IFG maßgeblich, die eine generelle Vertraulichkeit der Beschlüsse nicht hergeben. Die Anpassung der GOSen an die gesetzlichen und durch die Rechtsprechung präzisierten Vorgaben ist überfällig.[191]

Die Prüfung, ob Senatsbeschlüsse offenzulegen sind, erfolgt allein auf der Grundlage des IFG. Entgegenstehende, insbesondere untergesetzliche Vorschriften wie die Geschäftsordnung des Senats sind an die Rechtslage anzupassen.

Dem Senat ist bewusst, dass formelle Gesetze in der Normenhierarchie über der Geschäftsordnung des Senats stehen. In die Geschäftsordnung des Senats wird eine entsprechende Klarstellung aufgenommen.

5. Unzulässige Mehrfacherhebung von Gebühren bei Aktenauskunft

Unabhängig voneinander beantragten mehrere Personen Zugang zu einem Prüfvermerk bei der Senatsverwaltung für Justiz und Verbraucherschutz (SenJustVA). Mit diesem Vermerk kommt die SenJustVA zu dem Ergebnis, dass die „Letzte Generation", ein Zusammenschluss von Klimaaktivist:innen, nicht als kriminelle Vereinigung einzustufen ist. Die Antragsteller:innen erhielten die Mitteilung, dass die Übersendung des 30-seitigen Vermerks in einer geschwärzten Fassung zulässig sei. Unter Berücksichtigung des Bearbeitungsaufwands wurde jeweils eine Gebühr in Höhe von 15 Euro in Rechnung gestellt. Der Prüfvermerk war allerdings zuvor schon an andere Stellen in geschwärzter Fassung übermittelt worden.

Auch wenn es zutreffend ist, dass bei einer erneuten Aktenauskunft und Übersendung eines notwendigerweise mit Schwärzungen versehenen Dokuments diese Anonymisierungen nicht ein weiteres Mal geprüft werden müssen, so verbleibt bei jeder schriftlichen Auskunftserteilung dennoch ein Verwaltungsaufwand. Dieser Verwaltungsaufwand, der mit der Auskunftserteilung nach dem Berliner IFG einhergeht, ist, wie § 16 IFG ausdrücklich bestimmt, gebührenpflichtig. § 16 IFG verweist auf das Gesetz über Gebühren und Beiträge (GebBeitrG). Die nach § 6 Abs. 1 GebBeitrG einschlägige Verwaltungsgebührenordnung (VGebO) bestimmt in § 1 Abs. 1 VGebO, dass Verwaltungsgebühren nach dieser Gebührenordnung und dem anliegenden Gebührenverzeichnis erhoben werden. Tarifstelle 1004 des Gebührenverzeichnisses regelt die Gebühren für Amtshandlungen nach dem Berliner IFG. Nach Buchstabe a) Ziffer 2 wird für einfache schriftliche Auskünfte ein Gebührenrahmen von 5 bis 100,- Euro vorgegeben. Eine Gebührenfreiheit sieht die Tarifstelle 1004 nach Buchstabe a) Ziffer 1 lediglich bei mündlichen Auskünften vor, die

[189] Abgeordnetenhaus, Drs. 19/14 680, Schriftliche Anfrage vom 23. Januar 2023 mit Antwort des Senats vom 13. Februar 2023 zum Thema: „Warum sind Senatsbeschlüsse Herrschafts-wissen der Regierenden Bürgermeisterin?".

[190] Siehe Art. 58 Abs. 4 VvB.

[191] Bereits 2012 haben wir die Aktualisierung der GOSen sowie die proaktive Veröffentlichung der Senatsbeschlüsse im Internet empfohlen; siehe Abgeordnetenhaus, Wortprotokoll 17/36 zur Sitzung des Ausschusses für Digitale Verwaltung, Datenschutz und Informationsfreiheit am 17. Februar 2014, S. 22 ff., abrufbar unter https://www.parlament-berlin.de/ados/17/ITDat/protokoll/it17-036-wp.pdf.

Wir haben der Senatsverwaltung mitgeteilt, dass der Bearbeitungsaufwand für die Prüfung des Vermerks und die Durchführung von erforderlichen Schwärzungen nicht mehrfach, also mehreren Antragsteller:innen, gleichermaßen in Rechnung gestellt werden darf. Vielmehr muss die bereits zuvor offengelegte Fassung gebührenfrei übersendet werden. Für den Fall, dass dennoch eine Gebühr in Betracht gezogen werde,[192] haben wir gebeten, einen Gebührenverzicht zu prüfen.[193] Die Senatsverwaltung reduzierte die Gebühr daraufhin um die Hälfte des Betrags. Die verbleibende Gebühr in Höhe von 7,50 Euro begründete sie wie folgt: „Eine weitere Reduktion der Kosten oder kostenfreie Übersendung kann nicht erfolgen, da die Ihnen zu übersendende Fassung händisch erstellt und die erfolgreiche Anonymisierung Seite für Seite geprüft werden muss und insoweit ein Verwaltungsaufwand verbleibt."

Diese Auffassung ist weder tatsächlich noch rechtlich nachvollziehbar, war das Dokument doch genau in dieser Fassung bereits offengelegt worden. Aus den geltenden Gebührenvorschriften[194] kann die erneute Erhebung einer Gebühr nicht hergeleitet werden. Dies hanicht mit einem besonderen Arbeitsaufwand verbunden sind. Da vorliegend die Übersendung eines Dokuments begehrt worden war, verbleibt es auch nach den bereits notwendigerweise vorgenommenen Schwärzungen damit zwingend bei einer Gebühr im Bereich des oben genannten Gebührenrahmens. Dementsprechend ist die Auffassung, dass für wiederholte gleichgelagerte Auskünfte nach dem Berliner IFG Kostenfreiheit bestünde, rechtlich nicht haltbar. Auch für den vorgeschlagenen Gebührenverzicht bestand kein Raum, da angesichts der beschriebenen Mindestgebühr von 5,- Euro ein Rückgriff auf § 1 Abs. 2 VGebO nicht in Betracht kam. Auch wenn derselbe Bearbeitungsaufwand (hier für die Durchführung von erforderlichen Anonymisierungen) nicht mehrfach, also mehreren Antragsstellenden in Rechnung gestellt werden kann, wenn dieser Aufwand tatsächlich nur einmal anfällt, so ist auch im Falle einer mehrfachen schriftlichen Auskunftserteilung in derselben Sache jedenfalls eine geringe Gebühr in Ansatz zu bringen.

[192]Nach dem Gebührenverzeichnis der Verwaltungsgebührenordnung (VGebO) sind hier Gebühren zwischen 1 und 2 Euro pro Dokument bzw. Datei möglich, siehe Tarifstelle 1001e des Gebührenverzeichnisses der VGebO.
[193]Siehe § 1 Abs. 2 VGebO.
[194]Siehe Tarifstellen 1001 und 1004 des Gebührenverzeichnisses der VGebO sowie die von der Senatsverwaltung für Finanzen (SenFin) festgelegten Stundensätze in der Fassung vom 26. April 2023, abrufbar unter https://www.datenschutz-berlin.de/informationsfreiheit/rechtliche-grundlagen/gebuehren/.

ben wir der Justizverwaltung mitgeteilt, die uns daraufhin darüber informierte, dass eine der antragstellenden Personen ihren Antrag zurückgenommen habe, die andere das gewünschte Dokument gegen Zahlung von 7,50 Euro postalisch erhalten werde. Die Gebühr wurde nun damit gerechtfertigt, dass eine erneute Überprüfung der Schwärzungen erfolgen musste, um auszuschließen, dass die unkenntlich gemachten Textpassagen nicht doch durch die Verwendung verschiedener Drucker und Programme lesbar seien. Wir gehen davon aus, dass diese Aussage in künftigen vergleichbaren Fällen nicht mehr gilt. Denn die enthaltene Grundsatzproblematik, die auch bei datenschutzrechtlichen Vorgängen relevant werden könnte, sollte zwischenzeitlich technisch gelöst sein.

Die relativ niedrige Gebühr darf nicht darüber hinwegtäuschen, dass die Mehrfacherhebung einer auf denselben Verwaltungsaufwand bezogenen Gebühr bei verschiedenen Antragsteller:innen unzulässig ist. Nach der ersten Offenlegung eines Dokuments ist nicht davon auszugehen, dass derselbe Verwaltungsaufwand erneut entsteht. Spätere Antragsteller:innen sollten daher keine oder nur sehr geringe Gebühren für die erneute Bereitstellung des Dokuments entrichten müssen.

6. Anspruch auf Auskunft bei der Polizei

Ein Antragsteller wollte von der Polizei erfahren, wie oft sie zwischen Januar und März dieses Jahres zur Rettung von Tieren gerufen wurde. Hierauf erhielt er folgendes Schreiben: „Der Anwendungsbereich des IFG ist vorliegend nicht eröffnet. Ihr Anliegen habe ich entsprechend an den zuständigen Fachbereich der Polizeiakademie weitergeleitet. Anfragen im Rahmen eines Studienprojektes werden von dort bearbeitet. Sie erhalten von dort unaufgefordert eine Benachrichtigung."

Die Polizeiakademie, die nun mit der Anfrage betraut war, forderte den Antragsteller auf, ein mitgeliefertes Anfrageformular auszufüllen, eine Verschwiegenheitsverpflichtungserklärung sowie eine Datenschutzerklärung zu unterschreiben. Zusätzlich sei ein Autorisierungsschreiben einer Bildungseinrichtung beizufügen, aus dem sich nicht nur die Zugehörigkeit zur Einrichtung, sondern auch das Forschungsthema des Antragstellers ergebe. Dies könne auch durch Vorlage des Zulassungsschreibens der Forschungsarbeit bei der betreffenden Einrichtung erfolgen.

Wir haben der Polizei mitgeteilt, dass die Anfrage zwingend nach den Vorgaben des IFG zu bearbeiten ist, unabhängig davon, welche Stelle sich polizeiintern

für zuständig hält, und unabhängig davon, ob die Anfrage zu Studienzwecken erfolgt oder nicht. Es ist nicht erkennbar, aus welchem Grund „der Anwendungsbereich des IFG […] vorliegend nicht eröffnet“ sein soll. Die entsprechende von der Polizei ausgestellte Mitteilung ist folglich rechtswidrig. Ebenso rechtwidrig war die Aufforderung der Polizeiakademie, Voraussetzungen für den Informationszugang zu formulieren, die sich weder aus dem IFG noch aus anderen Vorschriften ergeben. Die angeforderten Erklärungen und Nachweise sowie die gewünschte Offenlegung des Motivs waren für die Bearbeitung des IFG-Auskunftsbegehrens nicht erforderlich, die Erhebung dieser personenbezogenen Daten dementsprechend unzulässig.[195]

Die Polizei hat daraufhin die bisherige Standardantwort für künftige Anfragen geändert. Es wird nun in ein und demselben Schreiben auf die kostenlose Unterstützung der Polizeiakademie hingewiesen, alternativ auf die gebührenpflichtige Auskunftserteilung nach dem IFG. Im konkreten Beschwerdefall hat die Polizei die begehrte Auskunft auf der Grundlage des IFG gegen die Zahlung einer geringen Gebühr erteilt.

In dem von der Berliner Beauftragten für Datenschutz und Informationsfreiheit beschriebenen Fall hat die Polizei den in Rede stehenden Auskunftsantrag nicht nach dem IFG Bln bearbeitet, sondern diesen zur weiteren Bearbeitung an die Polizeiakademie weitergeleitet, von wo die Auskünfte kostenfrei erteilt werden. Sie nahm an, dass dies im Sinne des Antragstellers sei, weil Auskünfte nach dem IFG Bln kostenpflichtig sind. Inzwischen verfährt sie so, wie von der Berliner Beauftragten für Datenschutz und Informationsfreiheit dargestellt und weist die Antragsteller auf die beiden möglichen Alternativen zur Auskunftserteilung hin.

Richtig ist, dass die Polizei den Antrag letztlich nach dem IFG Bln bearbeitet und dem Antragsteller in diesem Zusammenhang zunächst eine Anhörung mit der Information über die zu erwartende Gebührenhöhe zugesandt hat. Anders als von der Berliner Beauftragten für Datenschutz und Informationsfreiheit im Bericht dargestellt, ist die Auskunft jedoch nicht erteilt worden, weil der Antragsteller sich auf diese Anhörung hin nicht mehr zurückgemeldet hat.

Interne Organisationsstrukturen einer Behörde bzw. die Motive der Antragsteller:innen dürfen nicht dazu führen, dass zusätzliche Voraussetzungen für den Informationszugang formuliert werden, die sich nicht aus dem IFG ergeben.

7. Akteneinsichtsrecht des AStA

Der Allgemeine Studierendenausschuss (AStA) der Freien Universität (FU) Berlin hatte durch den Bericht einer Tageszeitung von der Finanzierung einer Stiftungsprofessur für Integrative und Anthroposophische

[195] Nach § 4a IFG ist die Verarbeitung personenbezogener Daten nur zulässig, soweit dies für die Erfüllung der im Gesetz genannten Aufgaben erforderlich ist.

Medizin an der Charité[196] erfahren und daraufhin Einsicht in sämtliche Unterlagen beantragt. Die Charité teilte mit, dass ein IFG-Auskunftsanspruch für den AStA als Teilkörperschaft des öffentlichen Rechts nicht bestehe. Sie verwies auf die Begründung zum IFG des Bundes[197], in der ein Auskunftsanspruch von juristischen Personen des öffentlichen Rechts verneint wird.[198] Hinsichtlich der darüber hinaus beantragten Gebührenbefreiung sei zudem fraglich, inwiefern der IFG-Antrag der Durchführung der Amtsgeschäfte des AStA dient.[199]

Nach § 3 Abs. 1 Satz 2 IFG sind juristische Personen antragsbefugt. Eine Beschränkung auf bestimmte Arten von juristischen Personen, etwa denen des Privatrechts oder solchen des öffentlichen Rechts, ist dem Wortlaut nach nicht vorgesehen. Es ließe sich allerdings – wie in der Begründung zum IFG des Bundes – annehmen, dass juristische Personen des öffentlichen Rechts von der Antragsberechtigung ausgeschlossen seien, da sie anstatt auf das IFG auf Amtshilfevorschriften, Auskunfts(verschaffungs)rechte und Übermittlungsbefugnisse zurückgreifen können. Wenn die juristische Person des öffentlichen Rechts aber ihrerseits grundrechtsberechtigt ist, der Gesetzeszweck eine Anspruchsberechtigung rechtfertigt und der Grundrechtsträger ein Informationsbedürfnis geltend macht – das in den Bereich seiner Grundrechtsfähigkeit fällt, es also in Ausübung des jeweiligen Grundrechts erfolgt –, ist die juristische Person des öffentlichen Rechts auch zur IFG-Antragstellung berechtigt.

Der Verfassungsgerichtshof (VerfGH) des Landes Berlin hat den AStA in einer Grundsatzentscheidung als juristische Person und Grundrechtsträger im Hinblick auf die Ausübung des Grundrechts aus Art. 21 VvB[200] anerkannt, der in gleicher Weise wie die FU Berlin selbst Grundrechtsschutz genießt.[201] Der AStA ist zudem auch Träger des Grundrechts der Rechtsweggarantie aus Art. 15 Abs. 1 und 4 VvB. Mit seinem IFG-Antrag verfolgt der AStA eine gesetzlich normierte Aufgabe, nämlich die Meinungsbildung der Studierenden zu ermöglichen.[202] Zugleich bezieht sich sein Informationsbedürfnis angesichts des Antragsgegenstandes auf

[196]Die Charité – Universitätsmedizin Berlin, so ihr vollständiger Name, vereint die medi-zinischen Fakultäten der FU Berlin und der Humboldt-Universität zu Berlin (HU). Sie ist eine Körperschaft des öffentlichen Rechts sowie Gliedkörperschaft der HU und der FU Berlin.
[197]Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz, IFG).
[198]Siehe Deutscher Bundestag, Drs. 15/4493, S. 7.
[199]Zu den Voraussetzungen einer Gebührenbefreiung siehe § 2 Abs. 1 und 2 VGebO.
[200]Art. 21 VvB besagt: „Kunst und Wissenschaft, Forschung und Lehre sind frei. Die Freiheit der Lehre entbindet nicht von der Treue zur Verfassung."
[201]VerfGH Berlin, Beschluss vom 21. Dezember 2000, 136/00.
[202]§ 18 Abs. 2 Satz 3 Nr. 2 Berliner Hochschulgesetz (BerlHG).

die Entwicklung von Wissenschaft, Forschung und Lehre, mithin auf den Schutzbereich von Art. 21 VvB.

Dessen ungeachtet besteht eine Antragsberechtigung einer öffentlichen Stelle aber auch dann, wenn sich diese nach der Zielsetzung des IFG mit den übrigen Anspruchsberechtigten in einer vergleichbaren Lage gegenüber der informationspflichtigen Stelle befindet und gerade keinen Zugriff auf die erwähnten Alternativen zur Informationsbeschaffung hat.[203] Auch dies traf auf den AStA zu: Er ist eine rechtsfähige Teilkörperschaft der FU Berlin mit Selbstverwaltungsbefugnis[204] und befindet sich gerade nicht in der gleichen Lage wie eine staatliche oder behördliche Stelle. Vielmehr tritt er gegenüber staatlichen Stellen als Interessenvertretung privater Personen, der Studierenden der FU Berlin auf, und ist damit selbst vergleichbar mit einer privaten Stelle. Er ist weder in behördliche Auskunftsstrukturen eingebunden noch kann er auf Amtshilfeersuchen oder entsprechende Mittel zur Befriedigung seines Informationsbedürfnisses zurückgreifen. In Erfüllung seiner Selbstverwaltungsaufgaben verfolgt der AStA zudem auch den Zweck des IFG: die Förderung demokratischer Meinungs- und Willensbildung sowie die Kontrolle staatlichen Handelns durch Zugang zu Informationen.

Die Charité hat sich schließlich unserer Auffassung angeschlossen, den AStA als antragsberechtigt im Sinne des IFG angesehen und die gewünschten Informationen gebührenfrei[205] zur Verfügung gestellt, weil die beantragte Offenlegung der Unterlagen der Durchführung der Amtsgeschäfte des AStA diente.

Der Fall ist bei beantragter Offenlegung von universitären Informationen von grundsätzlicher Bedeutung. Die Antragsbefugnis des AStA nach § 3 Abs. 1 Satz 2 IFG ist in der Regel ebenso zu bejahen wie die Gebührenbefreiung nach § 2 Abs. 1 Satz 1 Nr. 2 VGebO.

XI. Medienkompetenz

Kinder und Jugendliche werden von uns dabei unterstützt, die vernetzte und digitale Welt selbstbestimmt zu erleben. Dazu bieten wir Workshops an Grundschulen an und unterhalten Websites, die Kinder und Jugendliche zum Thema Datenschutz informieren. Unser Ziel ist

[203] Zum Jedermannsrecht bei Umweltinformationen siehe Bundesverwaltungsgericht (BVerwG), Urteil vom 21. Februar 2008, 4 C 13/07.
[204] § 18 Abs. 1 Sätze 2 und 3 BerlHG.
[205] Siehe § 2 Abs. 1 Satz 1 Nr. 2 VGebO.

es, ihnen zu vermitteln, bewusst und informiert mit dem Internet und den Medien umzugehen und ihre Daten zu schützen. Zusätzlich haben wir eine Veranstaltungsreihe zum Austausch mit medienpädagogischen Fachkräften ins Leben gerufen, um gemeinsam Methoden zur Ausbildung der Medienkompetenz zu erarbeiten.

Regelmäßig stehen Pädagog:innen vor der Herausforderung, den Schulalltag mit den digitalen Medien in Einklang zu bringen. Es erfordert einen sinnvollen und reflektierten Einsatz in der Unterrichtspraxis, um die Schüler:innen zum einen in ihrer Lebensrealität abzuholen und zum anderen in ihrem Medienverhalten zu schulen. Wir haben uns daher zum Ziel gesetzt, Medienpädagog:innen in ihrer Arbeit zu unterstützen, indem wir ihnen die rechtlichen Grundlagen des Datenschutzes vermitteln und gemeinsam Möglichkeiten zur Förderung der Medienkompetenz erarbeiten.

In Kooperation mit dem Jugendnetz Berlin haben wir Ende März dieses Jahres den ersten Fachtag zum Thema „Datenschutz trifft Medienkompetenz“ veranstaltet. Auf Basis der Erfahrungen der knapp 60 Teilnehmer:innen wurden die datenschutzrechtlichen Aspekte im Umgang mit digitalen Medien beleuchtet und Methoden der medien-pädagogischen Vermittlung von Datenschutz und Medienkompetenz herausgearbeitet. Der Austausch hat sich als ausgesprochen hilfreich erwiesen; wir planen daher, die Fachtage künftig regelmäßig durchzuführen.

Zudem haben wir im Berichtszeitraum 28 Workshops in Grundschulklassen der Jahrgangsstufen 4 bis 6 an verschiedenen Grundschulen in Berlin abgehalten. In jeweils fünf Unterrichtsstunden vermitteln wir den Schüler:innen die Relevanz von Datenschutz und machen ihnen ihre Rechte in Bezug auf Privatsphäre, informationelle Selbstbestimmung und Schutz der eigenen Daten bewusst. Besonderes Augenmerk gilt hierbei den Fragen, wie mit sozialen Medien und Werbung verantwortungsvoll umgegangen werden kann bzw. welche Risiken bestehen, was bei Cybermobbing zu tun ist und welche Veränderungen durch die Verwendung künstlicher Intelligenz zu erwarten sind. In unserem medienpädagogischen Konzept verfolgen wir einen handlungsorientierten Ansatz, bei dem die Schüler:innen Internetrecherchen zu ihren Rechten in der Datenschutzwelt durchführen. Zudem setzen wir auf projektorientierten Unterricht: Die Erstellung von Präsentationen zum Thema personalisierte Werbung fördert sowohl die Medienkompetenz als auch das kritische Denken der Kinder.

Um gemeinsam die Neuauflage der vor zehn Jahren gestarteten Website youngdata.de umzusetzen, schlossen sich die Mitarbeiter:innen der Öffentlichkeitsarbeit und Medienpädagogik verschiedener Aufsichtsbehörden zu einer länderübergreifenden Arbeitsgruppe zusammen. Zum Team gehörten neben uns die Aufsichtsbehörden von Hamburg, Mecklenburg-Vorpommern, Rheinland-Pfalz und dem Bund. Nach gut einem Jahr Vorbereitungszeit konnte der Relaunch zum 11. Mai dieses Jahres erfolgreich zum Abschluss gebracht werden. Die neu gestaltete Website wurde erfreulicherweise Anfang Dezember nach einer einmonatigen Abstimmungsphase unter 4.238 Jugendlichen mit dem 3. Platz des Kindersoftwarepreises TOMMI in der Kategorie „Jugendpreis Bildung“ ausgezeichnet.[206]

Auch unsere eigene Website data-kids.de, die Kinder zwischen 6 und 13 Jahren mit dem Datenschutz vertraut macht und dieses Jahr um neue Merk- und Ratespiele ergänzt wurde, wurde geehrt: Sie erhielt am 7. Dezember das Seitenstark-Gütesiegel, das gemeinsam von Seitenstark e. V., MDR Thüringen und den Landesmedienanstalten herausgegeben und vom Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) im Rahmen der Initiative „Gutes Aufwachsen mit Medien“ gefördert wird.[207] Das Siegel prämiert qualitativ hochwertige Onlineangebote für Kinder, um die Angebotsvielfalt digitaler Kindermedien nachhaltig zu fördern.[208]

Zur Förderung der Medienkompetenz für Kinder und Jugendliche sind zwei Bereiche entscheidend: auf der einen Seite die Stärkung der Lehr- und Fachkräfte in ihrer medienpädagogischen Arbeit mit Kindern, auf der anderen Seite die kindgerechte Vermittlung von datenschutzrechtlichen Aspekten und Kompetenz beim Umgang mit Medien. Je früher Kinder und Jugendliche verstehen, wie sie selbst Einfluss darauf nehmen können, was mit ihren Daten geschieht, desto eher werden sie selbstbewusst von ihren Rechten zu Datenschutz, Privatsphäre und informationeller Selbstbestimmung Gebrauch machen. Die Zusammenarbeit mit den Kolleg:innen weiterer Aufsichtsbehörden des Bundes und der Länder erweist sich hierbei als ausgesprochen produktiv und wird in weiteren Projekten fortgesetzt.

[206]Siehe Pressemitteilung zur TOMMI-Auszeichnung von youngdata.de, abrufbar unter https://youngdata.de/n/auszeichnung-fuer-youngdatade-jugendwebseite-der-datenschutzkonferenz-holt-3-platz-beim-medienpreis-tommi.
[207]Siehe Pressemitteilung zur Auszeichnung von data-kids.de mit dem Seitenstark-Gütesiegel, abrufbar unter https://www.datenschutz-berlin.de/pressemitteilung/ausgezeichnet-data-kidsde-erhaelt- seitenstark-guetesiegel/.
[208]Weitere Informationen zum Seitenstark-Gütesiegel sind abrufbar unter https://seitenstark.de/eltern-und-lehrkraefte/das-seitenstark-guetesiegel.

B. Wir in Deutschland

I. Gesetzesvorhaben des Bundes

1. Umsetzung der Europäischen Datenstrategie in nationales Recht

Gemeinsam mit anderen deutschen Datenschutzaufsichtsbehörden haben wir uns aktiv in Gesetzgebungsverfahren eingebracht, um eine nachhaltige und umfassende Debatte über die nationale Umsetzung der mit der Europäischen Datenstrategie verknüpften Rechtsakte auf Bundes- und Länderebene zu befördern und erste Vorschläge für ein deutschlandweites Digitalkonzept zu machen.

Nach der Vorstellung der Europäischen Datenstrategie am 19. Februar 2020 durch die Europäische Kommission sind mittlerweile wichtige Gesetze, wie etwa der Digital Services Act, der Digital Market Act, der Data Act und der Data Governance Act, in Kraft getreten und verlangen die Umsetzung auf nationaler Ebene. Für andere ebenso zentrale Rechtsakte wie den Artificial Intelligence Act sind politische Einigungen bereits erzielt oder sollen alsbald erreicht werden. Zusammen mit weiteren wichtigen Bausteinen wie dem Verordnungsentwurf für einen Datenraum im Gesundheitswesen entsteht so ein klares Bild der künftigen europäischen Rahmenbedingungen für Datennutzung und Zukunftstechnologien wie Künstliche Intelligenz (KI). Mit den Regulierungskonzepten ist die Aufforderung an die durch die Mitgliedstaaten zu bestimmenden Vollzugsbehörden verbunden, koordiniert und kooperativ für die kohärente Anwendung des neuen europäischen Datenrechtsrahmens Sorge zu tragen.

Ein nationales Digitalkonzept erfordert die Einführung risikoadäquater Schutzmechanismen und wirksame Kontrollmechanismen durch unabhängige Aufsichtsbehörden. Sind diese doch Grundbedingungen für das Vertrauen und die Akzeptanz der Menschen und damit für den Erfolg der digitalen Transformation. Die in den Gesetzgebungsverfahren eingebrachten Vorschläge zielen im Wesentlichen darauf ab, die bestehenden Strukturen zu nutzen und fortzuentwickeln. Dementsprechend empfehlen wir, die Datenschutzaufsichtsbehörden einzubinden, da diese ohnehin zuständig sind, wenn personenbezogene Daten verarbeitet werden. Zur Umsetzung der Europäischen Datenstrategie wird es aber erforderlich sein, zusätzliche Kooperationsregelungen als Bindeglied der unterschiedlichen Zuständigkeitsbereiche zu schaffen, mit denen die Zusammenarbeit der Datenschutzaufsichtsbehörden mit anderen Behörden, wie etwa Medienaufsicht, Verbraucherschutz oder Marktaufsicht, erfolgen kann. Nicht erst seit der

Etablierung der Kooperationsregelungen der Datenschutz-Grundverordnung (DSGVO) verfügen die Datenschutzaufsichtsbehörden über einen reichen Erfahrungsschatz in der Kooperation mit nationalen und europäischen Behörden. Es gilt, diese Expertise bei der Entwicklung und Umsetzung eines nationalen Digitalkonzepts zu nutzen.

Es bedarf dringend eines nationalen Digitalkonzepts, um die Europäische Datenstrategie wirksam und sinnvoll umzusetzen. Dabei sollten die bereits bestehenden Aufsichtsstrukturen im Datenschutzbereich genutzt werden. Zusätzlich sind klare Zuständigkeitsbereiche zuzuweisen und praktikable Regelungen zur Kooperation zwischen Datenschutzaufsichtsbehörden und anderen Behörden zu schaffen, damit die Umsetzung erfolgreich durchgeführt werden kann.

2. Onlinezugangsgesetz und Digitalisierung der Verwaltung

Mit dem Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie -weiterer Vorschriften zur Digitalisierung der Verwaltung (OZGÄndG) sollen auch neue datenschutzrechtliche Regelungen in Deutschlands zentrales Gesetz zur bundes-länderübergreifenden Verwaltungsdigitalisierung, das Onlinezugangsgesetz (OZG), aufgenommen werden.

Als Vorsitz der von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eingesetzten „Kontaktgruppe OZG 2.0“ haben wir in enger Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Beratungs- und Fachgespräche mit dem federführenden Bundesministerium des Innern und für Heimat (BMI) geführt sowie Stellungnahmen zum Referentenentwurf und später zum Gesetzesentwurf erarbeitet. Viele der Änderungsvorschläge, die im Rahmen unserer Abstimmungen mit dem BMI zum Referentenentwurf erörtert wurden, haben im Gesetzesentwurf Berücksichtigung gefunden.

Die datenschutzrechtlichen Anpassungen durch das OZGÄndG, die insbesondere im neuen, zusätzlich ins OZG eingefügten § 8a umgesetzt werden, sollen Klarheit hinsichtlich der datenschutzrechtlichen Verantwortung der zahlreichen an den OZG-Umsetzungsprojekten beteiligten öffentlichen Stellen herbeiführen.[209] Darüber hinaus schaffen insbesondere die Abs. 1 und 2 im neuen § 8a OZG gesetzliche Rechtsgrundlagen für

[209] Siehe hierzu die mit der Aufnahme von § 8a Abs. 4 in das OZG geregelte Verantwortungs-zuweisung i. S. d. Art. 4 Nr. 7 Hs. 2 DSGVO.

die Verarbeitung personenbezogener Daten im Rahmen der bundesländerübergreifenden Bereitstellung von OZG-Leistungen. In Bezug auf die praktische Umsetzung dieser neuen Regelungen zum Datenschutz stellt sich jedoch noch eine Reihe von Fragen. Als Vorsitz der „Kontaktgruppe OZG 2.0“ setzen wir uns dafür ein, dass diese Datenschutzfragen möglichst einheitlich durch die Aufsichtsbehörden des Bundes und der Länder bewertet werden, und unterstützen so die für die OZG-Umsetzung zuständigen Behörden.

Die Anpassungen im Entwurf eines OZGÄndG betreffen die Verantwortungszuweisung bei bundesländerübergreifenden Digitalisierungsprojekten. Gemeinsam mit den anderen Datenschutzaufsichtsbehörden des Bundes und der Länder werden wir den Prozess weiterhin begleiten und die für die OZG-Umsetzung zuständigen Behörden unterstützen.

3. Novellierung des Bundesdatenschutzgesetzes

Der Koalitionsvertrag der Bundesregierung sieht vor, wichtige Änderungen am Bundesdatenschutzgesetz (BDSG) vorzunehmen. Es ist beabsichtigt, die Zusammenarbeit der Datenschutzaufsichtsbehörden künftig enger zu gestalten, damit deutschlandweit eine einheitliche Durchsetzung des Datenschutzrechts gewährleistet ist. Dazu soll die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) institutionalisiert und in die Lage versetzt werden, verbindliche Beschlüsse zu fassen.

Bereits zu einem frühen Zeitpunkt haben wir uns am Gesetzgebungsverfahren beteiligt und zum Referentenentwurf zur Änderung des BDSG[210] sowohl im Rahmen der DSK als auch zusammen mit den Datenschutzaufsichtsbehörden der Länder Stellung bezogen. Die Stellungnahme der DSK[211] begrüßt in weiten Teilen das Gesetzgebungsvorhaben. Der DSK ist es wichtig, gesetzlich als Institution anerkannt zu werden. Um ihrer Aufgabe umfänglich gerecht werden zu können, bedarf es allerdings der bislang im Entwurf nicht vorgesehenen Einrichtung einer ständigen Geschäftsstelle.[212]

Das Gesetzgebungsvorhaben zur Novellierung des BDSG ist zu begrüßen, da es mit der Institutionalisierung der DSK einen wichtigen Beitrag dazu leistet,

[210]BMI, Referentenentwurf zum Ersten Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29. August 2023, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetzestexte/gesetzesentwuerfe/entwurf_aendG_bdsg.html.

[211]DSK, Stellungnahme zum Entwurf eines Ersten Gesetzes zur Änderung des Bundes-daten-schutzgesetzes (Stand: 9. August 2023) vom 6. September 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/st/23_09_06_DSK_Stellungnahme_BDSG.pdf.

[212]Ebd., S. 3.

dass die Datenschutzregelungen in Deutschland kohärent umgesetzt werden können.

4. Entwurf eines Gesundheitsdatennutzungsgesetzes

Das Bundesministerium für Gesundheit (BMG) hat im August dieses Jahres einen Referentenentwurf für ein Gesetz zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz, GDNG) vorgelegt. Im Vordergrund steht dabei die Verarbeitung von Gesundheitsdaten in der elektronischen Patientenakte zu Forschungszwecken. Die DSK hat zu den kritischen Punkten des Gesetzes Stellung genommen,[213] kurz zuvor haben bereits die Datenschutzaufsichtsbehörden der Länder eine gemeinsame Stellungnahme veröffentlicht.[214] Im Rahmen der von der DSK eingesetzten „Taskforce Forschungsdaten" waren wir an der Ausarbeitung der Stellungnahme beteiligt.

Die Pläne für das GDNG sehen Neuregelungen mit dem Schwerpunkt der Verarbeitung von Gesundheitsdaten zu Forschungszwecken vor, die die Nutzung von Daten innerhalb des Gesundheitssystems verbessern und die Verknüpfung von Gesundheitsdaten erleichtern sollen. Es ist beabsichtigt, durch das GDNG

- die Verknüpfung der Daten des beim Bundesinstitut für Arzneimittel und Medizin-produkte (BfArM) angesiedelten Forschungsdatenzentrums Gesundheit mit den Daten der klinischen Krebsregister zu regeln, ebenso wie
- die Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, Patientensicherheit und zu Forschungszwecken,
- die automatisierte Datenverarbeitung durch die Kranken- und Pflegekassen zu Zwecken des Gesundheitsschutzes mit Option zur individuellen Ansprache der Versicherten sowie
- eine Opt-out-Möglichkeit für die automatisierte Übermittlung und Nutzung der Daten aus der elektronischen Patientenakte an das Forschungsdatenzentrum.[215]

[213] DSK, Stellungnahme zum Referentenentwurf des Bundesministeriums für Gesundheit – Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten vom 14. August 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf.

[214] Siehe Unabhängige Datenschutzaufsichtsbehörden der Länder, Stellungnahme zu Artikel 5 des Referentenentwurfs eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten vom 10. August 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/st/23_08_10_Datenschutzaufsicht-Laender-zu-Art_5_GDNG-E.pdf.

[215] Siehe Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten in der Fassung des Kabinetts vom 30. August 2023, abrufbar unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/G/GDNG_Kabinett.pdf.

Das Forschungsdatenzentrum hat u. a. die Aufgabe, die beispielsweise von den Kranken-kassen übermittelten Daten aufzubereiten und Nutzungsberechtigten, wie etwa Wissenschaftler:innen, auf Antrag zur Verfügung zu stellen. Durch die Opt-out--Möglichkeit soll den Versicherten das Recht erhalten bleiben, einer automatisierten Übermittlung der Daten zu widersprechen. Hierzu ist es vorgesehen, in der elektronischen Patientenakte ein sog. Datencockpit einzurichten, in dem Versicherte ihren Widerspruch erklären und darüber hinaus alle bislang ausgeleiteten Daten sowie ihre bereits erklärten Widersprüche einsehen können.

Die DSK hat in ihrer Stellungnahme auf noch bestehende Defizite des geplanten GDNG hingewiesen und konkrete Änderungsvorschläge unterbreitet. Vor dem Hinter-grund des hohen Schutzbedarfs der Daten, deren Verarbeitung Gegenstand des GDNG ist, müssen im Gesetz selbst Maßnahmen und Garantien für ein hohes Vertrauensniveau getroffen werden, die informierte Entscheidungen der betroffenen Personen in dem jeweiligen Verarbeitungszusammenhang unter Wahrung der Sicherheitsanforderungen gewährleisten. Dem wird der Entwurf des GDNG an vielen Stellen nicht gerecht. So ist etwa die vorgesehene undifferenzierte Opt-out-Regelung zur Weiterleitung von Daten aus der elektronischen Patientenakte an das Forschungsdatenzentrum problematisch, insbesondere wenn Zwecke verfolgt werden, die wissenschaftlicher Forschung im Gemeinwohlinteresse nicht unterliegen. Auch die persönliche Ansprache der Versicherten in Form einer unverbindlichen Unterrichtung über Gesundheitsgefährdungen und Verdachtsdiagnosen durch die Kranken- und Pflegekassen ist datenschutzrechtlich in hohem Maß risikobehaftet und mit dem Recht auf Nichtwissen als ein Bestandteil des Rechts auf informationelle Selbstbestimmung nicht vereinbar.

In den früheren Entwürfen des GDNG war zudem eine Änderung von § 9 BDSG vorgesehen, die dem BfDI alleinige Zuständigkeiten über Bereiche zugewiesen hätte, für die bislang (auch) die Datenaufsichtsbehörden der Länder zuständig sind. In einer gemeinsamen Stellungnahme der Landesaufsichtsbehörden wurden die zahlreichen Bedenken verfassungs- sowie datenschutzrechtlicher Art vorgetragen, die mit einer solchen Zuständigkeitsverlagerung einhergegangen wären. Dies hätte insbesondere eine Übertragung der Datenschutzaufsicht über Stellen bedeutet, die gesundheitsbezogene Sozialdaten verarbeiten (etwa Jugendämter oder Sozialämter) und öffentliche Stellen der Länder und nicht des Bundes sind. Wir begrüßen, dass

in die zuletzt vorliegende Kabinettsfassung des Gesetzesentwurfs die Änderung des § 9 BDSG nicht mehr aufgenommen worden ist.

Gesetze, die einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung mit sich bringen, insbesondere wenn Gesundheitsdaten verarbeitet werden, müssen sich mit den datenschutzrechtlichen Anforderungen auseinandersetzen und erkennen lassen, wie die Verhältnismäßigkeit der Eingriffe in die Datenschutzrechte begründet und durch begleitende Maßnahmen sichergestellt wird. Nur wenn die Rechte und Freiheiten der betroffenen Personen im Gesetz ausreichend geschützt werden, kann eine Digitalisierung des Gesundheitswesens mit einer weiter gehenden Nutzung von Gesundheitsdaten gelingen und das erforderliche Vertrauen der Menschen geschaffen werden. Wir werden das weitere Gesetzgebungsverfahren und die Umsetzung in die Praxis begleiten.

5. Aufsichtszuständigkeit über Kirchen und religiöse Vereinigungen

Die Bestandsschutzregelung in Art. 91 DSGVO nimmt Kirchen und religiöse Vereinigungen unter gewissen Voraussetzungen vom Wirkungsbereich der DSGVO und der Zuständigkeit der staatlichen Aufsichtsbehörden aus, sofern sie ihre Datenschutzregelungen rechtzeitig an die DSGVO angepasst haben. In der Bundesrepublik gilt dies für die Vertreter:innen der römisch-katholischen Kirche und die Adressat:innen des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz), die sich auf die durch Art. 91 DSGVO ermöglichte Privilegierung stützen können.[216] Nicht alle Religionsgemeinschaften erfüllen allerdings die Voraussetzungen von Art. 91 DSGVO. Sind diese Religionsgemeinschaften als Körperschaften des öffentlichen Rechts anerkannt, so führt die sodann uneingeschränkt anzuwendende DSGVO zu rechtlichen Folgefragen, deren abschließende Klärung wir anstreben.

Regelmäßig erhalten wir Beschwerden von Betroffenen, die sich auf die unerwünschte Verarbeitung ihrer personenbezogenen Daten durch Religionsgemeinschaften beziehen. Häufig handelt es sich um Personen, die sich wegen Datenschutzverstößen etwa im Zusammenhang mit oder nach dem Austritt aus der Glaubensgemeinschaft an uns wenden. Die Religionsgemeinschaften verweisen dann oft pauschal auf ihren Status

[216] Siehe DSK, Beschluss vom 12. August 2019 zu spezifischen Aufsichtsbehörden, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/20190812_dsk_spezifische.pdf.

als Körperschaften des öffentlichen Rechts[217] und Art. 91 DSGVO. Hier ist jedoch eine genaue Prüfung erforderlich, ob die Voraussetzungen dieser Norm tatsächlich erfüllt sind. Nur für den Fall, dass die Religionsgemeinschaft umfassende Datenschutzregelungen i. S. d. Art. 91 Abs. 1 DSGVO anwendet, kann sie einer spezifischen Datenschutzaufsicht, die natürlich die Bedingungen in Kapitel VI der DSGVO erfüllen muss, unterliegen.

Nicht übersehen werden darf dabei, dass Art. 91 Abs. 1 DSGVO zwei zu unterscheidende Voraussetzungen formuliert und diese an klare zeitliche Vorgaben knüpft: Die jeweilige Religionsgemeinschaft muss umfassende Datenschutzregeln bereits „zum Zeitpunkt des Inkrafttretens“ der DSGVO angewendet haben und sie muss diese sodann mit der DSGVO in Einklang gebracht haben. Als Stichtag zur Anwendung umfassender Datenschutzregelungen war der 25. Mai 2016 als Tag des Inkrafttretens festgelegt.[218] Hat eine Religionsgemeinschaft dagegen erst nach diesem Stichtag, etwa kurz vor dem Wirksamwerden der DSGVO am 25. Mai 2018, umfassende Datenschutzregelungen geschaffen oder aber erst eingeführt, so ist diese formale Voraussetzung des Art. 91 Abs. 1 DSGVO nicht erfüllt.

Kann sich eine Religionsgemeinschaft nicht auf Art. 91 DSGVO berufen und sind die Regelungen der DSGVO folglich ohne spezifische Datenschutzaufsicht anzuwenden, gilt die Zuständigkeit der staatlichen Aufsichtsbehörden. Daran ändert auch der Status einer Religionsgemeinschaft als Körperschaft des öffentlichen Rechts grundsätzlich nichts. Abschließend zu klären ist in diesen Fällen jedoch, ob Religionsgemeinschaften, die den Körperschaftsstatus erlangt haben, als öffentliche oder nicht-öffentliche Stellen einzuordnen sind. Vor dem Hintergrund aktueller Rechtsprechung gehen wir davon aus, dass solche Organisationen den nicht-öffentlichen Stellen gleichzustellen sind, sodass die entsprechenden Zuständigkeitsregelungen der Landesdatenschutzgesetze Anwendung finden können.[219] Für diese Fälle sollten eindeutige Zuständigkeitsregelun-

[217]Religionsgemeinschaften können in Deutschland nach Art. 140 Grundgesetz (GG) i. V. m. Art. 137 Abs. 5 Satz 2 Weimarer Reichsverfassung (WRV) die Rechte einer Körperschaft des öffentlichen Rechts gewährt werden.

[218]Die DSGVO trat nach der Regelung des Art. 99 Abs. 1 DSGVO am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

[219]Siehe Verwaltungsgericht (VG) Hannover, Urteil vom 30. November 2022, 10 A 1195/21, Rn. 54; hier wird eine unionsrechtskonforme Auslegung der einschlägigen Zuständigkeits-normen vorgenommen.

gen in die Landesdatenschutzgesetze aufgenommen oder eine Klarstellung im Bundesdatenschutzgesetz erreicht werden.[220]

Religionsgemeinschaften, die in Deutschland als Körperschaften des öffentlichen Rechts anerkannt sind, können sich nicht pauschal auf Art. 91 DSGVO berufen. Regelmäßig kommt es auf den Zeitpunkt an, zu dem die Religionsgemeinschaft umfassende Datenschutzregeln angewendet hat. Sofern dies bereits vor dem Inkrafttreten der DSGVO der Fall war, können die Religionsgemeinschaften auch einer spezifischen Datenschutzaufsicht unterliegen. Andernfalls gilt die Zuständigkeit der staatlichen Datenschutzaufsicht. Für diese Fälle sollten eindeutige Zuständigkeitsregelungen in die Landesdatenschutzgesetze bzw. eine Zuweisung als nicht-öffentliche Stelle im Bundesdatenschutzgesetz aufgenommen werden.

II. Mitgestaltung der Datenschutz- und Informationsfreiheitskonferenz

1. Ergebnisse der Datenschutzkonferenz

Unter dem Vorsitz der Landesbeauftragten für Datenschutz Schleswig-Holstein (LfD SH) hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in diesem Jahr zahlreiche Entschließungen und Beschlüsse zu aktuellen datenschutzrechtlichen Themen gefasst.

Dabei hat sie sich u. a. zum Beschäftigtendatenschutz und zur automatisierten Datenanalyse bei Polizei und Nachrichtendiensten positioniert. Die Diskussionen während der Konferenzen waren darüber hinaus von Themen wie Künstliche Intelligenz (KI), Scoring, verschiedene Gesetzgebungsverfahren auf europäischer Ebene sowie der Institutionalisierung der DSK geprägt. Außerdem war die Gewährleistung eines hohen Datenschutzniveaus bei der medizinischen Forschung ein wichtiges Thema. Hierzu hat die DSK zwei Entschließungen verabschiedet: eine zur Stärkung des Datenschutzes in der Forschung und eine zu den Rahmenbedingungen für die gesetzliche Regulierung medizinischer Register. Auch außerhalb der regulären Konferenzen hat die DSK zu vielen datenschutzrechtlich relevanten Themen Stellung genommen. Beispiele dafür sind ihre Positionierung zum Targeting bei politischer

[220] Siehe Stellungnahme der DSK vom 12. April 2024 zum Gesetzesentwurf der Bundesregierung: Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/st/240412_BDSG-E_Stellungnahme_DSK.pdf.

Wahlwerbung oder ihre Entschließung zur geplanten Chatkontrolle.[221]

Die Datenschutzkonferenz arbeitet kontinuierlich an Orientierungshilfen, Stellungnahmen und Entschließungen, um mit gemeinsamen Positionen auf die Einhaltung des Datenschutzes in Deutschland und in Europa hinzuwirken.

2. Ergebnisse der Informationsfreiheitskonferenz

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) hat in -diesem Jahr unter dem Vorsitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) vier Entschließungen gefasst.

Mit einer Entschließung fordert die IFK ein zeitgemäßes Bundespressegesetz.[222] Hintergrund dafür ist, dass der Bund im Gegensatz zu den Ländern nicht über ein Pressegesetz verfügt. Der presserechtliche Auskunftsanspruch gegenüber Bundesbehörden ergibt sich stattdessen unmittelbar aus dem Recht auf Pressefreiheit, wie es im Grundgesetz (GG) festgehalten ist.[223] Obwohl das Bundesverwaltungsgericht (BVerwG) den Bundesgesetzgeber bereits 2013 aufgefordert hat, einen darüber hinausgehenden gesetzlichen Informationszugang zu regeln, lässt ein konkreter Gesetzesentwurf für ein modernes Bundespressegesetz weiter auf sich warten. Ein alleiniger Rückgriff auf das Informationsfreiheitsgesetz des Bundes (IFG) wird der grundgesetzlich garantierten besonderen Stellung der Medien nicht gerecht.

In einer weiteren Entschließung fordert die IFK ein einheitlich hohes Transparenzniveau in Bund und Ländern.[224] Während es in Bayern und in Niedersachsen noch immer keinen gesetzlich normierten, allgemeinen und voraussetzungslosen Zugang zu amtlichen Informationen gibt, bestehen in einigen Bundesländern bereits Transparenzgesetze mit umfassenden Pflichten zur proaktiven Veröffentlichung von Information in eigens dafür angelegten Transparenzportalen. Wiederum andere Bundesländer haben Informationsfreiheitsge-

[221]DSK, Entschließungen 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/entschliessungen.html; DSK, Beschlüsse 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/beschluesse-dsk.html.
[222]IFK, Die Demokratie braucht starke Medien – Bundespressegesetz jetzt einführen!, Entschließung vom 14. Juni 2023, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/IFK/2023/44-IFK-Entschliessung_Bundespressegesetz.pdf.
[223]Art. 5 Abs. 1 Satz 2 GG.
[224]IFK, Moderne Transparenzgesetze bundesweit – für eine lebendige Demokratie!, Entschließung vom 7. November 2023, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/IFK/2023/45-IFK_Entschliessung_Transparenzgesetze.pdf.

setze, die den Informationszugang nur auf Antrag gewähren. Vor diesem Hintergrund fordert die IFK die Abschaffung der bestehenden „Drei-Klassen-Gesellschaft“[225] zugunsten weitreichender Transparenzgesetze.

Mit einer dritten Entschließung trägt die IFK der Tatsache Rechnung, dass die Künstliche Intelligenz (KI) auf dem digitalen Vormarsch ist und vermehrt im Alltag eingesetzt wird.[226] Die IFK erkennt in ihr ein effektives Instrument zur schnellen Informationsbereitstellung durch öffentliche Stellen, sofern bestimmte Anforderungen beachtet werden, mit denen etwa die Überprüfbarkeit der technisch-organisatorischen Gestaltung und die Einhaltung datenschutzrechtlicher Vorgaben beim Einsatz von KI gewährleistet sind.

Die vierte Entschließung betrifft die Forderung nach proaktiver Veröffentlichung von Umweltinformationen in Deutschland.[227] In den meisten Gesetzen fehlt ein selbstständig einklagbarer Anspruch der Menschen auf eine Veröffentlichungspflicht von Umweltinformationen. Das muss sich aus Sicht der Informationsfreiheitsbeauftragten dringend ändern. Die IFK fordert daher die bisher untätigen Gesetzgeber auf, die Verpflichtung zur Unterrichtung der Öffentlichkeit zu modernisieren und als selbstständigen gesetzlichen Anspruch zu formulieren.

Alle vier in diesem Jahr verabschiedeten Entschließungen der IFK zielen auf eine Beschleunigung bei der Umsetzung der staatlichen Transparenzpflichten. Das Recht auf allgemeinen und voraussetzungslosen Zugang zu Informationen muss von staatlicher Seite deutschlandweit einheitlich geregelt und proaktiv umgesetzt werden. Dies ermöglicht nicht nur die Teilhabe und Mitnahme aller in Deutschland lebenden Menschen, sondern hilft insbesondere auch den Behörden und öffentlichen Stellen selbst, ihren Aufgaben anhand eindeutiger gesetzlicher Regelungen nachzukommen.

3. DSK-Beschluss zu Abo-Modellen

Zunehmend finden auf Websites Trackingtechnologien sog. Abo- bzw. Pay-or-Okay-Modelle Verwendung.

[225]Ebd., S. 1.

[226]IFK, Künstliche Intelligenz (KI) verantwortungsvoll für die Informationsbereitstellung nutzen!, Entschließung vom 7. November 2023, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/IFK/2023/45-IFK_Entschliessung_Kuenstliche-Intelligenz.pdf.

[227]IFK, 25 Jahre Århus-Konvention – Veröffentlichungsanspruch muss ins Gesetz!, Entschließung vom 7. November 2023, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/IFK/2023/45-IFK_Entschliessung_Arhus-Konvention.pdf.

Aus diesem Grund hat die DSK einen Beschluss gefasst, der die gesetzlichen Bedingungen an diese Modelle herausstellt.

Bei Abo- oder Pay-or-Okay-Modellen können Nutzer:innen zwischen zwei in einem Banner angebotenen Möglichkeiten wählen, um Zugang zu den Websites zu erhalten. Mit der einen Möglichkeit stimmen sie zu, dass Daten zu ihrem Website-Verhalten erhoben und zur Profilbildung sowie zur Bereitstellung personalisierter Werbung verwendet werden. Mit der anderen Möglichkeit schließen sie ein kostenpflichtiges Abonnement ab, bei dem sie dafür bezahlen, dass kein Tracking erfolgt und ihre Daten nicht weiter-verarbeitet werden. Im Beschluss der DSK vom März dieses Jahres sind die datenschutzrechtlichen Bedingungen für dieses Modell formuliert.[228]

Die Einwilligung in das Tracking ist nur wirksam, wenn die Voraussetzung der Frei-willigkeit durch die mögliche Wahl einer Alternative erfüllt ist und zwischen voneinander abweichenden Zwecken der Datenverarbeitung gewählt werden kann. Zusätzlich müssen die Bedingungen der DSGVO für Einwilligungen in Bezug auf Information, Transparenz, Verständlichkeit und Granularität eingehalten werden.[229]

Auch im Onlinebereich sind die Anforderungen der DSGVO an eine wirksame Einwilligung zu erfüllen. Nutzer:innen muss eine gleichwertige Wahlmöglichkeit zur Verfügung stehen, mit der sie die Einwilligung annehmen oder ablehnen können. Bezieht sich eine Einwilligung auf unterschiedliche Zwecke der Verarbeitung personenbezogener Daten in einer Erklärung, ist dies unzulässig. Nutzer:innen müssen die jeweiligen Zwecke einzeln und aktiv auswählen können, damit die Einwilligung auf freiwilliger Basis erfolgt.

III. Zusammenarbeit mit deutschen Datenschutzaufsichtsbehörden

1. Anforderungen an digitale Gesundheitsanwendungen

In diesem Jahr wurden einige Sicherheitslücken aufgedeckt, die bei Digitalen Gesundheitsanwendungen (DiGA)[230] wie etwa Gesundheits-Apps bestehen, die von Ärzt:innen verordnet und von gesetzlichen Kran-

[228]DSK, Bewertung von Pur-Abo-Modellen auf Websites vom 29. März 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf.
[229]Siehe ergänzend auch DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien (Version 1.1) vom 5. Dezember 2022, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf.
[230]Siehe § 139e Abs. 1 Sozialgesetzbuch Fünftes Buch (SGB V).

kenkassen erstattet werden. Sicherheitsmängel und fehlende Datenschutzkonformität bergen die Gefahr, dass besonders schützenswerte Gesundheitsdaten von Patient:innen unbefugt offenbart oder unrechtmäßig verarbeitet werden.

DiGA können bei der Erkennung, Beobachtung und Behandlung von Krankheiten oder Behinderungen helfen und zu einer selbstbestimmten gesundheitsförderlichen Lebensführung beitragen. Die derzeitige gesetzliche Regelung[231] sieht vor, dass die Herstellerfirmen in einer Selbsterklärung[232] nachzuweisen haben, ob die DiGA die datenschutzrechtlichen Anforderungen erfüllen. Im Einvernehmen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde 2021 das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) beauftragt,[233] Prüfkriterien zu erarbeiten, um künftig eine externe Zertifizierung nach Art. 42 Datenschutz-Grundverordnung (DSGVO) zu ermöglichen. Zum 1. August 2024 soll daher das bisherige Verfahren der Selbsterklärung abgelöst und durch das Nachweisverfahren unter Verwendung des Zertifikats geführt werden.

Das BfArM weist die Herstellerfirmen, die einen Antrag auf Aufnahme in das DiGA-Verzeichnis stellen, bereits jetzt auf die im August 2022 veröffentlichten Prüfkriterien[234] hin. Damit auch diejenigen Anwendungen, die bereits jetzt im Verzeichnis des BfArM eingetragen sind, einen hohen Schutz der Gesundheitsdaten der Patient:innen gewährleisten, sollen die Herstellerfirmen von DiGA auf die Prüfkriterien aufmerksam gemacht werden. Dafür haben wir als Vorsitz des Arbeitskreises „Gesundheit und Soziales“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der -Länder (DSK), den wir seit diesem Jahr gemeinsam mit der Sächsischen Datenschutz- und Transparenzbeauftragten (SDTB) führen, ein Schreiben erarbeitet. Dieses wurde über die zuständigen Aufsichtsbehörden den betreffenden Herstellerfirmen und -verbänden übermittelt. Auch die in Berlin ansässigen Herstellerfirmen von DiGA haben dieses Schreiben von uns erhalten. Wir haben ihnen mitgeteilt, dass die Anpassungen, die zur Erfüllung der Prüfkriterien erforderlich sind, bereits vor der Nachweispflicht ab August

[231] Siehe § 139e Abs. 2 Satz 2 Nr. 2 SGB V.
[232] Anlage 1 zur Digitale Gesundheitsanwendungen-Verordnung (DiGAV).
[233] Grund für den Auftrag war die Neuregelung des § 139e Abs. 11 SGB V.
[234] BfArM, Prüfkriterien für die von digitalen Gesundheitsanwendungen (DiGA) und digitalen Pflegeanwendungen (DiPA) nachzuweisenden Anforderungen an den Datenschutz (Version 1.0) vom 9. August 2022, abrufbar unter https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/diga-dipa-datenschutzkriterien.html.

2024 vorgenommen und die DiGA auf Einhaltung der datenschutzrechtlichen Vorgaben überprüft werden sollten.

Die DSK hat dieses Jahr zudem ein Positionspapier veröffentlicht, das sich auf diejenigen digitalen und insbesondere cloudbasierten Gesundheitsanwendungen bezieht, die nicht dem Anwendungsbereich des SGB V[235] unterfallen und dementsprechend nicht von der Nachweispflicht durch das Prüfzertifikat erfasst sind. Das Positionspapier erläutert die rechtlichen Anforderungen, die die Herstellerfirmen dieser Gesundheitsanwendungen zum Schutz der Patientendaten und zur Einhaltung der datenschutzrechtlichen Vorschriften umzusetzen haben.[236]

Bereits jetzt können Herstellerfirmen die Weichen für eine künftige erfolgreiche Zertifizierung ihrer DiGA stellen, indem sie diese einer kritischen Überprüfung unterziehen und entsprechend den Vorgaben der vom BfArM veröffentlichten Prüfkriterien anpassen. Nur wenn diese eingehalten werden, lässt sich ein zuverlässiger Schutz der Gesundheitsdaten von Patient:innen gewährleisten. Den Herstellerbetrieben von Anwendungen, die nicht dem SGB V unterfallen und damit keine Zertifizierung erhalten können, steht das Positionspapier der DSK zur Umsetzung der datenschutzrechtlichen Vorgaben als Hilfestellung zur Verfügung.

2. Datenauswertung zu Werbezwecken nur mit Einwilligung

Eine Bank beabsichtigte, nahezu alle ihr über die Kund:innen zur Verfügung stehenden Daten für Werbezwecke auszuwerten. Die Bank ging davon aus, dass eine derartige Profilbildung aufgrund ihrer eigenen berechtigten Interessen gerechtfertigt sei. Wir haben klargestellt, dass eine solche umfangreiche Verarbeitung nur auf der Grundlage einer Einwilligung der betroffenen Personen erfolgen kann.

Die Bank ist Teil eines Bankenverbands, der den Mitgliedsbanken für dieses Vorgehen einen entsprechenden Vorlagetext für ein Informationsschreiben an die Kund:innen zur Verfügung gestellt hatte. Dieses wurde von Banken aus verschiedenen Bundesländern verwendet. Darin heißt es unter dem Betreff „Verantwortungsvolle Datenverarbeitung“, dass zur Auswertung u. a. Daten aus dem Zahlungsverkehr der Kund:innen sowie

[235] Siehe § 139e Abs. 1 SGB V.

[236] DSK, Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen vom 6. November 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/2023_11_06_Beschluss_cloudbasierte_digitale_Gesundheitsanwendungen.pdf.

aus der Nutzung des Onlineangebots verwendet werden würden. Den Kund:innen wurde im Schreiben ein Widerrufsrecht eingeräumt.

Im Erwägungsgrund (ErwGr.) 47 DSGVO wird festgestellt, dass die Interessen und Grundrechte betroffener Personen insbesondere dann gegenüber den Interessen der Verantwortlichen überwiegen können, wenn die betroffenen Personen vernünftigerweise nicht mit einer weiteren Verarbeitung ihrer Daten rechnen müssen. Kund:innen, die bei ihrer Bank vorrangig Giro- und Sparkonten führen, können grundsätzlich nicht damit rechnen, dass ihre Zahlungsverkehrsdaten und ihr Internetverhalten von ihrer Bank zu Werbezwecken auswertet werden. Daran ändert auch das von der Bank versandte Informationsschreiben nichts. Die Erwartungen der betroffenen Personen können nicht durch die gesetzlichen Pflichtinformationen erweitert werden. Denn die ordnungs-gemäße Erfüllung der Informationspflichten hat keine positive Auswirkung auf die Abwägung der verschiedenen Interessen. Das Schreiben der Bank führt folglich nicht zur Rechtmäßigkeit der Datenverarbeitung. Letztendlich sind die schutzwürdigen Interessen der Betroffenen auch allein schon deshalb höher als die Wirtschaftsinteressen der Bank zu bewerten, da durch die Zahlungsverkehrsdaten sehr genaue Profile über die Betroffenen erstellt werden können. Ebenso sind die Daten zur Nutzung des Onlineangebots schützenswert, da diese persönliche Informationen über die Lebensgewohnheiten der Betroffenen enthalten.

Wir haben zusammen mit anderen deutschen Aufsichtsbehörden den Bankenverband darüber informiert, wie Daten zulässigerweise erhoben werden können, ein Muster für eine Einwilligungserklärung angefordert und Empfehlungen zur Überarbeitung der Einwilligungserklärung ausgesprochen. Dies entbindet die Mitgliedsbanken selbst, die für alle von ihnen durchgeführten Datenverarbeitungen verantwortlich sind, jedoch nicht davon, die Erklärung vor deren Anwendung zu überprüfen.

Zur Auswertung der Daten von Kund:innen zum Zahlungsverkehr und zur Nutzung des Onlineangebots durch eine Bank bedarf es einer rechtlichen Grundlage. Für Werbezwecke dürfen diese Daten regelmäßig nur mit der Einwilligung der Betroffenen verwendet werden.

3. Informationsfreiheit by Design

Zentrales Anliegen unseres Beitrags zum Arbeitskreis der Informationsfreiheitsbeauftragten (AKIF)[237] *war dieses Jahr das Thema „Informationsfreiheit by Design". Gemeinsam mit den Kolleg:innen der anderen Aufsichtsbehörden haben wir in der dafür eingerichteten, von Schleswig-Holstein geleiteten Arbeitsgruppe mögliche Grundlagen einer Umsetzung der Informationsfreiheit auf technisch-organisatorischer Ebene erarbeitet.*

Mit Informationsfreiheit by Design ist die Gesamtheit der aktuellen technischen und organisatorischen Instrumente gemeint, die zur Wahrnehmung und Erfüllung der Rechte nach den gesetzlichen Regelungen zu Informationsfreiheit, Informationszugang und Transparenz eingesetzt werden können. In einem Positionspapier von 2019 stellt die Konferenz der Informationsfreiheitsbeauftragten (IFK) die Zielsetzung der Informationsfreiheit by Design heraus: Sie bezweckt die Erleichterung des Zugangs zu Informationen, indem ihre Anforderungen von Beginn an mitgedacht und in die Gestaltung der Arbeitsprozesse und IT-Systeme der öffentlichen Stellen des Bundes und der Länder eingebunden werden. Konkret geht es dabei um

- die proaktive Veröffentlichung von Information über öffentlich zugängliche Onlineportale,
- die Speicherung von Informationen in elektronischen Datenbanken,
- die Benennung zuständiger Ansprechpersonen,
- die Bereitstellung von Verzeichnissen über verfügbare Informationen,
- die Berücksichtigung einer Kennzeichnung von schutzbedürftigen Informationen durch Dritte und
- die Ermöglichung eines wenigstens beschränkten Informationszugangs, sofern nur teilweise öffentliche oder private Interessen entgegenstehen.[238]

Die von der Arbeitsgruppe in diesem Jahr erarbeiteten Grundlagen bilden die Basis zur Entwicklung möglicher Vorgehensweisen und Maßnahmen, die Behörden und anderen öffentlichen Stellen helfen sollen, das Recht auf Informationszugang in technischer wie organisatorischer Hinsicht umzusetzen.

Informationsfreiheit by Design unterstützt Behörden und andere öffentliche Stellen bei der Umsetzung des

[237]Der AKIF setzt sich aus den Fachreferent:innen der Informationsfreiheitsbeauftragten des Bundes und der Länder zusammen und bereitet Sitzungen und Entschließungen der IFK auf fachlicher Ebene vor.
[238]IFK, Informationszugang in den Behörden erleichtern durch „Informationsfreiheit by Design", Positionspapier vom 12. Juni 2019, S. 2, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/IFK/2019/BlnBDI-2019-IFK-Positionspapier_Informationsfreiheit_by_Design.pdf.

Zugangs zu Informationen. Wird das Ziel der Transparenz von Anfang an bei der Gestaltung von IT-Systemen und der Entwicklung organisatorischer Abläufe berücksichtigt, trägt dies zur Effizienz und Verringerung des Aufwands bei. Es stärkt das Vertrauen der Menschen in die staatliche Verwaltung, wenn diese ihre Handlungsfähigkeit unter Beweis stellt, indem sie proaktiv agiert und das Recht auf Informationszugang von vornherein in ihre Prozesse einbezieht.

4. Anwendung des Standard-Datenschutzmodells

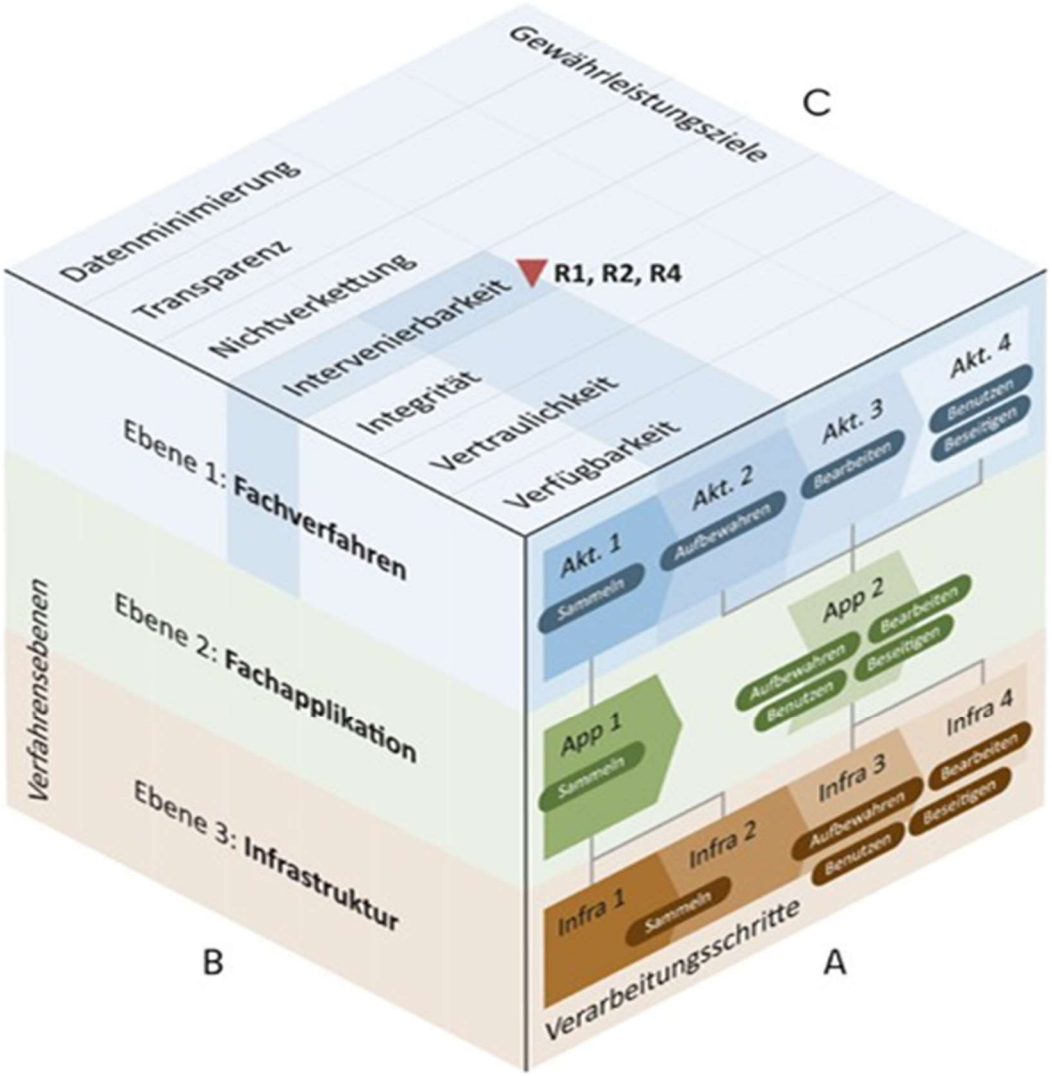
Regelmäßig ist Verantwortlichen und Auftragsverarbeitern nicht klar, was unter der Verarbeitung personenbezogener Daten zu verstehen ist und welche Maßnahmen zu ergreifen sind, um den in der DSGVO geforderten Schutz personenbezogener Daten zu gewährleisten. Die DSK hat daher das Standard-Datenschutzmodell (SDM)[239] publiziert, das eine Methode darstellt, mit der die rechtlichen Anforderungen anhand von sieben Gewährleistungszielen in konkrete technische und organisatorische Maßnahmen übersetzt werden können. Gemeinsam mit anderen deutschen Aufsichtsbehörden haben wir in einer Arbeitsgruppe der DSK das SDM weiterentwickelt und um den sog. SDM-Würfel als Analysetool ergänzt.

Der in Art. 5 Abs. 1 lit. a DSGVO formulierte Grundsatz der Transparenz fordert von Verantwortlichen, die eine Verarbeitung personenbezogener Daten planen oder bereits vornehmen, den von der Verarbeitung betroffenen Personen nachvollziehbar zu beschreiben, welche Daten auf welche Weise zu welchem Zweck und für -welchen Zeitraum verarbeitet werden. Zwar ist der Begriff der Verarbeitung in Art. 4 Nr. 2 DSGVO definiert. Unsere Erfahrungen in der Beratungspraxis zeigen jedoch, dass Verantwortliche immer wieder Schwierigkeiten dabei haben, die Komplexität der Daten-verarbeitungen so zu beschreiben, dass aus der Beschreibung zum einen die Risiken der Verarbeitung und zum anderen die technischen und organisatorischen Maßnahmen hervorgehen, die eingesetzt werden müssen, um diese Risiken zu minimieren.

Aus diesem Grund haben wir mit anderen deutschen Aufsichtsbehörden daran gearbeitet, den SDM-Würfel zu entwickeln, der die Feststellung der Risiken einer Datenverarbeitung visuell erleichtern soll. Der Würfel (siehe Grafik, S. 139) setzt sich aus drei Dimensionen zusammen:

[239] DSK, Das Standard-Datenschutzmodell (SDM), Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 3.0, verabschiedet am 24. November 2022, abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V30a.pdf.

- die Verarbeitungsschritte (A),
- die Verfahrensebenen (B) und
- die Gewährleistungsziele (C).



Die Dimension der Verarbeitungsschritte (A) unterteilt den Prozess der Verarbeitung eines personenbezogenen Datums in einzelne Teilprozesse, die den Verarbeitungsschritten von der Erhebung bis zur Löschung des personenbezogenen Datums entsprechen.

Die Dimension der Verfahrensebenen (B) teilt sich in drei unterschiedliche Ebenen auf: die Prozess- bzw. Fachverfahrensebene, die Fachapplikationsebene und die Infrastrukturebene. Damit können auch die zur Verarbeitung eingesetzten Betriebsmittel in die Risikoana-

lyse einbezogen und mit denjenigen Verarbeitungsschritten verknüpft werden, bei denen sie zum Einsatz kommen.

Die Dimension der Gewährleistungsziele (C) führt die sieben Gewährleistungsziele auf (Datenminimierung, Transparenz, Nichtverkettung, Intervenierbarkeit, Integrität, Vertraulichkeit und Verfügbarkeit), die jeweils davon beeinträchtigt werden können, welches Verfahren für welchen Verarbeitungsschritt gewählt wird.

Um nun festzustellen, welches Verfahren bei welchem Verarbeitungsschritt zu welcher Beeinträchtigung führt, muss in der Dimension der Gewährleistungsziele (C) der Bereich in den Blick genommen werden, an dem sich das gewählte Verfahren mit dem jeweiligen Verarbeitungsschritt kreuzt. Dort, wo sie aufeinandertreffen (rotes Dreieck), befinden sich die spezifischen Risiken (R1, R2, R4), die durch die Beeinträchtigung des jeweiligen Gewährleistungsziels zustande kommen. Dem SDM sowie den bereits veröffentlichten Bausteinen des Maßnahmenkatalogs[240] sind dann die entsprechenden Schutzmaßnahmen zu entnehmen, mit denen den spezifischen Risiken begegnet werden kann.

Der SDM-Würfel eignet sich sowohl für einfache als auch für komplexe Datenverarbeitungen. Er ist insbesondere auch bei Verarbeitungen mit voraussichtlich hohen Risiken hilfreich, bei denen Verantwortliche eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO vornehmen müssen.[241] Für Datenschutzmanagementsysteme kann sich der Würfel als Analysetool anbieten, um Verantwortlichen und Auftragsverarbeitern die Anwendung des SDM zu erleichtern und sie bei der Feststellung der jeweiligen Risiken und der zu ergreifenden Gegenmaßnahmen zu unterstützen.

Die von der länderübergreifenden Arbeitsgruppe erarbeiteten Ergänzungen zum SDM und insbesondere die Einführung des SDM-Würfels als Hilfsmittel zur -Analyse erleichtern Verantwortlichen und Auftragsverarbeitern, die Risiken auch in technisch komplexen Verarbeitungssituationen zu erfassen und angemessene technische und organisatorische Maßnahmen auszuwählen, die die Sicherheit ihrer Datenverarbeitungen

[240] Der vom AK „Technik“ veröffentlichte Katalog führt diejenigen Maßnahmen auf, die sich aus dem SDM ergeben und in die Praxis umgesetzt werden sollten. Dazu werden fortlaufend anwendungsbezogene Bausteine bereitgestellt, die die Umsetzung der Maßnahmen erleichtern sollen; siehe Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV), Standard-Datenschutzmodell, abrufbar unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

[241] Dabei kann u. a. auch die tabellarische Aufschlüsselung der Verarbeitungsschritte hilfreich sein; siehe DSK, Das Standard-Datenschutzmodell (SDM), Version 3.0, S. 38, Abb. 1, abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V30a.pdf.

gewährleisten. Wie viele deutsche Aufsichtsbehörden wenden auch wir das SDM in unseren Beratungen erfolgreich an, um Verantwortlichen und Auftragsverarbeitern die rechtlichen Anforderungen verständlich zu machen und die DSGVO in die Praxis zu überführen.

C. Wir in Europa

I. Gesetzesvorhaben der Europäischen Union

1. Verordnung über die Transparenz und das Targeting politischer Werbung

Die Europäische Kommission hat 2021 eine Verordnung[242] vorgeschlagen, mit der künftig manipulative Wahlwerbung verhindert werden soll. Der Entwurf legt spezifische Regeln zur Verarbeitung personenbezogener Daten fest, die freie demokra-tische Wahlen garantieren sollen. Im November dieses Jahres einigten sich der Rat der Europäischen Union (EU) und das Europäische Parlament auf die Umrisse der neuen Verordnung. Wir haben eine Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zum Vorschlag initiiert.

Freie Informationsgewinnung ist als Voraussetzung für die Meinungsbildung essenziell für demokratische Wahlen. Gezielte Manipulationsversuche, die auf der Verarbeitung von Daten der Wähler:innen und deren Aktivitäten oder Meinungen beruhen, stellen daher eine beträchtliche Gefahr für demokratische Prozesse dar. Gerade auf Onlineplattformen können Nutzer:innen besonders leicht auf ihre Empfänglichkeit für bestimmte Botschaften analysiert werden.

Der derzeitige Verordnungsentwurf[243] sieht daher vor, die Möglichkeiten der Verarbeitung personenbezogener Daten zum Zwecke politischer Werbung grundlegend zu beschränken. Es sollen nur Daten verarbeitet werden dürfen, die direkt bei den Betroffenen erhoben wurden und zu deren Verarbeitung die explizite Einwilligung dieser -Personen vorliegt. Daten, die den besonderen Kategorien personenbezogener Daten[244] angehören und als besonders schützenswert einzustufen

[242]Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung vom 25. November 2021, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52021PC0731.

[243]In diesen sind die vom Europäischen Parlament im Februar eingebrachten Änderungen aufgenommen; siehe Europäisches Parlament, Abänderungen zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung vom 2. Februar 2023, abrufbar unter https://www.europarl.europa.eu/doceo/document/TA-9-2023-0027_DE.html.

[244]Dazu zählen Daten zur Gesundheit, zur sexuellen Orientierung, zur ethnischen Herkunft, zur religiösen Zugehörigkeit und zur politischen Meinung; siehe Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO).

sind, dürften prinzipiell nicht verarbeitet und zur Erstellung von Profilen über einzelne Personen eingesetzt werden. Politische Werbung dürfte dementsprechend nicht mehr selektiv nach Einzelpersonen, sondern nur noch zufällig innerhalb einer potenziellen Zielgruppe angezeigt werden, wobei maximal vier personenbezogene, nicht besonders schützenswerte Datenkategorien zur Bestimmung der Zielgruppe herangezogen werden dürften. Politische Werbung müsse zudem verpflichtend als solche gekennzeichnet sein; dies schließt insbesondere auch die Angabe derjenigen mit ein, in deren Namen und Auftrag die Werbung erstellt wurde.[245]

Der europäische Gesetzgeber reagiert damit auf gezielte Manipulationsversuche, die bei den vergangenen Wahlen auf nationaler wie internationaler Ebene festzustellen waren, indem explizit politische Werbung verschleiert und als redaktionelle Inhalte oder private Postings in sozialen Medien ausgegeben wurde. Damit ließen sich von denselben Parteien unterschiedliche, teils gar widersprüchliche Botschaften ausspielen; je nachdem für welche Botschaften die jeweilige Person oder Personengruppe empfänglich war. Einen zwischenzeitlichen Höhepunkt fand diese Entwicklung im Vorgehen des britisch-US-amerikanischen Datenanalyseunternehmens Cambridge -Analytica. Das Unternehmen hat 2016 für den Wahlkampf um die US-Präsidentschaft sowie zum -Brexit-Referendum die Persönlichkeitsprofile von über 87 Millionen Facebook--Nutzer:innen ausgewertet, um diese per sog. Microtargeting, also durch individuell auf ihr Profil zugeschnittene Botschaften, in ihrem Wahlverhalten zu beeinflussen.

Die von uns initiierte und von der DSK herausgegebene Stellungnahme[246] begrüßt das Vorhaben der Verordnung, betont aber, dass die Einwilligung als zentrale Rechtsgrundlage für den Einsatz zielgerichteter politischer Werbung an ihre Grenzen stoße. Es bedürfe daher der zusätzlichen Regulierung besonders risikobehafteter Verarbeitungen. Die freie Entscheidung über die Verarbeitung der eigenen personenbezogenen Daten müsse gesetzlich so abgesichert werden, dass die Zwecke der Verarbeitung für die betroffenen Personen eindeutig nachvollziehbar seien und die grundrechtlich

[245]Als gemeinsam Verantwortliche sind dementsprechend nicht nur die Herausgeber:innen der politischen Werbung, sondern ebenso diejenigen anzusehen, die die Werbung in Auftrag gegeben und finanziert oder die Auswahl der zu bewerbenden Zielgruppen getroffen haben; siehe Art. 26 Abs. 1 DSGVO und Europäischer Gerichtshof (EuGH), Urteil vom 5. Juni 2018, C-210/16, Rn. 38.

[246]DSK, Datenschutz sichert freie politische Willensbildung, Stellungnahme vom 21. Juni 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/st/23-06-21_DSK-Stellungnahme_Politisches-Targeting.pdf.

verankerte Einwilligung[247] vollumfänglich als Instrument der informationellen Selbstbestimmung zum Tragen komme.

Die Erhebung personenbezogener Daten durch Websites und Plattformen ermöglicht eine umfassende Profilbildung von einzelnen Nutzer:innen und Personengruppen sowie ihre Empfänglichkeit für bestimmte Botschaften. Insbesondere im Hinblick auf demokratische Wahlen und Abstimmungen ist das Risiko der gezielten Fehlinformation und Manipulation von Wähler:innen daher entsprechend hoch. Dem Datenschutz kommt an dieser Stelle eine Schlüsselrolle zu: Nur die rechtmäßige, faire und transparente Verarbeitung der personenbezogenen Daten potenzieller Wähler:-innen ermöglicht die freie Informationsgewinnung ohne gezielte Manipulation einzelner Personen oder Personengruppen. Effektiver Datenschutz ist daher unerlässlich für die Sicherung eines freien politischen Meinungsbildungsprozesses und die Basis dafür, dass andere Grundrechte überhaupt erst ausgeübt werden können.

2. Einführung des Digitalen Euro als gesetzliches Zahlungsmittel

Die Europäische Zentralbank (EZB) beabsichtigt, eine digitale Zentralbankwährung als gesetzliches Zahlungsmittel einzuführen und den EU-Bürger:innen als elektronische Form von Bargeld zur Verfügung zu stellen. Die Europäische Kommission hat dafür im Juni dieses Jahres einen Gesetzgebungsvorschlag vorgelegt, der den rechtlichen Rahmen für die Einführung schaffen soll. Zusammen mit dem Europäischen Datenschutzausschuss (EDSA), dem Europäischen Datenschutzbeauftragten (EDSB) und anderen europäischen Aufsichtsbehörden haben wir eine Stellungnahme[248] erarbeitet, die auf die datenschutzrechtlichen Anforderungen an einen solchen Digitalen Euro hinweist.

Der Digitale Euro soll als gesetzliches und von der EZB garantiertes zusätzliches Zahlungsmittel eingeführt werden. Die technischen Details, insbesondere zu dessen Nutzung im Alltag wie auch zu den damit verbundenen Verarbeitungen personen-bezogener Daten durch Händler:innen, Geschäftsbanken, Zahlungsdienstleister:innen, nationale Zentralbanken und die EZB, sind noch nicht abschließend geklärt. Vorgesehen ist bislang jedoch, dass der Digitale Euro sowohl in einer Online- als auch in einer Offline-Variante nutzbar

[247] Siehe Art. 8 Abs. 2 Satz 1 Charta der Grundrechte der Europäischen Union (GRCh).
[248] EDSA und EDSB, Gemeinsame Stellungnahme 2/2023 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einführung des digitalen Euro vom 17. Oktober 2023, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-022023-proposal_de.

sein soll.[249] Bei der Offline-Variante sollen Transaktionen auch ohne Anbindung an eine zentrale Infrastruktur vorgenommen und die offengelegten personenbezogenen Daten auf ein Minimum reduziert werden. Dabei würde Geld digital von einem Konto abgebucht und in eine Art virtuelles Portemonnaie eingezahlt werden können, mit dem sich beispielsweise per Smartphone bezahlen lässt. Damit soll der Digitale Euro bargeldähnlich nutzbar sein.

In der Stellungnahme des EDSA und des EDSB, an der wir mitgearbeitet haben, wird vor allem die Pflicht zur Wahrung der Vertraulichkeit herausgestellt. Die Nutzung digitaler Zahlmethoden hinterlässt Datenspuren. Informationen über die gesamte Palette durchgeführter Zahlungen eignen sich besonders gut, aussagekräftige Profile über Personen zu bilden. Auch besonders schützenswerte Daten wie Gesundheits- und Aufenthaltsdaten oder Daten zur Mediennutzung lassen sich aus den Zahlungsdaten ablesen. Aus diesem Grund sind bei der Ausgestaltung des Digitalen Euro als gesetzliches Zahlungsmittel besonders hohe Anforderungen an die Einhaltung der datenschutzrechtlichen Vorschriften zu stellen. Wir werden weiter darauf hinwirken, dass die Nutzung des Digitalen Euro unter möglichst geringer Verarbeitung personenbezogener Daten erfolgt.

Das Zahlungs- und Konsumverhalten von Personen, sofern es nachverfolgt werden kann, ermöglicht die Bildung aussagekräftiger Profile. Die Beibehaltung anonymer Zahlarten ist daher bei der Einführung einer offiziellen digitalen Zentralbank-währung von größter Relevanz. Gleichzeitig müssen alle Anstrengungen unternommen werden, damit die Nutzung des Digitalen Euro mit einem Minimum an verarbeiteten personenbezogenen Daten auskommt bzw. dass weitestgehend anonyme Nutzungsmöglichkeiten erarbeitet werden.

3. Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework

Am 10. Juli dieses Jahres hat die EU-Kommission einen neuen Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework (DPF) angenommen. Sie kommt damit zu der Einschätzung, dass in den USA für das DPF und unter Berücksichtigung der Executive Order 14086 des US-Präsidenten ein angemessenes Schutzniveau für bestimmte Übermittlungen personenbezogener Daten besteht. Übermittlungen an selbstzertifizierte US-Empfänger:innen können damit wieder

[249] EZB, Häufig gestellte Fragen zum digitalen Euro, 18. Oktober 2023, abrufbar unter https://www.ecb.europa.eu/paym/digital_euro/faqs/html/ecb.faq_digital_euro.de.html.

auf Grundlage eines Angemessenheitsbeschlusses erfolgen.

Nachdem der EuGH 2020 den Angemessenheitsbeschluss für das sog. EU-U.S. Privacy Shield für ungültig erklärte,[250] besteht nach drei Jahren inzwischen wieder eine Möglichkeit, personenbezogene Daten auf Grundlage eines Angemessenheitsbeschlusses[251] in die USA zu übermitteln. Sofern eine Rechtsgrundlage[252] für die Verarbeitung vorliegt, können personenbezogene Daten an unter dem DPF selbstzertifizierte US-Empfänger:innen nun wieder ohne weitere Übermittlungsinstrumente nach den Artikeln 46 oder 49 DSGVO übermittelt werden.

Voraussetzung hierfür ist eine Zertifizierung der empfangenden Stelle nach dem DPF. Dafür müssen die empfangenden Stellen den Ermittlungs- und Durchsetzungsbefugnissen der US-amerikanischen Wettbewerbs- und Verbraucherschutzbehörde (Federal Trade Commission, FTC) oder des US-Verkehrsministeriums (Department of Transportation, DOT) unterliegen. Eine Liste selbstzertifizierter Organisationen wird vom US-Handelsministerium (Department of Commerce, DOC) geführt.[253]

Verantwortliche bzw. die in die USA übermittelnden Stellen (Datenexporteure) müssen daher prüfen, ob die jeweils geplanten Übermittlungen in den Anwendungsbereich des Beschlusses fallen und ob die empfangenden US-Organisationen auch unter dem DPF zertifiziert sind.

Zur Klärung der wichtigsten Fragen haben wir auf unserer Website eine Themenseite eingerichtet.[254] Zudem hat die DSK ausführliche Anwendungshinweise[255] erstellt. Darin werden die wesentlichen Inhalte des DPF, die zentralen Vorgaben für Datenexporteure sowie Rechtsschutzmöglichkeiten für Betroffene praxisnah erläutert.

[250]Siehe JB 2020, 1.2.
[251]Siehe Art. 45 DSGVO.
[252]Siehe Art. 6 DSGVO.
[253]Die Liste ist auf der vom US-Handelsministerium eigens zum DPF eingerichteten Website veröffentlicht, abrufbar unter https://www.dataprivacyframework.gov/list.
[254]Siehe https://www.datenschutz-berlin.de/themen/unternehmen/internationaler-datenverkehr/.
[255]DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/
230904_DSK_Ah_EU_US.pdf.

Der EDSA hat den Entwurf für den nun angenommenen Angemessenheitsbeschluss bewertet.[256] Darin weist er auf eine Reihe bereits früher angemahnter und neuer Aspekte hin, die einem ausreichenden Datenschutzniveau in den USA entgegen-stehen könnten. Dies sind beispielsweise Mängel beim Recht auf Auskunft und bei der Weiterübermittlung von Daten aus den USA in andere Drittländer, Ausnahmen von den Schutzvorkehrungen sowie die weiterhin bestehenden US-Überwachungsprogramme und die Wirksamkeit des neu eingeführten Rechtsbehelfsmechanismus.

Unter dem DPF selbstzertifizierte Organisationen verpflichten sich, gewisse Standards und Prinzipien einzuhalten. Außerdem müssen sie wirksame und leicht zugängliche Rechtsbehelfsmechanismen für Betroffene bereitstellen. So können Betroffene bei mehreren Stellen – u. a. direkt bei der US-Organisation oder bei den EU-Datenschutz-aufsichtsbehörden – Beschwerden einreichen.[257] Auch steht es den Betroffenen offen, ein verbindliches Schiedsverfahren anzustrengen. Um die Rechtmäßigkeit eines staatlichen Zugriffs auf Daten durch US-Behörden im Bereich der nationalen Sicherheit zu überprüfen, wurde ein zweistufiger Rechtsbehelfsmechanismus eingeführt.

Übermittlungen außerhalb des Anwendungsbereichs des Angemessenheitsbeschlusses oder an US-Empfänger:innen, die nicht unter dem DPF zertifiziert sind, können dagegen nicht auf den neuen Angemessenheitsbeschluss gestützt werden. Stattdessen sind für entsprechende Übermittlungen – wie bisher auch – andere Übermittlungs-instrumente aus Kapitel V der DSGVO erforderlich.[258] Für die Prüfung der US-Rechtslage und Rechtspraxis kann auf die Bewertung der EU-Kommission aus dem neuen Angemessenheitsbeschluss zurückgegriffen werden.

Mit dem Angemessenheitsbeschluss für das DPF können Übermittlungen an bestimmte, selbstzertifizierte US-Empfänger:innen wieder auf Grundlage eines Angemessenheitsbeschlusses übermittelt werden. Verantwortliche müssen prüfen, ob die geplanten Übermitt-

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

[257]Siehe DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf, Kapitel III.1.

[258]Siehe ebd., Kapitel IV.

lungen in den Anwendungsbereich des Beschlusses fallen und ob die empfangenden US-Organisationen unter dem DPF zertifiziert sind.

II. Mitarbeit im Europäischen Datenschutzausschuss

1. Transparenz und Einheitlichkeit der Bußgeldzumessung

Im Mai dieses Jahres hat der Europäische Datenschutzausschuss (EDSA) die endgültige Fassung seiner Leitlinien zur Bußgeldzumessung verabschiedet.[259] Die Leitlinien setzen einheitliche Maßstäbe, nach denen die europäischen Datenschutzaufsichtsbehörden ihre Bußgelder zu bemessen haben. Damit wird die Sanktionierung von Datenschutzverstößen EU-weit harmonisiert und das Verfahren zur Bemessung der Bußgelder offengelegt. In Vertretung aller deutschen Aufsichtsbehörden haben wir zusammen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) an der Erstellung der Leitlinien mitgewirkt.[260]

Die Leitlinien des EDSA sehen fünf Schritte vor, die zur Bemessung der Bußgelder anzuwenden sind:
Im ersten Schritt werden die Verarbeitungsvorgänge identifiziert und festgestellte Verstöße auf die Anwendbarkeit von Art. 83 Abs. 3 Datenschutz-Grundverordnung (DSGVO) geprüft.

Im zweiten Schritt wird der Ausgangswert für die Bußgeldberechnung anhand der Art und Schwere des jeweiligen Verstoßes sowie des Umsatzes des Unternehmens bestimmt.

Im dritten Schritt wird der berechnete Wert in Bezug auf erschwerende oder mildernde Umstände angepasst, die aufgrund des früheren oder gegenwärtigen Verhaltens des Verantwortlichen oder Auftragsverarbeiters zu berücksichtigen sind.[261]

Im vierten Schritt werden die gesetzlich vorgesehenen Höchstbeträge[262] für die jeweiligen Verstöße identifiziert, die in der Bußgeldbemessung nicht überschritten werden dürfen.

[259] EDSA, Leitlinien 04/2022 für die Berechnung von Geldbußen im Sinne der DSGVO (Version 2.1) vom 24. Mai 2023, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_de.
[260] Siehe auch JB 2022, 15.1.
[261] Art. 83 Abs. 2 DSGVO.
[262] Art. 83 Abs. 4 bis 6 DSGVO.

Im fünften und letzten Schritt ist zu prüfen, ob die berechnete Bußgeldhöhe den Anforderungen von Art. 83 Abs. 1 DSGVO an die Wirksamkeit, Verhältnismäßigkeit und Abschreckungskraft genügt.

Die Leitlinien des EDSA machen das Verfahren der Bußgeldzumessung transparent. Sie stärken die Durchsetzungskraft der europäischen Datenschutzaufsichtsbehörden und stellen die einheitliche Anwendung der DSGVO in der Europäischen Union sicher. Seit ihrer Verabschiedung finden die Leitlinien bei sämtlichen Bußgeldzumessungen unserer Behörde Anwendung.

2. Verbot verhaltensbasierter Werbeaktivitäten durch Meta-Dienste

Der EDSA hat die zuständige irische Datenschutzaufsichtsbehörde (DPC) mit verbindlichem Beschluss verpflichtet, gegenüber dem Unternehmen Meta Platforms -Ireland Ltd. ein Verbot für alle verhaltensbasierten Werbeaktivitäten anzuordnen, die ohne Einwilligung erfolgen. Zuvor hatte der EDSA bereits die Rechtswidrigkeit dieser Verarbeitungen festgestellt. Meta war jedoch der gesetzten Umsetzungsfrist für eine rechtskonforme Datenverarbeitung nicht nachgekommen.

Auf Antrag der norwegischen Datenschutzaufsichtsbehörde Datatilsynet verabschiedete der EDSA am 27. Oktober dieses Jahres in einem Ad-hoc-Plenum einen verbindlichen Beschluss im Dringlichkeitsverfahren.[263] Darin wird die DPC verpflichtet, gegenüber Meta ein Verarbeitungsverbot für alle verhaltensbasierten Werbeaktivitäten auszusprechen, die auf Grundlage berechtigter Interessen oder eines Vertrags mit den Nutzer:innen[264] erfolgen.[265] Über die EDSA-Expertengruppe „Strategic Advisory“ waren wir an diesem Verfahren beteiligt.

Bereits im Dezember des Jahres 2022 stellte der EDSA mit zwei verbindlichen Beschlüssen die Rechtswidrigkeit der Verarbeitungen zum Zwecke verhaltensbasierter Werbung durch Meta fest. Nachdem Meta die Verstöße nach Ablauf der damals gesetzten Umsetzungsfrist nicht behoben und die DPC als federführende Aufsichtsbehörde keine Zwangsmaßnahmen zur Durchsetzung des Beschlusses eingeleitet hatte, verhängte die norwegische Aufsichtsbehörde im Rahmen einer einstweiligen Maßnahme – zunächst nur für das eigene Land – ein dreimonatiges Verarbeitungsverbot für

[263] Siehe Art. 66 Abs. 2 DSGVO.
[264] Siehe Art. 6 Abs. 1 Satz 1 lit. f, Art. 6 Abs. 1 Satz 1 lit. b DSGVO.
[265] EDSA, Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR) vom 27. Oktober 2023, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_en.

diese Verarbeitungen. Das Verbot wurde von einem Osloer Gericht zwischenzeitlich bestätigt.[266] Um das Verbot auch nach Ablauf der drei Monate beizubehalten und alle im Europäischen Wirtschaftsraum (EWR) von der Verarbeitung betroffenen Nutzer:innen zu schützen, beantragte Norwegen im Verfahren vor dem EDSA die Bestätigung und Ausweitung dieses Verarbeitungsverbots für den gesamten EWR.

Gemeinsam mit den anderen deutschen Aufsichtsbehörden unterstützten wir den Antrag und konnten zusammen mit Norwegen weitere Mitgliedstaaten für diese Maßnahme gewinnen, weshalb sich eine Mehrheit für die Bestätigung und Ausweitung des Verbots aussprach. Aufgrund des verbindlichen Beschlusses des EDSA vom 27. Oktober wurde die DPC verpflichtet, innerhalb von zwei Wochen einen nationalen Bescheid zu erlassen, der Meta die Datenverarbeitung zum Zwecke verhaltensbasierter Werbung auf Grundlage berechtigter Interessen oder eines Vertrags mit den Nutzer:innen[267] -verbietet. Meta wiederum hatte eine Woche Zeit, um diese Maßnahme umzusetzen.

Anfang November hat das Unternehmen nun ein Abomodell eingeführt, das Nutzer:innen von Facebook und Instagram vor die Wahl stellt, monatlich einen Geldbetrag zu zahlen oder in die Verarbeitung ihrer Daten zum Zweck der verhaltensbasierten Werbung einzuwilligen. Die Aufsichtsbehörden werden die Rechtmäßigkeit dieses -Verfahrens überprüfen.

Zusammen mit anderen deutschen und europäischen Aufsichtsbehörden konnten wir erreichen, dass die DPC die rechtswidrige Datenverarbeitung durch Meta verbieten muss. Dieser erfolgreiche Abschluss eines Dringlichkeitsverfahrens nach Art. 66 DSGVO ermutigt zur künftigen Anwendung entsprechender Dringlichkeitsmaßnahmen in einem Mitgliedstaat und deren Ausweitung auf den gesamten EWR, um nicht umgesetzte Entscheidungen über den EDSA durchzusetzen. Dass damit auch die jeweils zuständige Aufsichtsbehörde zum Eingreifen gegen fortdauernde Grundrechtsverstöße verpflichtet wird, ist ein Signal an Verantwortliche, die auf dem europäischen Markt aktiv sind: Der EDSA zeigt Zähne.

[266] Siehe die zugehörige Pressemitteilung der norwegischen Datenschutzaufsichtsbehörde, abrufbar unter https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/the-norwegian-data-protection-authority-won-against-meta-in-oslo-district-court/.
[267] Siehe Art. 6 Abs. 1 Satz 1 lit. b und f DSGVO.

3. Gestaltung des Registrierungsprozesses bei TikTok

Im Rahmen eines Streitbeilegungsverfahrens hat der EDSA über unseren Einspruch gegen einen Beschlussentwurf der DPC zum Registrierungsprozess bei TikTok entschieden. Dabei machte der EDSA nochmals deutlich, dass die manipulative Gestaltung von Klickstrecken (sog. Dark Patterns) einen Verstoß gegen die DSGVO darstellt, wenn sie Nutzer:innen davon abhält, datenschutzfreundliche Einstellungen vorzunehmen.

Die DPC hatte im Rahmen des europäischen Kooperationsmechanismus[268] im September des Jahres 2022 einen Beschlussentwurf für eine Maßnahme gegen TikTok vorgelegt. Im Kern hatte die DPC folgende Verstöße festgestellt: Die Voreinstellungen eines TikTok-Accounts von Minderjährigen waren so gewählt, dass der gepostete Inhalt automatisch für alle Internetnutzer:innen – selbst wenn diese nicht Nutzer:innen von -TikTok waren – sichtbar war. Eine mögliche Beschränkung der Sichtbarkeit, beispielsweise auf Freund:innen oder ausgewählte Nutzerkonten, mussten Nutzer:innen aktiv einstellen. Darin sah die DPC einen Verstoß gegen die Pflicht zum Schutz personenbezogener Daten durch Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen[269] sowie gegen den gesetzlichen Grundsatz der Datenminimierung[270]. Zudem befand die DPC, TikTok informierte minderjährige Nutzer:innen nicht ausreichend klar darüber, dass der hochgeladene Inhalt automatisch für alle Internetnutzer:innen sichtbar war.

Aus unserer Sicht kam noch ein weiterer Verstoß hinzu, der in dem Beschlussentwurf unberücksichtigt geblieben war: Der Registrierungsprozess war für die minderjährigen Nutzer:innen so gestaltet, dass datenschutzfreundliche Einstellungen deutlich erschwert wurden – beispielsweise durch die optische Hervorhebung und uneindeutige Beschriftung von Buttons – oder deutlich aufwendiger zu erreichen waren, da sie mehrere Klicks erforderten (sog. Nudging oder Dark Patterns). Wenn solche Designs Nutzer:innen dazu verleiten, unbeabsichtigte und potenziell schädliche Entscheidungen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten zu treffen, oder sie davon abgehalten werden, bewusste Entscheidungen über die Verarbeitung ihrer Daten zu treffen, kann dies ein Verstoß

[268] Siehe Art. 56, Art. 60 ff. DSGVO.
[269] Siehe Art. 25 DSGVO.
[270] Siehe Art. 5 Abs. 1 lit. c DSGVO.

gegen den gesetzlichen Grundsatz von Treu und Glauben[271] sein.[272]

Als für die innerdeutsche Koordinierung zuständige Aufsichtsbehörde[273] haben wir mit Unterstützung weiterer deutscher Aufsichtsbehörden gegen den Beschlussentwurf der DPC Einspruch eingelegt. Entsprechend den Regelungen des europäischen Kooperationsmechanismus musste der EDSA in der Folge über die Einsprüche in einem Streitbeilegungsverfahren[274] entscheiden. An der Vorbereitung des verbindlichen EDSA-Beschlusses haben wir in der entsprechenden europäischen Arbeitsgruppe für Deutschland mitgearbeitet. In seinem endgültigen, verbindlichen Beschluss hat sich der EDSA sodann unserer Auffassung vollständig angeschlossen.[275]

Die DPC hat den Beschluss umgesetzt und gegen TikTok einen entsprechenden Bescheid erlassen, mit dem zusätzlich angeordnet wird, dass TikTok seine Datenverarbeitung auch im Hinblick auf den Grundsatz von Treu und Glauben in Einklang mit der DSGVO bringen muss. Sie hat ein Bußgeld von insgesamt 345 Millionen Euro gegen TikTok verhängt.[276]

Betreiber:innen von sozialen Netzwerken und ähnlichen Onlineangeboten müssen sicherstellen, dass bei der Registrierung eines Kontos die persönlichen Einstellungen grundsätzlich – by default – datenschutzfreundlich eingestellt sind. Sie dürfen Nutzer:innen auch nicht durch die manipulative Gestaltung des Registrierungsprozesses davon abhalten, datenschutzfreundliche Einstellungen zu wählen. Insbesondere wenn Inhalte durch Minderjährige im Internet veröffentlicht werden, müssen Verantwortliche sicherstellen, dass die Nutzer:innen dies willentlich und bewusst tun.

4. Leitlinien zum Auskunftsrecht

Im April dieses Jahrs hat der EDSA nach öffentlicher Konsultation Leitlinien zum Recht auf Auskunft nach

[271]Siehe Art. 5 Abs. 1 lit. a DSGVO.
[272]Siehe auch EDSA, Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them (Version 2.0) vom 24. Februar 2023, S. 2, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.
[273]Die deutsche TikTok-Niederlassung befindet sich in Berlin.
[274]Siehe Art. 65 DSGVO.
[275]EDSA, Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR) vom 2. August 2023, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en.
[276]DPC, Pressemitteilung vom 15. September 2023, abrufbar unter https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok.

Art. 15 DSGVO beschlossen.[277] An der Erarbeitung haben wir uns umfangreich beteiligt. Die Leitlinien beantworten eine Vielzahl von Fragen, wie auf Auskunftsverlangen betroffener Personen zu reagieren ist.

Aus den Leitlinien lässt sich u. a. entnehmen, dass Verantwortliche keine umfassenden Angaben von der betroffenen Person verlangen dürfen, sondern nur diejenigen, die erforderlich sind, um die Person zu identifizieren – etwa pseudonyme Kennungen wie IP-Adressen oder Cookies.[278] Verantwortliche müssen sicherstellen, dass die Daten zwischen dem Eingang des Auskunftsersuchens und der Erteilung der Auskunft nicht gelöscht oder verändert werden – auch wenn sich herausstellt, dass die Daten falsch sind oder die Verarbeitung rechtswidrig ist.[279] Die betroffenen Personen können für ihr Auskunftsersuchen grundsätzlich alle Kommunikationswege nutzen; nicht nur diejenigen, die der Verantwortliche für Datenschutzfragen angibt.[280] Werden Daten für verschiedene Zwecke verarbeitet, so muss sich aus der Auskunft ergeben, welche Daten für welche Zwecke verarbeitet werden.[281] Entsprechendes gilt etwa auch für die Löschfristen, die zudem konkret anzugeben sind, notfalls durch Angabe der Speicherfrist und des die Frist auslösenden Ereignisses.[282]

Die Leitlinien des EDSA geben Verantwortlichen eine recht umfassende Hilfestellung, wie sie mit Auskunftsersuchen nach Art. 15 DSGVO umzugehen haben. Sie gehören zur Pflichtlektüre aller Verantwortlichen und der im Datenschutzrecht beratenden Personen.

5. Orientierung für digitale Dienste

Wer digitale Dienste nutzt, tut dies mit einem Gerät, beispielsweise einem Smartphone mit integriertem Browser und installierten mobilen Anwendungen oder intelligenten Lautsprechern mit digitalen Assistenten. Die Daten, die im Zuge der Nutzung auf dem Gerät gespeichert oder auf die durch den Dienst zugegriffen wird, können zur Nachverfolgung der Interaktion der Nutzer:innen mit dem jeweils genutzten Dienst, aber auch dienstübergreifend verwendet werden. Dies hat Folgen für die Privatsphäre der Nutzer:innen. Daher

[277]EDSA, Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht (Version 2.1) vom 17. April 2023, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_de.

[278]Ebd., Rn. 125, siehe auch Rn. 45, 61.

[279]Ebd., Rn. 36, 38, 39.

[280]bd., Rn. 53 ff.

[281]Ebd., Rn. 113.

[282]Ebd., Rn. 118.

ist eine Speicherung von Daten in einer Endeinrichtung und der Zugriff auf gespeicherte Daten nur mit Einwilligung der betroffenen Personen oder im Rahmen der Erforderlichkeit zulässig. Die Leitlinien des EDSA klären die Frage, bei welchem technischen Vorgehen diese Regelung greift.

Die von uns und der nationalen Datenschutzaufsichtsbehörde Frankreichs (CNIL) koordinierte „Technology Expert Subgroup" hat dieses Jahr im Auftrag des EDSA -Leitlinien[283] zur Auslegung von Art. 5 Abs. 3 der E-Privacy-Richtlinie erarbeitet, die der deutschen Regelung in § 25 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) zugrunde liegt. Sie haben das Ziel, ein klares Verständnis dafür zu fördern, wann technische Verfahren in den Anwendungsbereich der gesetzlichen Regelung fallen. Es werden daher die vier grundlegenden Merkmale beleuchtet, die Vorgehensweisen aufweisen müssen, um unter die gesetzliche Regelung zu fallen:

- Welche Art von Informationen wird erfasst?
- Was alles stellt eine Endeinrichtung i. S. d. § 2 Abs. 2 Nr. 6 TTDSG dar?
- Wann kann von einem Zugriff auf gespeicherte Daten gesprochen werden?
- Wann ist von einer Speicherung von Informationen auf dem Gerät auszugehen?

Die Leitlinien gehen von der Intention des Gesetzgebers aus, die Privatsphäre von Nutzer:innen umfassend zu schützen,[284] und stellen klar, dass alle Arten von Informationen durch die Regelung erfasst werden. Es spielt keine Rolle, ob die Informationen personenbezogen sind oder nicht, wie es zu ihrer Speicherung kommt und wer diese veranlasst hat. Bei den relevanten Endeinrichtungen handelt es sich um alle Geräte, die an ein öffentliches Kommunikationsnetz direkt oder indirekt angeschlossen sind und mit digitalen Diensten über dieses Netz interagieren, solange und soweit sie Daten und Nachrichten nicht ausschließlich weiterleiten. Klassische Endeinrichtungen sind Arbeitsplatzcomputer, Tablets und Smartphones. Erfasst werden aber auch Smart-Home-Geräte, vernetzte Fahrzeuge und andere Geräte des Internet of Things (IoT).

Die Definition einer Endeinrichtung wirft die Frage auf, wann von einem Zugang zu einem digitalen Dienst

[283]EDSA, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive vom 14. November 2023, abrufbar unter https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en.

[284]Diese Intention wurde auch vom Europäischen Gerichtshof (EuGH) bestätigt; siehe EuGH, Urteil vom 1. Oktober 2019, C 673/17, Rn. 70.

über ein öffentliches Kommunikationsnetz die Rede ist. Bei dem klassischen Internetzugang ist das klar. Die Leitlinien weisen jedoch darauf hin, dass es weder auf das Kommunikationsmedium noch auf die Zwischenschaltung irgendwelcher vermittelnder weiterer Geräte, weder auf die Zahl der an dem Kommunikationsnetz angeschlossenen Teilnehmer:innen noch auf den öffentlich-rechtlichen Betrieb oder eine zentralisierte und dauerhafte Verwaltung des Netzes ankommt. So gehören auch Netzwerke von Geräten dazu, die ad hoc zusammengestellt werden und Kommunikationsverfahren für Übertragungen über kurze Distanz verwenden, solange sie öffentlich zugänglich sind.

Auch in Bezug auf den Zugang zu gespeicherten Informationen ist ein umfassender Blick auf alle zur Verfügung stehenden Methoden und Konstellationen von beteiligten Akteuren notwendig. Von einem Zugriff auf Informationen in der Endeinrichtung ist auszugehen, unabhängig davon, wer die Speicherung der Informationen veranlasst hat, die einem Dienst bekannt gegeben werden. Er kommt auch zustande, wenn ein Dienst die Endeinrichtung instruiert, gespeicherte Daten zu versenden, und ein anderer Dienst sie empfängt. So sind in Websites vielfach Elemente enthalten, die den Browser der Nutzer:innen veranlassen, weitere Informationen nachzuladen. Im Zuge dieses Abrufs von Informationen gibt der Browser sowohl langfristig gespeicherte Informationen weiter, wie etwa bestimmte Konfigurationsoptionen, als auch Informationen, die mit dem Element verbunden sind, das das Nachladen verursacht. In diesem kann der Dienst, der die Website bereitstellt, intransparent für die Nutzer:innen vielfältige Informationen über ihre Nutzung kodieren. Diese Informationen können über eine Kette von Zugriffen hinweg miteinander verbunden und dafür genutzt werden, ein Profil über die nutzende Person aufzubauen.

Die Leitlinien stellen klar, dass die gesetzliche Regelung alle Formen der Speicherung von Informationen auf Endeinrichtungen erfasst. Es kommt dabei weder auf den Zweck noch die Zeitdauer oder das Speichermedium an. In Konsequenz der Regelung in § 25 TTDSG sind die Anbieter:innen digitaler Dienste daher verpflichtet, sorgfältig zu analysieren, inwieweit es im Zuge der Erbringung ihres Diensts dazu kommt, dass Informationen in Endeinrichtungen gespeichert werden oder auf gespeicherte Informationen zugegriffen wird. Für jeden Vorgang des Zugriffs oder der Speicherung verlangt der Gesetzgeber eine informierte freiwillige Einwilligung der Nutzer:innen, es sei denn, der Zweck des Vorgangs richtet sich allein auf die Durchführung der Datenübertragung, etwa in der Abwicklung eines Kommunikationsprotokolls, oder der Vorgang ist im

engen Sinne erforderlich, um einen ausdrücklich gewünschten Dienst zu erbringen.

Um einen umfassenden Schutz der Privatsphäre der Personen zu gewährleisten, die digitale Dienste nutzen, sind die gesetzlichen Vorgaben auf alle Formen der Speicherung von Informationen in Endeinrichtungen und des Zugriffs auf gespeicherte Informationen anzuwenden. Die Informationen können beliebiger Natur sein, die Speicherung auf beliebigen Speichermedien und für beliebig lange oder kurze Zeiträume erfolgen und ein Zugriff auf gespeicherte Daten vorliegen, unabhängig davon, wer die Speicherung der offengelegten Daten bewirkt hat und ob die Quelle der Anweisung an die Endeinrichtung zur Übermittlung der Daten mit den Empfänger:innen übereinstimmt. Ebenso ist die Anwendung der gesetzlichen Regelung unabhängig von der Art der Endeinrichtung und ihrer Anbindung an ein öffentliches Kommunikationsnetz.

6. Abschlussbericht der Cookie Banner Taskforce

Angesichts der Vielzahl an Beschwerden über den Einsatz von Cookies und die Gestaltung der Einwilligungsbanner auf Websites hatte der EDSA im September 2021 eine Arbeitsgruppe, die sog. Cookie Banner Taskforce, eingerichtet.[285] Diese hatte zum Ziel, die Rechtsauffassung der Aufsichtsbehörden untereinander abzustimmen und zu einer europaweit einheitlichen Anwendung der datenschutzrechtlichen Bestimmungen beizutragen. Wir waren aktiv daran beteiligt und haben die Ergebnisse gemeinsam mit den anderen Mitgliedern der Arbeitsgruppe im Januar dieses Jahres veröffentlicht.

Der Abschlussbericht[286] führt aus, dass die Beurteilung des Einsatzes von Cookies und Einwilligungsbannern nur anhand der in nationales Recht umgesetzten Vorgaben der E-Privacy-Richtlinie erfolgen kann, für die Bewertung der aus ihnen resultierenden Datenverarbeitungen allerdings die DSGVO zum Tragen kommt. Erst wenn geprüft ist, ob die Bedingungen für eine gültige Einwilligung und die Wahrung der Informationspflicht erfüllt sind, lässt sich beurteilen, ob ein rechtlicher Verstoß in der Nutzung von Cookies und der Gestaltung von Bannern vorliegt oder nicht.

[285]EDSA, Pressemitteilung vom 27. September 2021, abrufbar unter: https://edpb.europa.eu/news/news/2021/edpb-establishes-cookie-banner-taskforce_en.
[286]EDSA, Report of the work undertaken by the Cookie Banner Taskforce vom 17. Januar 2023, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en.

Die Banner dürfen keinesfalls so gestaltet sein, dass der Eindruck entsteht, ohne Einwilligung sei der Zugriff auf den Inhalt der Website verwehrt. Die Besucher:innen müssen ihre Einwilligung freiwillig erteilen und dürfen nicht zu deren Abgabe gezwungen werden. Dementsprechend listet der Bericht grundlegende Merkmale in der Gestaltung der Banner auf, die die Bedingungen an eine wirksame Einwilligung nach der DSGVO nicht erfüllen:

- Keine Möglichkeit zur Ablehnung auf derselben Ebene wie die Einwilligung
- Vorangekreuzte Auswahlfelder
- Täuschende Farbgebung oder unzureichender Kontrast der Ablehnungsoption
- Ungenügend hervorgehobene oder außerhalb des Banners platzierte Textlinks
- Berufung auf ein berechtigtes Interesse als Rechtsgrundlage für die Verarbeitung
- Fehlerhafte Kategorisierung der essenziellen bzw. technisch notwendigen Cookies
- Keine Möglichkeit des Widerrufs der Einwilligung

Die Ergebnisse der Cookie Banner Taskforce spiegeln die gemeinsame Rechtsauffassung der europäischen Aufsichtsbehörden bei der Bewertung nach der DSGVO in Bezug auf die Einwilligung in die Datenverarbeitung durch Cookies wider. Sie entsprechen dabei auch der Position der Datenschutzkonferenz (DSK) in ihrer Orientierungshilfe für Anbieter:innen von Telemedien.[287] Allerdings greifen sie der eigenständigen Analyse und Beurteilung nicht vor, die jede Aufsichtsbehörde im Fall von Beschwerden oder betroffenen Websites vornehmen muss. Der Abschlussbericht formuliert nur den Maßstab, der mit den nationalen, die E-Privacy-Richtlinie umsetzenden Bestimmungen abgeglichen werden muss.

7. Fortschritte bei der Datenschutzzertifizierung

Die ersten Datenschutzzertifizierungsprogramme sind in Deutschland und Europa genehmigt worden. Wir haben das Zertifizierungsprogramm der in Bremen -ansässigen datenschutz cert GmbH als Co-Reviewer begutachtet, um die Genehmigung des Programms zu beschleunigen. Mit dem Programm sollen verantwortliche Stellen und Auftragsverarbeiter in Deutschland zertifiziert werden können. Gemeinsam mit der italienischen Datenschutzaufsichtsbehörde (GPDP) haben wir dem Programm-eigner -relevante Hinweise für die

[287] DSK, Orientierungshilfe für Anbieter:innen von Telemedien (Version 1.1) vom 5. Dezember 2022, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf; siehe dazu auch JB 2021, 14.2.

Verbesserung des Programms gegeben. Als Berichterstatter nehmen wir das europäische Feedback auf und werden es im nächsten Jahr in die Stellungnahme des EDSA einfließen lassen.

Vor der Erteilung von Datenschutzsiegeln durch eine Zertifizierungsstelle muss als erster Schritt ein Zertifizierungsprogramm genehmigt werden. Im zweiten Schritt wird eine Zertifizierungsstelle für das Programm akkreditiert. Diese kann dann die Datenverarbeitung zertifizieren und damit das Siegel erteilen. In den ersten beiden Schritten arbeitet die zuständige Datenschutzaufsichtsbehörde mit der Deutschen Akkreditierungsstelle (DAkkS) zusammen. Zusätzlich muss der EDSA eine Stellungnahme zum Kriterienkatalog abgeben, bevor das Programm genehmigt werden kann. Der Kriterienkatalog enthält die Anforderungen an die zu zertifizierende Verarbeitung. Er wird ergänzt durch Prüfmethoden und Anwendungshinweise. Im Vorfeld der Stellungnahme des EDSA begutachten zwei Aufsichtsbehörden das Programm und arbeiten ihren Bericht in die Stellungsnahme des EDSA ein.

Zusammen mit der GPDP haben wir den Genehmigungsprozess des Programms der datenschutz cert GmbH unterstützt, um die Datenschutzzertifizierung in Deutschland voranzubringen. Die datenschutz cert GmbH hat ein gutes generisches Zertifizierungsprogramm für Verantwortliche und Auftragsverarbeiter vorgelegt, anhand des gemeinsamen Feedbacks von uns und unseren italienischen Kolleg:innen weiter verbessert und an existierenden EDSA-Leitlinien ausgerichtet. Die datenschutz cert GmbH ist bereits für andere Zertifizierungen von der DAkkS akkreditiert, sodass wir nach der Genehmigung auf eine baldige Akkreditierung hoffen, damit (auch) diese Zertifizierungsstelle mit ihren Siegeln den Betroffenen bei der Suche nach datenschutzkonformen Produkten und Dienstleistungen helfen kann.

Zeitgleich haben wir 2023 bei einem Anbieter aus dem Medizinbereich bewirkt, dass dieser ein unechtes Datenschutzzertifikat von der Website genommen hat. Durch die Förderung echter und die Eindämmung unechter Siegel erleichtern wir Betroffenen und Verantwortlichen die Auswahl.

Die Erstellung und Genehmigung generischer Zertifizierungsprogramme ist mit einem erheblichen Aufwand verbunden, sowohl für die Programmeigner:in als auch für uns als beteiligte Aufsichtsbehörde. Unser Anspruch ist, trotz des hohen Abstraktionsgrades der Zertifizierungskriterien einen angemessenen Detailgrad für rechtliche, technische und organisatorische

Anforderungen zu erreichen, um die korrekte und einheitliche Anwendung des Zertifizierungsprogramms in der Praxis sicherzustellen. Durch die eingehende Prüfung des Kriterienkatalogs sichern wir gute Ausgangsbedingungen für den Zertifizierungsprozess.

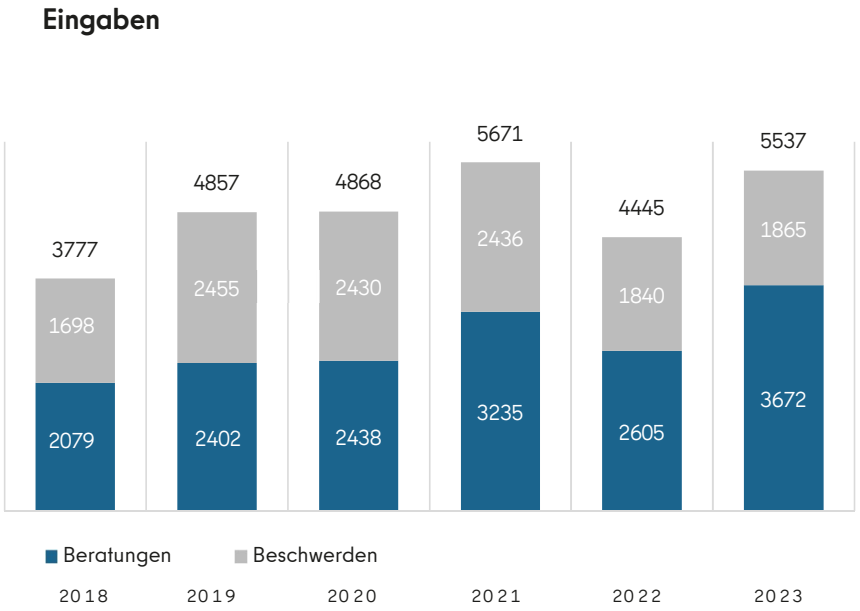
D. Anhang

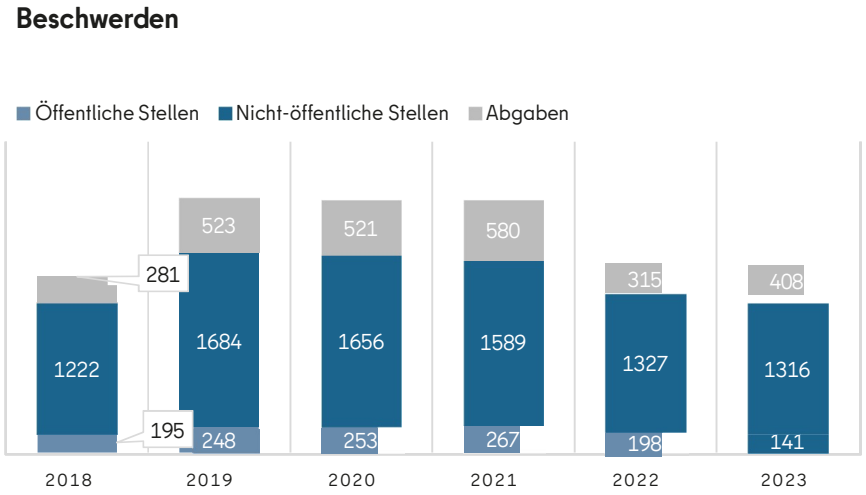
I. Statistik

In diesem Jahr verzeichnete die Behörde eine weiterhin hohe Anzahl von Eingaben durch die Bürger:innen, wobei insbesondere die schriftlichen Beratungen signifikant zugenommen haben. Die Zahl der gemeldeten Datenpannen verblieb auf dem hohen Niveau der Vorjahre. Die Darstellung des Kapitels orientiert sich an den einheitlichen Statistikkriterien der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK).

1. Beratungsanfragen und Beschwerden

Insgesamt wurden 5.537 Eingaben von Bürger:innen in diesem Jahr erfasst. Die beachtliche Steigerung bei den schriftlichen Beratungen sticht dabei besonders hervor: Über das Jahr verteilt wandten sich 3.672 betroffene Personen per E-Mail oder Brief mit einer Anfrage an uns, etwa weil sie Unterstützung bei der Geltendmachung ihrer Rechte benötigten oder Beratung zu einem Datenschutzverstoß wünschten. Dies bedeutet eine Zunahme der Beratungsanfragen um 41 Prozent im Vergleich zum Vorjahr, als lediglich 2.605 Anfragen eingingen. Zusätzlich erreichten uns 1.865 persönliche Beschwerden von Betroffenen – eine moderate Steigerung zum Vorjahr (1.840 Beschwerden).

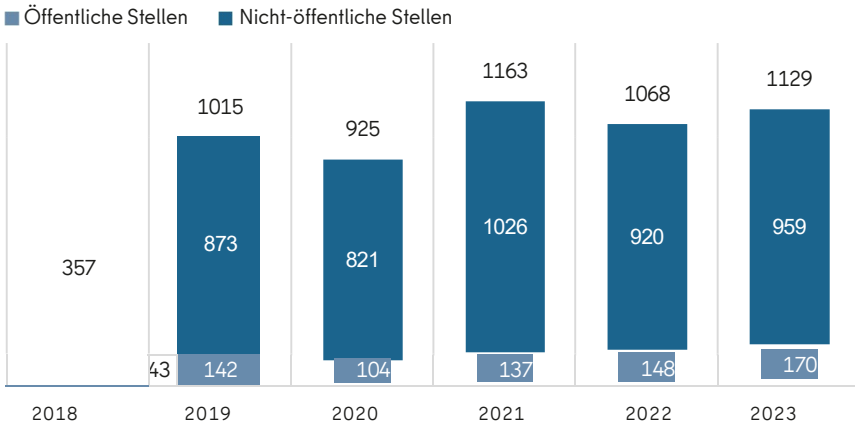




Für den Großteil der Beschwerden eröffneten wir Verfahren in eigener Zuständigkeit. Dies waren in diesem Jahr 1.457 Verfahren. Die meisten davon (1.316) richteten sich gegen private Stellen, die restlichen (141) betrafen Behörden und andere öffentliche Stellen. In 408 Fällen lagen die Beschwerden nicht in unserem Zuständigkeitsbereich, weshalb wir sie an die jeweils zuständigen Aufsichtsbehörden abgegeben haben.

2. Meldung von Datenpannen

Meldungen von Datenpannen



Der Begriff „Datenpanne“ bezeichnet eine Verletzung des Schutzes personenbezogener Daten, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten führt. Verantwortliche sind grundsätzlich verpflichtet, eine Datenpanne innerhalb von 72 Stunden bei unserer Behörde zu melden. In diesem Jahr stieg die Gesamtanzahl der gemeldeten Datenpannen im Vergleich zum Vorjahr an. Während im Jahr 2022 insgesamt 1.068 Meldungen erfasst wurden, erhöhte sich diese Zahl 2023 auf 1.129. Die Aufschlüsselung der Zahlen zeigt, dass öffentliche Stellen im diesem Jahr 170 Datenpannen meldeten (Vorjahr: 148). Ebenso stieg die Anzahl der Meldungen von nicht-öffentlichen Stellen von 920 im Jahr 2022 auf 959 im Jahr 2023.

3. Anträge nach dem Informationsfreiheitsgesetz

Wir erhielten 44 Anträge auf Aktenauskunft bzw. Akteneinsicht. Die Antragsgegenstände entsprachen denen des Vorjahrs und betrafen Informationen zu Meldungen von Datenpannen, Datenschutzbeschwerden und Prüfverfahren sowie statistische Angaben zu Sanktionsmaßnahmen.
Eingaben nach dem Informationsfreiheitsgesetz (IFG) erhielten wir in 111 Fällen, in denen unsere Behörde aufgrund einer mutmaßlich nicht oder unzureichend erteilten Auskunft bzw. Einsicht durch öffentliche Stellen im Land Berlin angerufen wurde. Das bedeutet einen Anstieg um fast ein Drittel gegenüber dem Vorjahr. Die Beschwerden betrafen sämtliche Senatsverwaltungen, auch nachgeordnete Einrichtungen sowie fast alle Bezirksämter.

4. Europäische Verfahren

Die Datenschutz-Grundverordnung (DSGVO) sieht vor, dass in Fällen grenzüberschreitender Datenverarbeitung eine europaweite Zusammenarbeit der Datenschutzaufsichtsbehörden erfolgen muss. Im Rahmen dieses Kooperationsverfahrens wird eine federführende Aufsichtsbehörde ernannt, die die Ermittlungen in dem jeweiligen Fall leitet. Weitere Aufsichtsbehörden können sich als betroffene Stellen melden, wenn die Verantwortlichen eine Niederlassung in ihrem Land haben oder die Datenverarbeitung erhebliche Auswirkungen auf die Bürger:innen ihres Landes hat. In diesem Jahr wurden wir in 20 Verfahren als federführende Aufsichtsbehörde bestimmt. Eine Betroffenheit ergab sich in 297 Fällen. In 28 Verfahren erließen wir einen Beschlussentwurf oder einen endgültigen Beschluss.

Europäische Verfahren mit unserer Beteiligung 2023

Verfahren nach Art. 56 DSGVO (betroffen)	297
Verfahren nach Art. 56 DSGVO (federführend)	20
Verfahren nach Art. 60 ff. DSGVO (federführend)	28

5. Abhilfemaßnahmen

Stellen wir einen Verstoß von Verantwortlichen gegen die DSGVO fest, können wir verschiedene Abhilfemaßnahmen ergreifen.[288] Dementsprechend haben wir in -diesem Jahr Folgendes veranlasst: Wir haben 139 Verwarnungen ausgesprochen. In zwei -Fällen wurde eine Anordnung getroffen. Wir haben 26 Bußgeldbescheide mit 64 Buß-geldern in Höhe von insgesamt 549.410 Euro erlassen. Die entsprechenden Verfahren waren bis Ende des Jahres jedoch noch nicht alle rechtskräftig abgeschlossen. Zudem sind 12 Zwangsgeldbescheide ergangen. In sechs Fällen haben wir einen Strafantrag gestellt. Über das Jahr verteilt wurden 31 Bußgeldverfahren eingestellt und 71 Verfahren neu eröffnet.

[288] Siehe Art. 58 Abs. 2 DSGVO.

Abhilfemaßnahmen 2023

Warnungen	0
Verwarnungen	139
Anweisungen und Anordnungen	2
Geldbußen	64

II. Abkürzungen

Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AKIF	Arbeitskreis der Informationsfreiheitsbeauftragten
Alt.	Alternative
ArbG	Arbeitsgericht
Art.	Artikel
ASOG Bln	Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (Allgemeines Sicherheits- und Ordnungsgesetz)
AStA	Allgemeiner Studierendenausschuss
AufenthG	Aufenthaltsgesetz
BAG	Bundesarbeitsgericht
BBBG	Gesetz über die Anstalt öffentlichen Rechts Berliner Bäder- Betriebe (Bäder-Anstaltsgesetz)
BDSG	Bundesdatenschutzgesetz
beBPo	besonderes elektronisches Behördenpostfach
BerlHG	Berliner Hochschulgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BlnDSG	Berliner Datenschutzgesetz
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern und für Heimat
BRAK	Bundesrechtsanwaltskammer
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerwG	Bundesverwaltungsgericht
BVG	Berliner Verkehrsbetriebe
BWB	Berliner Wasserbetriebe
bzw.	beziehungsweise
CDU	Christlich Demokratische Union
CNIL	Commission Nationale de l'Informatique et des Libertés (Nationale Datenschutzaufsichtsbehörde Frankreichs)
CSD	Christopher Street Day
DAkkS	Deutsche Akkreditierungsstelle
d.h.	das heißt
DiDat	Ausschuss für Digitalisierung und Datenschutz
DiGA	Digitale Gesundheitsanwendungen
DiGAV	Digitale Gesundheitsanwendungen-Verordnung
DigLLV	Digitale Lehr- und Lernmittelverordnung
DiPA	Digitale Pflegeanwendungen
DOC	Department of Commerce (US-Handelsministerium)
DOT	Department of Transportation (US-Verkehrsministerium)
DPC	Data Protection Commission (Nationale Datenschutzaufsichtsbehörde Irlands)
DPF	EU-U.S. Data Privacy Framework (Datenschutzrahmen EU-USA)
Drs.	Drucksache
DSGVO	Datenschutz-Grundverordnung

DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz)
ebd.	ebenda
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuch
EGMR	Europäischer Gerichtshof für Menschenrechte
EGovG Bln	E-Government-Gesetz Berlin
EKD	Evangelische Kirche in Deutschland
Engl.	englisch
ErwGr.	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
EZB	Europäische Zentralbank
f.	folgende/folgender (Seite/Artikel/Paragraf)
ff.	folgende (Seiten/Artikel/Paragrafen)
FTC	Federal Trade Commission (US-Wettbewerbs- und Verbraucherschutzbehörde)
FU	Freie Universität Berlin
GDNG	Gesetz zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz)
GeoZG Bln	Gesetz über den Zugang zu digitalen Geodaten im Land Berlin (Geodatenzugangsgesetz Berlin)
GG	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GOSen	Geschäftsordnung des Senats
GPDP	Garante per la Protezione dei Dati Personali (Nationale Datenschutzaufsichtsbehörde Italiens)
GRCh	Charta der Grundrechte der Europäischen Union
GVBl.	Gesetz- und Verordnungsblatt
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
Hs.	Halbsatz
HTML	Hypertext Markup Language
HU	Humboldt-Universität zu Berlin
IFG	Berliner Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
IKT	Informations- und Kommunikationstechnologie
IoT	Internet of Things (Internet der Dinge)
IP	Internetprotokoll
IPV	Integrierte Personalverwaltung
ISBJ	Integrierte Software Berliner Jugendhilfe
i.S.d.	im Sinne des
IT	Informationstechnologie
ITDZ	IT-Dienstleistungszentrum Berlin
i.V.m.	in Verbindung mit
IWGDPT	International Working Group on Data Protection in Technology (Internationale Arbeitsgruppe für Datenschutz in der Technologie, auch Berlin Group)
JAktAG	Justizaktenaufbewahrungsgesetz

JAktAV	Verordnung über die Aufbewahrung und Speicherung von Justizakten
JB	Jahresbericht
JI-Richtlinie	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
KBA	Kraftfahrt-Bundesamt
KfZ	Kraftfahrzeug
KI	Künstliche Intelligenz
LABO	Landesamt für Bürger- und Ordnungsangelegenheiten
LAG	Landesarbeitsgericht
LDA	Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg
LEA	Landesamt für Einwanderung
LfD SH	Landesbeauftragte für Datenschutz Schleswig-Holstein
LfDI MV	Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
Lit.	littera (Buchstabe)
Ls.	Leitsatz
Ltd.	Limited Company by Shares (britische Kapitalgesellschaft)
LUSD	Berliner Lehrkräfte-Unterrichts-Schuldatenbank
MDR	Mitteldeutscher Rundfunk
MFA	Mehrfaktor-/Multifaktor-Authentifizierung
MS 365	Microsoft 365
MVZ	Medizinisches Versorgungszentrum
m.w.N.	mit weiteren Nachweisen
Nr.	Nummer
NSU	Nationalsozialistischer Untergrund
OLG	Oberlandesgericht
OSS	One-Stop-Shop
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
OZG	Onlinezugangsgesetz
OZGÄndG	Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz)
PIN	Persönliche Identifikationsnummer
POLIKS	Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung
PStG	Personenstandsgesetz
PStV	Personenstandsverordnung
RBB	Rundfunk Berlin-Brandenburg
RdB	Rat der Bürgermeister
Rn.	Randnummer
RVG	Rechtsanwaltsvergütungsgesetz
S.	Seite
SaaS	Software-as-a-Service
SCC	Standardvertragsklauseln

SchuldatenV	Schuldatenverordnung
SchulG	Berliner Schulgesetz
SDM	Standard-Datenschutzmodell
SDTB	Sächsische Datenschutz- und Transparenzbeauftragte
SE	Societas Europaea (Europäische Aktiengesellschaft)
SenBJF	Senatsverwaltung für Bildung, Jugend und Familie
SenFin	Senatsverwaltung für Finanzen
SenJustVA	Senatsverwaltung für Justiz und Verbraucherschutz
SenMVKU	Senatsverwaltung für Mobilität, Verkehr, Klimaschutz und Umwelt
SenStadt	Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen
SGB	Sozialgesetzbuch
SMS	Short Message Service
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
stopp	Strafprozessordnung
TAN	Transaktionsnummer
TIA	Transfer Impact Assessment
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz)
TU	Technische Universität Berlin
u.a.	unter anderem
UAbs.	Unterabsatz
UIG	Umweltinformationsgesetz
U.S./USA	United States of America
Usw.	und so weiter
UWG	Gesetz über den unlauteren Wettbewerb
UZwG Bln	Gesetz über die Anwendung unmittelbaren Zwanges bei der Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Landes Berlin
VBB	Verkehrsverbund Berlin-Brandenburg
VerfGH	Verfassungsgerichtshof
VG	Verwaltungsgericht
VGebO	Verwaltungsgebührenordnung
VOIS	Verwalten, Organisieren, Integrieren, Systematisieren (Soft- wareplattform zur Integration kommunaler Fachverfahren)
Vs.	versus
VvB	Verfassung von Berlin
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
WRV	Weimarer Reichsverfassung
WÜd	Wiener Übereinkommen über diplomatische Beziehungen
z.b.	zum Beispiel
2FA	Zwei-Faktor-Authentifizierung