Abgeordnetenhaus BERLIN

Drucksache 19/2884
14.01.2026

19. Wahlperiode

Vorlage – zur Kenntnisnahme –

Stellungnahme des Senats zum Bericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2024

Der Senat von Berlin
InnSport – 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 2024

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 13. Januar 2026

Der Senat von Berlin

Kai Wegner

Regierender Bürgermeister

Iris Spanger

Senatorin für Inneres und Sport

Stellungnahme des Senats

zum Bericht der

Berliner Beauftragten für

Datenschutz und

Informationsfreiheit

für das

Jahr 2024

(nach § 12 Abs.2 Berliner Datenschutzgesetz)

Inhaltsverzeichnis

Vorwort

Die Europäische Union hat in den letzten Jahren im Rahmen ihrer Daten- und Digitalstrategie eine Reihe von Rechtsakten erlassen, um im Rahmen der europäischen Werte Potenziale der Datennutzung besser auszuschöpfen. Dabei spielen etwa der Digital Services Act, der Data Act, die KI-Verordnung und der Data Governance Act eine Rolle, die viele Schnittstellen zur Datenschutz-Grundverordnung aufweisen, diese aber im Wesentlichen unberührt lassen sollen. Diese Schnittstellen werden in der Datenschutzaufsicht der kommenden Jahre eine besondere Rolle spielen.

Zur nationalen Durchführung der Europäischen Datenstrategie und ihrer Rechtsakte sollte daher ein national stringentes Gesamtkonzept der Aufsicht überlegt werden, das auch die vorhandenen föderalen Aufsichtsstrukturen im Datenschutz in den Blick nimmt. Rechtspolitische Äußerungen und erste Gesetzesentwürfe zu den verschiedenen Digitalrechtsakten weisen jedoch darauf hin, dass der Bund die Richtung einer zentralistischen Aufsicht eingeschlagen hat. Mit Sorge beobachte ich diese Bestrebungen einer Kompetenzverlagerung zum Bund, die auch die Datenschutzaufsicht betrifft und die Mitgestaltungs- und Einflussmöglichkeiten der Länder im Hinblick auf die digitalen Zukunftsthemen vermindern würde. Dies wäre auch zum Nachteil der Berliner:innen sowie der regionalen Unternehmen und Vereine, die von unseren individuellen Beratungen, spezifischen Veranstaltungsformaten und unserer lokalen Ansprechbarkeit profitieren. Letztlich könnte verloren gehen, was dezentrale, föderale Strukturen ausmacht: Partizipation, Bürger:innennähe, Nachvollziehbarkeit, Machtausgleich und vor allen Dingen Qualitätssicherung und Best Practice in der gemeinsamen Abstimmung unter den Ländern. Es sollte daher genau geschaut werden, wie eine funktionale, effektive Aufsicht beibehalten und für die neuen Rechtsakte etabliert werden kann, ohne dass auf die Vorteile einer lokalen Aufsichtsstruktur verzichtet werden muss.

Die Überwachung und die Durchsetzung der Datenschutz-Grundverordnung bei der Anwendung von KI

findet mehr und mehr Eingang in unsere Aufsichtspraxis. In ersten Prüfverfahren der KI-Nutzung von Unternehmen haben wir bereits Datenschutzverstöße ausmachen können, die es in der Zukunft zu vermeiden bzw. abzustellen gilt. Bedeutsam ist dabei insbesondere die Frage, auf welcher Rechtsgrundlage die Verarbeitung von personenbezogenen Daten bei der Entwicklung und dem Einsatz von KI erfolgt und wie die erforderliche Transparenz für die betroffenen Personen hergestellt werden kann. Von Relevanz ist zudem, dass beim Einsatz von generativer KI bzw. großen Sprachmodellen häufig zweifelhaft ist, ob die Verarbeitung personenbezogener Daten beim Training der KI-Modelle rechtmäßig war. Wie wirkt sich etwa ein rechtswidriges Training von KI auf den späteren Einsatz des Modells in einem KI-System aus? Erste Antworten auf diese sehr wesentlichen Fragen gibt die Stellungnahme des Europäischen Datenschutzausschusses, die Ende des Jahres veröffentlicht wurde und an der auch wir intensiv mitgewirkt haben.

Die Medienkompetenz von Kindern und Jugendlichen sowie pädagogischen Fachkräften zu fördern, bleibt eine wichtige Aufgabe für uns. Im Mittelpunkt steht die informationelle Selbstbestimmung junger Menschen. In diesem Jahr nahmen wir dazu an wichtigen Bildungs- und Digitalveranstaltungen teil, gaben Workshops an Schulen und begleiteten den neuen multimedialen Datenschutzwegweiser für Kitas der Senatsverwaltung für Bildung, Jugend und Familie. Damit bieten wir praxisnahe Unterstützung und schaffen mehr Transparenz bei Datenschutzfragen im Kitaalltag.

Eine aufschlussreiche Lektüre wünscht

Meike Kamp
Berliner Beauftragte für Datenschutz und Informationsfreiheit

A. Wir in Berlin

I. Gerichtsverfahren

1. Adresshandel vor Gericht

In zwei Fällen sind wir wegen der Überprüfung der Zulässigkeit des gewerblichen Handels mit Adressdaten in Verfahren vor dem Berliner Verwaltungsgericht (VG Berlin). In beiden Fällen beauftragten die werbenden Stellen jeweils Adresshändler:innen, postalische Werbung an potenzielle Kund:innen bzw. Wähler:innen zu versenden. Die Werbenden und die Adresshändler:innen handelten dabei nach unserer Auffassung als gemeinsame Verantwortliche. Die Verarbeitung personenbezogener Daten zum Zwecke der Versendung von Werbung hielten wir vorliegend für rechtswidrig. Wir verwarnten daher jeweils die werbenden Stellen mit Sitz in Berlin, die hiergegen Rechtsschutz vor dem VG Berlin ersuchten.

In einem Fall verwarnten wir den Landesverband einer Partei, weil dieser einem Beschwerdeführer ein Wahlwerbeheft zugeschickt hatte. Der Beschwerdeführer hatte der Partei seine Daten hierfür nicht zur Verfügung gestellt. Vielmehr „mietete“ der Landesverband zur einmaligen Nutzung zu Werbezwecken von einem -Adresshändler Adressdaten, denen u. a. die Merkmale „Performer“, „konservativ-etabliert“ oder „liberal-intellektuell“ zugeschrieben wurden. Daraufhin übermittelte der Adresshändler mehr als 130.000 Datensätze im Auftrag der Partei an einen sog. Lettershop, der dann im Rahmen einer Auftragsverarbeitung das vom werbenden Unternehmen zur Verfügung gestellte Werbematerial an die vom Adresshändler übergebenen Adressen versendete.

Im anderen Fall erhielt eine Beschwerdeführerin ein Werbeschreiben eines Unternehmens für eine Kulturveranstaltung. Auch hier hatte die Beschwerdeführerin ihre Daten nicht mitgeteilt, sondern das Unternehmen einen Adresshändler eingeschaltet. Dieser selektierte aus seinem Datenbestand nach den Vorgaben des Unternehmens Personen, denen die Merkmale „wohnhaft in Berlin“ oder „wohnhaft in Brandenburg“ und „Kaufkraft stark überdurchschnittlich“ oder „Kaufkraft überdurchschnittlich“ zugeordnet waren. Die Datenübermittlung erfolgte ebenfalls im oben beschrieben Lettershop-Verfahren.

Die Adresshändler:innen und die Werbenden sind nach unserer Bewertung vorliegend jeweils gemeinsam Verantwortliche. Die Datenschutz-Grundverordnung (DSGVO) geht nach Art. 26 von gemeinsam Verantwortlichen aus, wenn zwei oder mehr Verantwortliche

gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen.[1] Gemeinsamer Zweck der Verarbeitung ist hier die Direktwerbung an die von den Adresshändler:innen anhand der Kriterien der Werbenden ausgewählten Adressat:innen.

Gleiches gilt auch für die wesentlichen Mittel des Versands der Direktwerbung, bei dem das Verfahren durch die Adresshändler:innen und den konkreten Inhalt des Werbeschreibens sowie die Auswahl der Adressat:innen durch die Werbenden (mit)festgelegt wurde. Der Annahme einer gemeinsamen Verantwortlichkeit steht auch nicht entgegen, dass ein Lettershop eingesetzt wurde und die Werbenden in bestimmten Konstellationen keinen Zugang zu den personenbezogenen Daten hatten. Nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH)[2] kann über die Zwecke und Mittel der Datenverarbeitung auch entscheiden, wer die Daten nicht selbst verarbeitet, also selbst keinen Zugriff auf sie hat. Im Rahmen unserer Verfahren haben die Werbenden bestritten, gemeinsam mit den jeweiligen Adresshändler:innen verantwortlich zu sein. Die nach Art. 26 DSGVO notwendige Vereinbarung zwischen gemeinsam Verantwortlichen wurde dementsprechend nicht abgeschlossen.

Die Verarbeitung der personenbezogenen Daten zum Zwecke der Bewerbung erfolgte in unseren Beschwerdefällen auch ohne Rechtsgrundlage. Die Werbenden konnten sich nicht auf ein berechtigtes Interesse[3] stützen. Dem berechtigen Interesse steht hier die vernünftige Erwartung der betroffenen Personen entgegen,[4] dass ihre personenbezogenen Daten weder zu Zwecken des Adresshandels monetarisiert werden, noch dass sie ohne vorherigen Kontakt zu dem Werbenden bzw. ohne Freigabe gezielte Werbung erhalten. Im Falle des Landesverbands der Partei ist zusätzlich zu beachten, dass Parteien bei den Meldebehörden eine Wählerauskunft haben, um an Adressdaten von Personen zu gelangen, die überhaupt wahlberechtigt sind,[5] sodass auch in diesem Punkt die Erforderlichkeit des Adresshandels in Frage steht.

Die Partei hat ihr Verfahren nicht weiter betrieben, sodass die Klage als zurückgenommen fingiert wurde. Die Verwarnung ist damit bestandskräftig und bindet die Partei zukünftig. In dem Verfahren des Kulturunternehmens wird eine gerichtliche Entscheidung für das kommende Jahr erwartet. Zwischenzeitlich hat sich auch der

[1] Art. 26 Abs. 1 Satz 1 DSGVO.
[2] EuGH, Urteil vom 10. Juli 2018, C-210/16, Rn. 38.
[3] Siehe Art. 6 Abs. 1 Satz 1 lit. f DSGVO.
[4] Siehe Erwägungsgrund (ErwGr.) 47 DSGVO.
[5] § 50 Abs. 1 Bundesmeldegesetz (BMG).

EuGH mit den Anforderungen der entgeltlichen Weitergabe von personenbezogenen Daten zu Werbezwecken nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO befasst. Der EuGH hat u. a. festgestellt, dass neben der Ermöglichung der Kontrolle der betroffenen Personen über die Offenlegung ihrer Daten auch die „maßgebliche und angemessene Beziehung“[6] dieser zum werbenden Unternehmen eine wichtige Rolle spielt.[7]

In den Klageverfahren vor dem VG Berlin geht es um die gemeinsame Verantwortlichkeit von Werbenden und Adresshändler:innen sowie um die Grenzen des Art. 6 Abs. 1 Satz 1 lit. f DSGVO im Adresshandel und damit um wesentliche datenschutzrechtliche Fragestellungen in diesem Bereich, zu denen wir uns eine Klärung erhoffen. Das Thema Adresshandel begegnet uns als Aufsichtsbehörde aber nicht nur im Bereich der postalischen Werbung. Wir erhalten auch vermehrt Beschwerden, bei denen werbende Unternehmen die E-Mail-Adressdatensätze dritter Unternehmen zur Versendung von Werbe-E-Mails an Verbraucher:innen nutzen. Neben der gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO spielt in diesen Fällen auch eine Rolle, dass E-Mail-Werbung nach § 7 Abs. 2 Nr. 2 Gesetz gegen den unlauteren Wettbewerb (UWG) grundsätzlich einwilligungsbedürftig ist.

2. Die DSGVO in Abgrenzung zur ePrivacy-Richtlinie

Das VG Berlin hat sich mit dem Verhältnis der sog. e-Privacy-Richtlinie[8] zur DSGVO auseinandergesetzt und klargestellt, dass die Zielrichtung des auf der ePrivacy-Richtlinie beruhenden § 7 UWG zwar die Zulässigkeit von Direktwerbung betrifft, die Norm jedoch gerade nicht die Rechtmäßigkeit der Datenverarbeitung regelt.[9] In dem Verfahren hatte eine Verantwortliche gegen eine Verwarnung geklagt, mit der wir die Verwendung von E-Mail-Adressen zu Werbezwecken beanstandet hatten. Die Klägerin hat gegen das Urteil des VG Berlin einen Antrag auf Zulassung zur Berufung gestellt.

Die Klägerin betreibt ein Internetportal zur Anmietung von Ferienunterkünften. Fragten Kund:innen über dieses Portal eine Ferienwohnung bei Vermieter:innen an, speicherte die Betreiberin des Portals die angegebene E-Mail-Adresse und nutzte diese, um Werbung zu verschicken.

[6] ErwGr. 47 Satz 1 und 2 DSGVO.
[7] Siehe EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 51 ff.
[8] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).
[9] VG Berlin, Urteil vom 13. Juni 2022, 1 K 365/20 (nicht rechtskräftig).

Wir verwarnten die Klägerin, weil es an einer Rechtsgrundlage zu dieser Verarbeitung der E-Mail-Adressen fehlte. Die Klägerin reichte vor dem VG Berlin Klage ein und trug vor, dass wir im konkreten Fall gar nicht als Aufsichtsbehörde hätten handeln dürfen, da sich die Frage nach der Zulässigkeit des Versands der Werbe-E-Mails ausschließlich nach den Regelungen der ePrivacy-Richtlinie, also den Regelungen des UWG, richte und nicht nach der DSGVO. Im Übrigen bestünde für eine Direktwerbung an Bestandskund:innen auch ein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

Das VG Berlin sah keinen Anwendungsvorrang der e-Privacy-Richtlinie gegenüber der DSGVO,[10] sondern vertrat die Ansicht, dass vorliegend unterschiedliche Zielrichtungen verfolgt werden: Während Art. 13 ePrivacy-Richtlinie, der in § 7 UWG umgesetzt wurde, den Schutz vor unzumutbarer Belästigung bezweckt, verfolgt Art. 6 DSGVO das Ziel, die Betroffenen vor der unrechtmäßigen Verwendung ihrer personenbezogenen Daten zu schützen.

Das Gericht befand im Weiteren: Eine schriftliche Einwilligung, die mehrere Sachverhalte betrifft – hier die Zustimmung zu den allgemeinen Geschäftsbedingungen der Klägerin – muss entsprechend den Vorgaben der DSGVO so gestaltet sein, dass die Einwilligung in die Verarbeitung personenbezogener Daten von den anderen Sachverhalten klar zu unterscheiden ist.[11] Dies war vorliegend nicht der Fall. Bei Fehlen der nach § 7 Abs. 2 Nr. 2 UWG erforderlichen Einwilligung sei auch ein Rückgriff auf den Erlaubnistatbestand des Art. 6 Abs. 1 Satz 1 lit. f DSGVO (Interessenabwägung) nicht möglich.[12] Es lag auch kein Ausnahmetatbestand nach § 7 Abs. 3 UWG vor. Diese Vorschrift setzt voraus, dass die Kund:innen bei der Erhebung und jeder weiteren Verwendung der Adresse „klar und deutlich“ darauf hingewiesen werden, dass sie der Verwendung jederzeit widersprechen können.[13] Im vorliegenden Fall erfolgte der Hinweis zur Widerspruchsmöglichkeit erst unmittelbar nach einer Eigenwerbung der Klägerin am Ende der Anmeldeseite, sodass er leicht übersehen werden konnte und die vorgenannten Vorgaben des UWG nicht erfüllte.

Die Klägerin hat gegen das Urteil einen Antrag auf Zulassung der Berufung beim Oberverwaltungsgericht

[10] Siehe Art. 95 DSGVO.
[11] Siehe dazu Art. 7 Abs. 2 DSGVO.
[12] Siehe Oberverwaltungsgericht (OVG) Saarlouis, Beschluss vom 16. Februar 2021, 2 A 355/19, Rn. 34.
[13] § 7 Abs. 3 Nr. 4 UWG.

Berlin-Brandenburg gestellt. Eine Entscheidung steht noch aus.

E-Mail-Werbung auf der Grundlage einer pauschalen Zustimmung zu den AGB reicht für eine wirksame datenschutzrechtliche Einwilligung nicht aus: Die Einwilligung in die Verarbeitung personenbezogener Daten muss klar von den anderen Sachverhalten zu unterscheiden sein. Verantwortliche müssen bei E-Mail-Werbung auch im Datenschutzrecht die wettbewerbsrechtlichen Vorgaben aus § 7 Abs. 2 Nr. 2 und Abs. 3 UWG beachten (Einheit der Rechtsordnung), deren Nichteinhaltung zur Unzulässigkeit der Verarbeitung nach Art. 6 Abs. 1 Satz 1 DSGVO führt.

II. Bußgeldentscheidungen

1. Bußgeld wegen Sicherheitslücken in einer Praxismanagementsoftware

Wegen fehlender bzw. fehlerhaft implementierter Maßnahmen für die Gewährleistung eines angemessenen Schutzniveaus haben wir ein Bußgeld in Höhe von 60.000 Euro gegen einen Anbieter verhängt, der eine Plattform für das Management von Arztpraxen, medizinischen Versorgungszentren und Kliniken mit einem zugehörigen Gesundheitsportal zur Patientenkommunikation entwickelt hat und dieses betreibt. Die bei der Entwicklung der Plattformsoftware eingesetzten Mechanismen und Prozesse waren nicht ausreichend bzw. dysfunktional, um mögliche Datenschutz- und Sicherheitsrisiken systematisch abzuprüfen und dadurch Lücken zu detektieren. In der Umsetzung waren die Prozesse daher nicht geeignet, eine Webanwendung nach dem Stand der Technik zu gestalten.

Die Praxismanagementsoftware auf der Plattform des Unternehmens enthielt eine Reihe von Sicherheitslücken:

- Es war angemeldeten Patient:innen möglich, die E-Mail-Zugangsdaten einiger zugeordneter Arztpraxen einzusehen. In der Folge war der E-Mail-Zugang von insgesamt fünf ärztlichen Einrichtungen potenziell kompromittiert.
- Es war angemeldeten Patient:innen möglich, aufgrund fehlender Berechtigungsprüfungen und überflüssiger Softwarekomponenten Registrierungsdaten aller anderen Patient:innen einzusehen, u. a. deren IDs, die IDs der Arztpraxen, häufig E-Mail-Adressen und bei einigen Patient:innen auch deren vollständige Namen und Geburtsdaten. Hiervon waren insgesamt 29.495 Patient:innen mit Accounts im Gesundheitsportal betroffen.

- Bedingt durch die fehlenden Berechtigungsprüfungen waren umfangreiche Datensätze abrufbar, welche u. a. Dokumente aus dem Behandlungskontext, Blutwerte, Diagnosen, Konfigurationen aus den Praxen wie Client-Zertifikate für die Telematikinfrastruktur, Rechnungen sowie Laborergebnisse oder Krankschreibungen enthielten.
- Eine zur Übermittlung von Dokumenten von medizinischen Leistungserbringer:innen an Patient:innen eingesetzte, als Ende-zu-Ende-Verschlüsselung bezeichnete Sicherheitsmaßnahme enthielt einen Programmierfehler. Aufgrund des Fehlers war diese für Angreifer:innen, die den Datenverkehr innerhalb der eingesetzten TLS-Verbindung manipulieren können, für eine sog. Downgrade-Attacke nutzbar. Somit war es unberechtigten Dritten potenziell möglich, die versendeten Dokumente im Klartext einzusehen. Hiervon waren 198 Einrichtungen mit insgesamt 1.623.732 Patient:innen betroffen.

Für die Bußgeldzumessung haben wir die Leitlinien des Europäischen Datenschutzausschusses (EDSA) für die Berechnung von Geldbußen i. S. d. Datenschutz-Grundverordnung (DSGVO)[14] angewendet. Bei der Zumessung berücksichtigten wir, dass mit den Daten Gesundheitsdaten[15] gefährdet waren. Ein tatsächlicher Datenabfluss konnte aber nicht nachgewiesen werden. Bußgeldmindernd wurde eingestuft, dass sich die Verantwortliche in der Zusammenarbeit mit unserer Behörde kooperativ zeigte. Bis zur endgültigen Beseitigung der Sicherheitslücken wurden betroffene Systeme sofort abgeschaltet und ein umfangreicher Katalog an Maßnahmen identifiziert, die das Risiko für das künftige Auftreten gleichartiger Sicherheitslücken wirksam reduzieren sollen. Ebenfalls bußgeldmindernd wurde die zeitnahe Benachrichtigung aller Betroffenen bewertet.

Entwickler:innen und Anbieter:innen webbasierter Anwendungen im Gesundheitsbereich müssen bereits in der Konzeptionsphase systematisch etwaige Datenschutz- und Datensicherheitsrisiken der zu entwickelnden Systeme mitdenken. Hier bietet es sich an, die Methodik des Standard-Datenschutzmodells anzuwenden, um anhand der Gewährleistungsziele die datenschutzrechtlich erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus zu identifizieren. Diese Maßnahmen müssen sowohl während der Entwicklung als auch

[14]EDSA, Leitlinien 4/2022 für die Berechnung von Geldbußen i. S. d. DSGVO, Version 2.1, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_de.
[15]I. S. d. Art. 9 DSGVO.

im laufenden Betrieb implementiert werden, um die Sicherheit der Verarbeitung gerade auch sensibler personenbezogener Daten zu garantieren. Kommt es aufgrund fehlender oder fehlerhaft implementierter Maßnahmen zu Sicherheitslücken, kann dies sanktioniert werden.

2. Missbräuchliche POLIKS-Abrufe

Ein großer Teil unserer Bußgeldverfahren betraf wieder Polizeibeamt:innen, die unbefugt, d. h. zu nichtdienstlichen Zwecken, personenbezogene Daten von Dritten aus den polizeiinternen Datenbanken abgerufen und teilweise auch weiterverwendet haben.

Die Polizei nutzt ihre Datenbank POLIKS 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 bspw. die vollständigen Namen, Geburtsdaten, Anschriften und Informationen zum Familienstand, aber auch Vorstrafen und Zeugenaussagen. 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 für private Zwecke zu nutzen. Dennoch wird der Zugang zu POLIKS immer wieder dazu missbraucht, Daten zu nicht-dienstlichen Zwecken abzufragen.

In diesem Jahr haben wir 50 Verfahren gegen Polizeibeamt:innen eingeleitet und insgesamt 23 Bußgeldbescheide erlassen; u. a. in den folgenden Fällen:

- Eine Polizeibeamtin suchte während einer mehrjährigen Krankheit Dienststellen in Wohnortnähe auf, um dort systematisch Anfragen zu ihrem und dem sozialen Umfeld eines befreundeten Kollegen zu tätigen.
- Ein Polizeibeamter fragte nach Beendigung der Beziehung Daten zu seiner Ex-Freundin sowie diversen ihrer Familienmitglieder in insgesamt 170 Fällen ab.
- Ein Polizeibeamter, der selbst Opfer eines Diebstahls wurde, wollte durch Datenbankabrufe ein durch die brandenburgische Polizei geführtes Ermittlungsverfahren beschleunigen, indem er eigene Ermittlungen über POLIKS vornahm, obwohl er dienstlich für diese Ermittlungen nicht zuständig war.

- Ein Polizeibeamter speicherte die im Rahmen des Polizeidiensts erlangte private Telefonnummer einer Geschädigten, um mit ihr im Nachgang privat in Kontakt zu kommen.
- Ein Polizeibeamter fragte einen Vorgang ab, in dem er selbst als Täter geführt wurde, um so Einfluss auf das Verfahren nehmen zu können.
- Eine Polizeibeamtin stiftete einen Kollegen an, für sie eine private Abfrage zu tätigen.
- Ein Polizeibeamter fragte die Meldeadresse einer Person des öffentlichen Lebens ab, die später durch Dritte Drohschreiben erhielt. Ein Zusammenhang zwischen Drohschreiben und Abruf konnte allerdings nicht nachgewiesen werden.

Die fortwährenden missbräuchlichen Abrufe erfordern ein Gegensteuern durch ein erweitertes Schutzkonzept der Polizei. Auch wenn die bisher aufgedeckten Fälle des missbräuchlichen Datenabrufs im Verhältnis zur Gesamtzahl der polizeilichen Abfragen relativ gering erscheinen mögen, ist davon auszugehen, dass die tatsächliche Zahl der Missbrauchsfälle deutlich höher liegt. Denn die technischen Hürden für einen missbräuchlichen Zugriff sind nach wie vor niedrig und viele unberechtigte Abfragen bleiben vermutlich unentdeckt. Der bisherige Ansatz, Verstößen primär durch eine Anpassung der Weisungslage und verstärkte Kontrollen vorzubeugen, hat sich als unzureichend erwiesen. Mit momentan über 18.000 Bildschirmarbeitsplätzen und knapp 6.700 Mobilgeräten mit POLIKS-Apps[16] ist POLIKS ein komplexes System, bei dem die beschriebenen organisatorischen Maßnahmen allein nicht ausreichen. Stattdessen müssen technische Lösungen in den Vordergrund rücken, die Datenschutzverstöße von vornherein erschweren oder verhindern.

Die Polizei Berlin nimmt die Hinweise der Berliner Beauftragten für Datenschutz und Informationsfreiheit hinsichtlich der missbräuchlichen Nutzung polizeilicher Informationssysteme ernst. Der Schutz personenbezogener Daten hat höchste Priorität. Die Polizei Berlin ist sich der Sensibilität des Umgangs mit personenbezogenen Daten bewusst und verfolgt eine Null-Toleranz-Strategie bei Datenmissbrauch. So verfügt die Polizei Berlin bereits über ein engmaschiges Kontrollsystem. Protokolldaten werden regelmäßig stichprobenartig und anlassbezogen ausgewertet. Bei Verdacht auf Datenschutzverstöße werden bußgeldrechtliche Maßnahmen konsequent eingeleitet. Auch wenn jeder Einzelfall eines unberechtigten Datenabrufs zu Recht kritisch bewertet wird, ist die Anzahl solcher Verstöße im Verhältnis zur Gesamtzahl der POLIKS-Abfragen äußerst gering. Täglich erfolgen zehntausende legitime Datenabfragen durch Berliner Polizeibedienstete im Rahmen ihrer gesetzlichen Aufgaben, zur Gefahrenabwehr, Strafverfolgung und Gefahrenprognose. Die im Jahr 2024 verzeichneten 50 Verdachtsfälle stehen damit in einem deutlich unterproportionalen Verhältnis zur Gesamtzahl von über 23 Mio. POLIKS-Abfragen jährlich. Dies verdeutlicht, dass die weit überwiegende Mehrheit der Mitarbeitenden der Polizei Berlin verantwortungsvoll mit den ihnen zur Verfügung stehenden Daten umgeht. Ein absoluter Schutz gegen missbräuchliche Datenabrufe ist in einem so komplexen System wie POLIKS, das mehreren tausend Mitarbeitenden zur Erfüllung ihrer hoheitlichen Aufgaben zur Verfügung steht, auch bei fortgeschrittenen technischen Schutzmaßnahmen nicht realistisch umsetzbar.

[16]Siehe Abgeordnetenhaus von Berlin, Schriftliche Anfrage vom 30. Januar 2024, Abghs.-Drs. 19/18090.

Konkret sollten automatisierte Plausibilitätsprüfungen bei Datenabfragen implementiert werden, die ungewöhnliche Zugriffsmuster erkennen und bspw. bei gehäuften Abfragen zu einer Person automatisch Warnungen auslösen. Die Zugriffskontrolle sollte durch kürzere Abmeldefristen und eine durchgängige Zwei-Faktor-Authentifizierung an allen Arbeitsplätzen verschärft werden. Zudem ist eine dynamische Steuerung der Zugriffsrechte nötig – etwa durch temporäre Rechtevergaben nur für konkrete Vorgänge oder Inhalte und durch einen automatischen Rechteverfall nach Abschluss der Bearbeitung. Wir stehen dazu inhaltlich mit der Polizei im Austausch und mahnen strenge Maßstäbe u. a. bei Vor-Ort-Kontrollen an.

Unberechtigten Datenabrufen in POLIKS muss durch geeignete technische Maßnahmen wie Plausibilitätsprüfungen, kurze Abmeldefristen und Zwei-Faktor-

Die Polizei Berlin hat in den vergangenen Jahren kontinuierlich technisch-organisatorische Maßnahmen zum Schutz der in POLIKS gespeicherten Daten weiterentwickelt. Diese Maßnahmen wurden regelmäßig in enger Abstimmung mit der Berliner Beauftragten für Datenschutz und In-formationsfreiheit getroffen. So sind unter anderem umfangreiche Datenschutzkontrollen sowie Schulungs-/Sensibilisierungsmaßnahmen, wie die Anpassung der jährlichen Belehrung um die Unzulässigkeit von Selbstabfragen verbindlicher Bestandteil der internen Prozesse und sind laut einer Vergleichsringabfrage aus dem Jahr 2022 überdurchschnittlich umfangreicher. Die technisch-organisatorischen Maßnahmen werden dennoch stetig evaluiert und ggf. angepasst. Ebenso werden die von der Berliner Beauftragten für Datenschutz und Informationsfreiheit vorgeschlagenen Maßnahmen geprüft.

Einzelfälle lassen sich trotz dieser umfassenden organisatorischen, technischen und sanktionierenden Vorkehrungen nicht vollständig verhindern. Es ist wichtig, bei der Weiterentwicklung von Schutzkonzepten auch die Funktionsfähigkeit der Polizei nicht zu beeinträchtigen. Zu rigide technische Zugangshürden, wie etwa zu kurze Abmeldefristen, restriktive Rechtevergabe oder dauerhafte Zweifaktor-Authentifizierung im Streifen- und Einsatzdienst, können im Einsatzfall zu Verzögerungen führen, die gerade in Gefahrenlagen gravierende Auswirkungen haben können. Eine umfassende verantwortungsvolle Sicherheitsarchitektur in dem Zusammenhang muss daher sowohl Datenschutz als auch Einsatzrealität berücksichtigen.

Authentifizierung vorgebeugt werden. Wo diese Maßnahmen an ihre Grenzen stoßen, muss eine konsequente Sanktionierung greifen. Dazu gehören die systematische Aufdeckung von Verstößen durch automatisierte Auswertung der Protokolldaten und wirksame Stichprobenkontrollen. Einschränkungen der Zugriffsrechte für die Dauer der Überprüfung von Verdachtsfällen sollten dabei stets erwogen werden.

3. Kammergericht nach EuGH-Urteil: Sofortige Beschwerde im Verfahren gegen Deutsche Wohnen SE erfolgreich

Der Europäische Gerichtshof (EuGH) hatte im letzten Jahr unsere Aufsichtspraxis bestätigt und festgestellt, dass datenschutzrechtliche Bußgelder direkt gegen Unternehmen festgesetzt werden können. Laut EuGH haftet das Unternehmen auch für Verstöße, die von Personen begangen wurden, die im Rahmen der unternehmerischen Tätigkeit und im Namen dieser juristischen Person gehandelt haben.[17] Dieser Ansicht ist nun auch das Kammergericht (KG Berlin) gefolgt.[18] Dem Rechtsstreit liegt ein Bußgeldbescheid in Höhe von insgesamt 14,5 Mio. Euro zugrunde, den wir 2019 gegen die Deutsche Wohnen SE erlassen haben. Mit dem Beschluss des Kammergerichts wurde die Sache jetzt zu neuer Entscheidung an das Landgericht Berlin (LG Berlin) zurückverwiesen.

Das LG Berlin hatte 2021 unser Bußgeldverfahren gegen die Deutsche Wohnen SE wegen eines Verfahrenshindernisses eingestellt. Das Gericht ging davon aus, dass unsere Vorgehensweise – auch ohne eine konkrete Handlung von Leitungspersonen oder gesetzlichen Vertreter:innen darzulegen –, unmittelbar gegen die juristische Person als Betroffene (in diesem Fall die Deutsche Wohnen SE) vorzugehen, vom deutschen Ordnungswidrigkeitenrecht nicht gedeckt sei. Nachdem Rechtsmittel eingelegt wurden, hatte das Kammergericht das Verfahren ausgesetzt und Fragen zur Auslegung der DSGVO dem EuGH vorgelegt. Nach Durchführung des Vorabentscheidungsverfahrens und nach dem Urteil des EuGH hat das Kammergericht den Einstellungsbeschluss des LG Berlin nun aufgehoben.

Im Einklang mit der EuGH-Rechtsprechung[19] stellte das Kammergericht fest, dass die Deutsche Wohnen SE als juristische Person taugliche Adressatin eines Bußgeldbe-scheides sein und als solche unmittelbar und nicht nur als Verfahrens- oder Nebenbeteiligte bebußt werden kann.[20]

[17] EuGH, Urteil vom 5. Dezember 2023, C-807/21, Rn. 44.
[18] KG Berlin, Beschluss vom 22. Januar 2024, 3 Ws 250/21, 3 Ws 250/21 – 161 AR 84/21.
[19] Siehe JB 2023, A.II.1.
[20] KG Berlin, Beschluss vom 22. Januar 2024, 3 Ws 250/21, 3 Ws 250/21 – 161 AR 84/21, Rn. 6.

Darüber hinaus stellte das Kammergericht klar, dass der Bußgeldbescheid die gesetzlichen Wirksamkeitsvoraussetzungen[21] erfüllt. Im Bescheid seien die Vorwürfe „ausgesprochen konkret und ausführlich“ sowie die Tathandlungen „bemerkenswert und – gemessen an den vom EuGH formulierten materiell-rechtlichen Haftungsvoraussetzungen ersichtlich – überobligatorisch konkret“ dargestellt worden.[22] Der Rechtsstreit über den Bußgeldbescheid wird nun beim LG Berlin weitergeführt. Dort wird die zuständige Kammer für Bußgeldsachen über den Einspruch der Deutsche Wohnen SE entscheiden.

Ist ein Datenschutzverstoß einer juristischen Person zurechenbar, muss der Bußgeldbescheid nicht bezeichnen, welche identifizierte natürliche Person gehandelt hat. Bußgeldverfahren können dann regelmäßig unmittelbar gegen die Unternehmen als Betroffene geführt werden, selbst wenn Leitungspersonen von dem konkreten Handeln ihrer Mitarbeitenden keine Kenntnis hatten.

4. Entscheidung des Landgerichts Berlin: Das Ignorieren einer Verwarnung kann sich bußgelderhöhend auswirken

Im Jahr 2022 hatten wir ein Bußgeld gegen ein Unternehmen wegen eines Interessenskonflikts eines betrieblichen Datenschutzbeauftragten innerhalb der Konzernstruktur eines E-Commerce-Konzerns verhängt.[23] Die Person des betrieblichen Datenschutzbeauftragten war zugleich Geschäftsführer von zwei Dienstleistungsgesellschaften, die im Auftrag desjenigen Unternehmens personenbezogene Daten verarbeiteten, für welches er als Datenschutzbeauftragter benannt war. Diese von ihm geführten Dienstleistungsgesellschaften waren ebenfalls Teil des Konzerns, kümmerten sich um den Kundenservice und bearbeiteten die Bestellungen.

Das Unternehmen hatte Einspruch gegen unseren Bußgeldbescheid eingelegt. Das LG Berlin hat sich nun mit dem Fall befasst und in seiner Entscheidung[24] zur Bemessung der Bußgeldhöhe Folgendes ausgeführt: Das LG Berlin schätzt die Schwere des von uns festgestellten Verstoßes anders als wir als gering ein, da keine besonders sensi-blen Daten von dem Interessenskonflikt berührt waren. Betroffen waren nur allgemeine Kontaktdaten wie Namen, Adresse, Telefonnummer und E-

[21] Siehe § 66 Ordnungswidrigkeitengesetz (OWiG).
[22] KG Berlin, Beschluss vom 22. Januar 2024, 3 Ws 250/21, 3 Ws 250/21 – 161 AR 84/21, Rn. 13, 15.
[23] Siehe JB 2022, 12.5.
[24] LG Berlin, Urteil vom 8. Juli 2024, (519 OWi LG) 214 Js 1/24 OWi (6/24).

Mail-Adresse, die von der Tochtergesellschaft im Auftrag des bebußten Unternehmens verarbeitet wurden.

Auch bezog sich das LG Berlin bei der Festlegung der Höhe des Bußgeldes auf eine vom LG Bonn getroffene Entscheidung[25]. So führte das LG Berlin aus, dass der Umsatz des Konzernverbunds als Bemessungsgröße bei einer, wie im vorliegenden Fall, eher geringen Schwere des Verstoßes eine nur untergeordnete Rolle spielt. Damit eine Geldbuße wirksam, abschreckend und verhältnismäßig ist,[26] genügt es daher nach Auffassung des LG Berlin, dass die Nichtbeachtung der verletzten Vorschrift – aus Sicht des bebußten Unternehmens – aufgrund der angesetzten Summe gegenüber einem regelkonformen Verhalten als unwirtschaftlich erscheint.

Das LG Berlin hat allerdings den Umstand, dass unsere Behörde zuvor eine Verwarnung ausgesprochen hatte und dass trotz des darin enthaltenen ausdrücklichen rechtlichen Hinweises der Zustand nicht geändert wurde, schließlich bußgelderhöhend nach Art. 83 Abs. 2 e und i DSGVO gewertet.

Andauernde oder wiederholte Verstöße gegen datenschutzrechtliche Vorgaben können ein Zeichen für systematische Mängel sein, die eine (höhere) Geldbuße erfordern. Die Entscheidung des LG Berlin unterstreicht die Aufgabe von Unternehmen, Hinweisen und bestandskräftigen Abhilfemaßnahmen der Aufsichtsbehörden nachzukommen.

III. Informationsfreiheit

1. Anträge nach dem Informationsfreiheitsgesetz – Erhebung einer Postadresse

Das Bundesverwaltungsgericht (BVerwG) hat in einem Urteil festgestellt: Das Informationsfreiheitsgesetz des Bundes (IFG Bund) setzt voraus, dass die Behörde Kenntnis von der Identität desjenigen hat, der einen Antrag auf Informationszugang stellt. Zur Klärung der Identität darf die Behörde die Postanschrift des Antragstellers erheben, ohne dass darin ein Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) zu sehen ist.

Zunächst ist darauf hinzuweisen, dass Rundschreiben nicht unter § 18 Absatz 2 Satz 3 Berliner Informationsfreiheitsgesetz (IFG) fallen, sondern lediglich empfehlenden Charakter haben. Sie dienen der fachlichen Steuerung eines einheitlichen Verwaltungshandelns.

Dem Verfahren liegt eine Klage des Bundesministeriums des Inneren und für Heimat (BMI) gegen eine Verwarnung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zugrunde.[27] Hin-

Die Bedenken der Berliner Beauftragten für Datenschutz und Informationsfreiheit werden nicht geteilt. Grundsätzlich löst die Stellung eines IFG-Antrags ein Verwaltungsverfahren aus, in dem die an-

[25] LG Bonn, Urteil vom 11. November 2020, 29 OWi 1/20.
[26] I. S. d. Art. 83 Abs. 1 DSGVO.
[27] BVerwG, Urteil vom 20. März 2024, 6 C 8.22.

tergrund war eine Vermittlungsbitte eines Antragstellers, der beim BMI einen IFG-Antrag per E-Mail über die Plattform FragDenStaat gestellt hatte. Für die Beantwortung bestand das BMI auf der Übermittlung der Postanschrift und einer persönlichen E-Mail-Adresse des Antragstellers. Nach Übersendung der geforderten Daten teilte es dann per Post mit, dass keine Informationen zu der Anfrage vorliegen.

Laut BVerwG lag hier kein Datenschutzverstoß vor. Die mit der Verarbeitung der Postanschrift einhergehenden Datenverarbeitungsvorgänge seien rechtmäßig gewesen, da sie für eine Aufgabe erforderlich gewesen seien, die im öffentlichen Interesse liege und dem Verantwortlichen übertragen worden sei,[28] namentlich der ordnungsgemäßen Bearbeitung der Bekanntgabe der abschließenden Entscheidung.[29] Die erforderliche Rechtsgrundlage für die Verarbeitung[30] sei in diesem Fall § 3 Bundesdatenschutzgesetz (BDSG) i. V. m. den Regelungen des IFG Bund.[31] Zwar gebe es keine ausdrückliche Rechtsgrundlage zur Klärung der Identität des Antragsstellers im IFG Bund. Aus § 7 Abs. 1 IFG Bund lasse sich aber ableiten, dass zur sachgerechten Bearbeitung eines Antrags ersichtlich sein müsse, wer den Antrag stellt.[32] Diese Schlussfolgerung ergebe sich aus dem vom IFG Bund vorgesehenen Prüfprogramm und zur Sicherstellung der Vollstreckung möglicher Gebühren.[33] Das Gericht verweist zudem auf die Gesetzesbegründung, nach der die Behörde „im Einzelfall […] die Identität des Antragstellers feststellen können" müsse.[34]

Die Informationsfreiheitsbeauftragten der Länder stellten im Rahmen der Konferenz der Informationsfreiheitsbeauftragten (IFK) zu der Entscheidung fest, dass die Erwägungen aus einem dort betreffenden Einzelfall (Bereich Bund) aufgrund der heterogenen Gesetzeslage nicht auf alle Länder übertragbar sind. Unabhängig davon waren sich die Informationsfreiheitsbeauftragten der Länder einig, dass durch die Formalisierung des Verfahrens, standardmäßig Postanschriften anzufordern, deutlich mehr Verwaltungsaufwand auch bei eintragstellende Person als Beteiligte gemäß § 1 Absatz 1 des Gesetzes über das Verfahren der Berliner Verwaltung i. V. m. § 13 Absatz 1 Nummer 1 Verwaltungsverfahrensgesetz (VwVfG) und § 3 Absatz 1 Satz 1 IFG identifizierbar sein muss. Anonyme Verwaltungsverfahren sind dem deutschen Verwaltungsrecht fremd.

Aus verfahrensökonomischen Gründen ist zudem die Angabe einer Anschrift erforderlich. Nur so kann die Behörde sicherstellen, dass Anträge von realen Personen gestellt werden und Gebührenbescheide wirksam zugestellt werden können. Wer gegenüber dem Staat Transparenz geltend macht und Auskünfte verlangt, sollte selbst nicht intransparent sein. Der Schutz personenbezogener Daten wird gewahrt; eine generelle Zulassung anonymer Anträge ist daraus jedoch nicht abzuleiten – insbesondere nicht bei Verfahren mit Drittbeteiligung.

Die früher umstrittene Fragestellung der Zulässigkeit einer Verarbeitung des Namens und der Postanschrift der antragstellenden Person ist durch die im Rundschreiben Nr. 1/2024 der Senatsverwaltung für Inneres und Sport vom 8. August 2024 zitierte Entscheidung des Bundesverwaltungsgerichts klar und eindeutig beantwortet. Dies gilt auch für das IFG des Landes Berlin. Die Offenlegung der Identität der antragstellenden Person widerspricht auch nicht dem mit dem IFG angestrebten Grundsatz eines bürgerfreundlichen Verfahrens. Vielmehr wird dieser umso eher verwirklicht, wenn die Behörde rechtssicher erkennen kann, mit wem sie tatsächlich kommuniziert.

Auch unter haushaltsrechtlichen Gesichtspunkten ist es unzumutbar, ein gebührenpflichtiges Verfahren einzuleiten, wenn die Identität des Gebührenschuldners unklar bleibt.

[28] Siehe Art. 6 Abs. 1 Abs. 1 Satz 1 lit. e DSGVO.
[29] BVerwG, Urteil vom 20. März 2024, 6 C 8.22, Rn. 55 ff.
[30] Siehe Art. 6 Abs. 1 Abs. 1 lit. e, Abs. 3 Satz 1 lit. b DSGVO.
[31] BVerwG, Urteil vom 20. März 2024, 6 C 8.22, Rn. 25 ff.
[32] Ebd., Rn. 57.
[33] Ebd., Rn. 58.
[34] Ebd., Rn. 59 mit Verweis auf BT-Drs. 15/4493, S. 14.

fach zu beantwortenden Offenlegungsanträgen entstehen kann. Sie werden die informationspflichtigen Stellen weiterhin dahingehend beraten, Anträge niedrigschwellig, informationsfreundlich und damit unbürokratisch zu bearbeiten.

Auch für Berlin kann festgestellt werden, dass das Urteil des BVerwG, das sich auf das IFG Bund bezieht, nicht ohne Weiteres auf das Berliner Informationsfreiheitsgesetz (IFG) übertragbar ist. Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Erfüllung des Informationszugangs ist in Berlin § 4a IFG und nicht § 3 BDSG in Verbindung mit den Regelungen des IFG Bund, wie es Gegenstand des Urteils des BVerwG war. Der Gesetzesbegründung zum IFG Berlin ist keinerlei Hinweis zu entnehmen, der eine allgemeine Pflicht zur Anforderung von Postadressen zur Identitätsfeststellung vor Antragsbearbeitung stützen könnte. Vielmehr betont die Begründung des Gesetzentwurfs die bürgerfreundliche Ausgestaltung des Verfahrens.

Richtigerweise gibt es Fälle, in denen eine Identifizierung von Antragstellenden auch mit Postadresse notwendig sein kann. In vielen Fällen wird dies aber nicht der Fall sein. Soweit es nicht erforderlich ist, werden wir daher weiterhin bei unserer Vermittlungstätigkeit sowie bei IFG-Anträgen an unser eigenes Haus darauf hinwirken, dass auf die Erfassung der Postadresse verzichtet wird, um eine bürgerfreundliche Bearbeitung zu gewährleisten. Damit wird auch verhindert, dass selbst bei einfach zu beantwortenden Offenlegungsanträgen deutlich mehr Verwaltungsaufwand entsteht.

Dem Haushaltsinteresse kann im Übrigen auch auf anderem Wege Rechnung getragen werden. So können Behörden von der Möglichkeit Gebrauch machen, dass Kosten bereits im Voraus beglichen werden.[35] Im Rahmen unserer IFG-Vermittlungstätigkeit werden wir anderen informationspflichtigen Stellen in Berlin empfehlen, sich an diesen Maßstäben zu orientieren und im Rahmen des eingeräumten Ermessens für eine bürgerfreundliche Bearbeitung zu entscheiden.

Diese Einschätzung teilten wir auch der Senatsverwaltung für Inneres und Sport mit, die – ohne uns als für die IFG-Kontrolle zuständige Behörde einzubinden – in einem Rundschreiben an verschiedene Behörden vor dem Hintergrund des Urteils des BVerwG Hinweise „zur Verarbeitung des Namens und der Postanschrift der antragstellenden Person als personenbezogenes Datum nach § 4a IFG Berlin“ gegeben hatte. Darin weist die Innenverwaltung darauf hin, dass eine Erhebung

[35] Siehe z. B. § 17 Gesetz über Gebühren und Beiträge Berlin (GebBtrG BE).

der Postadresse möglich sei, macht aber nicht auf die Möglichkeit einer informationsfreundlicheren und unbürokratischeren Bearbeitung aufmerksam. Wir teilten der Senatsverwaltung mit, dass nach unserer Auffassung ein Name und eine E-Mail-Adresse ausreichend sein kann, um einen IFG-Antrag zu bearbeiten, und auch keine zwingende Verknüpfung von „Name und Postanschrift“ bei der Identitätsfeststellung erforderlich ist. Bei der Senatsverwaltung haben wir einen Austausch in der Sache angeregt und unsere Unterstützung bei der Anpassung des Rundschreibens angeboten.

Das Urteil des BVerwG bezieht sich auf das IFG Bund und nicht auf die Regelungen im IFG Berlin. Der Gesetzesbegründung zum IFG Berlin ist keinerlei Hinweis zu entnehmen, der eine allgemeine Pflicht zur Anforderung von Postadressen zur Identitätsfeststellung vor Antragsbearbeitung stützen könnte. Wir werden weiterhin grundsätzlich keine Postanschrift für die IFG-Antragsstellung fordern, wenn dies zur weiteren Bearbeitung nicht erforderlich ist. Eine Erforderlichkeit kann bspw. gegeben sein, weil eine antragstellende Person nicht von der Möglichkeit Gebrauch machen möchte, Kosten bereits im Voraus zu begleichen, und daher die Zustellung eines Gebührenbescheids erforderlich ist. Oder es bestehen Zweifel an der Identität einer antragstellenden Person, aber die zweifelsfreie Feststellung ist im Einzelfall zur Prüfung von Ausschlussgründen (bspw. zum Schutz von personenbezogenen Daten Dritter) erforderlich. Im Rahmen der Vermittlungstätigkeit werden wir anderen informationspflichtigen Stellen in Berlin ebenfalls empfehlen, sich im Rahmen ihres Ermessens für eine bürgerfreundliche Bearbeitung der Anträge ohne Erhebung der Postanschrift zu entscheiden.

2. Gemeinsam die Informationsfreiheit und das Transparenzrecht stärken

Sinn und Zweck des IFG ist neben der Kontrolle staatlichen Handelns auch die Förderung der demokratischen Meinungs- und Willensbildung.[36] Zivilgesellschaftliche Organisationen spielen dabei eine wichtige Rolle. Um dem Rechnung zu tragen und voneinander zu lernen, organisierten wir ein Auftakttreffen mit zivilgesellschaftlichen Organisationen zum Meinungsaustausch über die Informationsfreiheit und das Transparenzrecht.

Mit Vertreter:innen von Mehr Demokratie e. V., der Open Knowledge Foundation Deutschland e. V. und der Regionalgruppe Berlin-Brandenburg von Transparency International Deutschland e. V. diskutierten wir dabei auf Fachebene über folgende Themen:

[36] § 1 IFG.

- die bereits seit Längerem angedachte Weiterentwicklung des Berliner Informationsfreiheitsgesetzes zu einem Transparenzgesetz
- das Thema Aktenführung bei Behörden
- die auch im vorliegenden Jahresbericht thematisierte Entscheidung des BVerwG zur Datenverarbeitung der Anschrift von Antragstellenden nach dem IFG Bund[37]

Ebenfalls diskutierten wir über unsere Erfahrungen in der Bildungsarbeit mit Kindern und Jugendlichen im Bereich Datenschutz und Informationsfreiheit. Durch dieses Auftakttreffen konnten wir wichtige Impulse für unsere Arbeit mitnehmen. Um das kollektive Wissen verschiedener Akteur:innen noch besser nutzen zu können, wünschen wir uns für die Zukunft eine Erweiterung des Kreises der Teilnehmenden.

Die Weiterentwicklung und das Wirksamwerden von Informationsfreiheit und Transparenzrecht kann nur mit einem lebendigen Austausch verschiedener Gruppen gelingen. Wir sind offen für Ideen aus der Zivilgesellschaft und von anderen Akteur:innen. Langfristig ist ein regelmäßiger Informationsaustausch angedacht, sowohl mit Vertreter:innen der Zivilgesellschaft als auch mit anderen Stakeholdern in diesem Bereich, die sich in Berlin für die Informationsfreiheit und das Transparenzrecht einsetzen.

3. Schnelle Bearbeitung von IFG-Anträgen

In diesem Jahr ist es uns ein besonderes Anliegen, auf ein Thema aufmerksam zu machen, das uns auch nach 25 Jahren der Geltung des IFG im Land Berlin immer wieder beschäftigt. Es handelt sich um Schwierigkeiten bei der Umsetzung der gesetzlich normierten Pflicht, über IFG-Anträge unverzüglich zu entscheiden.[38]

Gemäß § 14 Absatz 1 Satz 1 Berliner Informationsfreiheitsgesetz (IFG) ist über einen Antrag auf Akteneinsicht oder Aktenauskunft unverzüglich zu entscheiden (d. h. ohne schuldhaftes Zögern). Nach § 15 Absatz 5 IFG muss eine ablehnende Entscheidung innerhalb von zwei Wochen nach Antragstellung erfolgen. Die Frist gilt nicht, wenn der Antrag positiv beschieden werden soll oder erst eine Anhörung stattfinden muss.

Unverzüglich bedeutet „ohne schuldhaftes Zögern“.[39] Dies erfordert ein Tätigwerden innerhalb einer nach den Umständen des Einzelfalls zu bemessenden zumeist kurzen Prüfungs- und Überlegungsfrist.[40]

Jeder antragstellenden Person ist zum frühestmöglichen Zeitpunkt der Hinweis auf die Gebührenpflichtigkeit und die voraussichtliche Größenordnung zu geben.

Daher müssen sich Verwaltungen nach Eingang unmittelbar mit einem IFG-Antrag befassen. Regelmäßig bedeutet dies, sich der Bitte um Kostenvorabinformation

Diese Grundsätze sind in der Berliner Verwaltung bekannt und sie werden auch regelmäßig angewendet. Der Berliner Senat kann jedoch nicht vollständig ausschließen, dass es in Einzelfällen und aus

[37] Siehe A.III.1.
[38] Siehe § 14 Abs. 1 Satz 1 IFG.
[39] Legaldefinition in § 121 Abs. 1 Satz 1 BGB.
[40] Siehe § 14 Abs. 1 Satz 2 IFG.

anzunehmen, die inzwischen standardmäßig in Anträgen formuliert wird. Naheliegenderweise ist hierzu erforderlich, dass zunächst der Umfang der angefragten Informationen hausintern geklärt wird, woraufhin eine realistische, aber nicht prohibitiv wirkende Kostenschätzung vorzunehmen ist. Nach Kostenübernahmeerklärung der antragstellenden Person ist mit der detaillierten Prüfung der gewünschten Dokumente auf mögliche IFG-Ausschlusstatbestände[41] zu beginnen und ggf. Anhörungsverfahren mit -Betroffenen durchzuführen.[42] Kann über einen Antrag nicht schon innerhalb von zwei Wochen abschließend entschieden werden, sollte der antragstellenden Person eine Eingangsbestätigung geschickt werden.[43]

Die Wirklichkeit der Berliner Verwaltung sieht häufig anders aus. Das merken wir an den Beschwerden, die wir wegen zögerlicher Bearbeitung erhalten und bei denen wir tätig wurden; manchmal unter Hinweis auf eine drohende Untätigkeitsklage[44] gegen das Land Berlin, die es zu vermeiden gilt. So erhielten Beschwerdeführer:innen nach Antragstellung von informationspflichtigen Stellen über einen längeren Zeitraum keine Antwort, z. T. trotz Erinnerungen auch keine Eingangsbestätigung. Eine späte Antwort begründete eine Verwaltung bspw. mit „der seit längerer Zeit anhaltenden hohen Arbeitsbelastung im Zusammenhang mit der Digitalisierung im Öffentlichen Gesundheitsdienst“. In einer weiteren Antwort, die eine Verwaltung nach unserer Intervention dem Beschwerdeführer ca. sieben Wochen nach Antragstellung schickte, wurde um mehr Zeit für die Prüfung gebeten. Es würde versucht, sich nach den Urlaubstagen zeitnah darum zu kümmern.

Es zeigt sich insgesamt, dass die Bearbeitung von IFG-Anträgen in einigen Verwaltungen noch immer hintangestellt und nicht als eigenständige öffentliche Aufgabe verstanden wird. In einem Fall wurde ein Antrag sogar ausdrücklich als belästigend tituliert.[45] Trotz angespannter Personalsituation darf nicht verkannt werden, dass angefragte Behörden grundsätzlich gehalten sind, sich in ihrer Arbeitsorganisation und Aktenführung auf die mit der Erfüllung von IFG-Anträgen verbundenen Aufgaben einzustellen. Die Bearbeitung solcher Anträge sollte im Land Berlin 25 Jahre nach Inkrafttreten des Gesetzes von 1999 als originäres Aufgabengebiet

unterschiedlichen Ursachen zu Verzögerungen bei der Bearbeitung von IFG-Anträgen kommt. Dabei ist zu berücksichtigen, dass die Bearbeitung von Anträgen auf Aktenauskunft und Akteneinsicht häufig äußerst komplexe tatsächliche und rechtliche Prüfungen und Beteiligung von anderen Stellen und Dritten auslöst, so dass eine Entscheidung innerhalb von nur 14 Tagen rein faktisch auf Grenzen stößt, auch weil andere nicht minder wichtige Aufgaben und Rechtsansprüche nicht zurückgestellt werden können. Die Berliner Behörden sind jedoch stets bemüht, die Frist einzuhalten.

[41] §§ 6 ff. IFG.
[42] § 14 Abs. 2 IFG.
[43] § 33 Abs. 1 Gemeinsame Geschäftsordnung der Berliner Verwaltung – Allgemeiner Teil (GGO I).
[44] § 75 VwGO.
[45] Vom Landesamt für Flüchtlingsangelegenheiten anlässlich einer Anfrage zur Vereinbarung mit Bulgarien über die Rücknahme von Geflüchteten.

von den informationspflichtigen Stellen betrachtet und behandelt werden.[46]

Die Behörden, insbesondere deren Leitungen, müssen ihre Organisations- und Personalstrukturen so ausrichten, dass sie neben ihren eigentlichen Sachaufgaben auch die gesetzlichen Pflichten nach dem IFG erfüllen können. Verfahrensabläufe können gerade in großen Verwaltungen dadurch gestrafft werden, dass IFG-Anträge nicht an die allgemeinen Poststellen, sondern an eigens eingerichtete Funktionsadressen geschickt werden, die im Internetangebot der informationspflichtigen Stellen abrufbar sind.

4. Akteneinsicht in bezirkliche Bauakten

In diesem Jahr erreichten uns mehrere Beschwerden, weil einige Bezirke die nach dem IFG beantragten Akteneinsichten in Bauakten abgelehnt oder von nicht IFG-konformen Voraussetzungen abhängig gemacht hatten. In den Verfahren zeigten sich erhebliche Unsicherheiten bei der Anwendung des IFG.

So beantragte eine Person den Zugang zu Informationen aus historischen Bauakten im Bezirksamt Steglitz Zehlendorf. Das Interesse galt der Zeit von 1930 bis 1940 und bezog sich auf die Klärung von Baujahr, historischen Adressen und Bauherren von zunächst 30 Gebäuden. Das zuständige Amt verlangte vor einer Einsichtnahme in die archivierten Grundstücksakten standardmäßig die Vorlage einer Vollmacht der aktuellen Eigentümerin bzw. des aktuellen Eigentümers; wer das jeweils war, war der antragstellenden Person nicht bekannt. Später stellte sich heraus, dass die gewünschten Informationen den jeweiligen Baugenehmigungen zu entnehmen waren. Wir konnten das Amt davon überzeugen, dass die Beibringung von Vollmachten bzw. Anhörung der Betroffenen nicht erforderlich ist, und begründeten dies unter Bezugnahme auf die neuere Rechtsprechung zu Umweltinformationen. Zu solchen Informationen gehören grundsätzlich Baugenehmigungen für Gebäude, weil mit ihnen eine Baumaßnahme freigegeben wird, die sich aufgrund der Versiegelung des Bodens wahrscheinlich nachteilig auf die Umwelt auswirkt.[47] Dass durch die Offenbarung der 80 bis 90 Jahre alten Baugenehmigungen Interessen von aktuellen Eigentümerinnen oder Eigentümern erheblich beeinträchtigt würden, war fernliegend. Deshalb handelte es sich nicht um geschützte Informationen, sodass die

[46]Siehe auch BVerwG, Urteil vom 17. März 2016, 7 C 2.15, Rn. 24 (betr. IFG Bund von 2005).
[47]Bayerischer Verwaltungsgerichtshof (BayVGH), Urteil vom 20. Dezember 2022, 5 B 22.1532, Rz. 25, 27, auch unter Bezugnahme auf die neuere Rechtsprechung des BVerwG.

Anhörung der vorgenannten Personen entfiel.[48] Die antragstellende Person konnte schließlich die Akteneinsichten vor Ort gebührenfrei wahrnehmen.[49]

Ein weiterer Fall im Bezirksamt Steglitz-Zehlendorf betraf Informationen zu einer Baugenehmigung für den Dachgeschossausbau in einem denkmalgeschützten Gebäude. Das Amt teilte der antragstellenden Person mit, dass sie entweder die Vollmacht der Grundstückseigentümerin (eine GmbH) vorlegen oder das Amt die Anhörung der GmbH durchführen müsse. Wir haben dem Amt mitgeteilt, dass hier personenbezogene Daten nicht berührt sind und demzufolge eine Anhörung der GmbH allenfalls wegen schützenswerter Betriebs- oder Geschäftsgeheimnisse[50] durchzuführen wäre. Da auch solche nicht begründet werden konnten, erhielt die antragstellende Person schließlich die beantragten Kopien der den Bau betreffenden Dokumente.

Im Bezirksamt Treptow-Köpenick hatte eine Person Einsicht in die Baugenehmigung des Nachbarn beantragt. Der Informationszugang war zunächst gestattet und ein Termin zur Einsichtnahme vereinbart worden. Zu dem Bauvorhaben gehörte der Bau einer Tiefgarage mit vermuteten Auswirkungen auf den Grundwasserspiegel. Die antragstellende Person befürchtete dadurch Beschädigungen des Mauerwerks des eigenen Gebäudes und sah sich durch vom Bauherrn angebrachte sog. Rissmarker darin bestärkt. Da der Bauherr nach Anhörung die Zustimmung zur Einsichtnahme verweigerte, wurde der diesbezüglich anberaumte Termin vom Amt kurzfristig aufgehoben. Die antragstellende Person erhielt jedoch später alle gewünschten Informationen, einschließlich derjenigen von der Wasserbehörde. Eine erhebliche Beeinträchtigung der Interessen des Bauherrn durch die Offenlegung der personenbezogenen Informationen war nicht erkennbar.

Einige Unruhe wurde im Bezirksamt Mitte verursacht, weil dort ein Papier kursierte, mit dem der Umgang mit Anträgen von Studierenden auf Akteneinsicht in Bauakten festgelegt werden sollte. Danach war Voraussetzung für die Bearbeitung u. a. ein von der betreuenden Professorin bzw. dem betreuenden Professor unterzeichnetes Schreiben der Hochschule, das etwa Angaben zur Matrikelnummer der bzw. des Studierenden und Angaben zum Thema der Studienarbeit als Nachweis des berechtigten Interesses enthalten sollte. Sofern ein solches Schreiben beigebracht wurde, sollte auf die Anhörung der jeweiligen Grundstückseigentümerin oder des jeweiligen Grundstückseigentümers

[48] Siehe § 18 a Abs. 1 IFG i. V. m. § 9 Abs. 1 Satz 1 Nr. 1 und Satz 3 Umweltinformationsgesetz (UIG).
[49] Siehe § 18 a Abs. 4 Satz 3 Nr. 1 IFG.
[50] § 7 IFG.

verzichtet werden. Diese Voraussetzungen waren aus dem IFG nicht herleitbar. Auch war keine Rechtsgrundlage für die Verarbeitung von für den Antrag nicht erforderlichen personenbezogenen Daten der antragstellenden Studierenden erkennbar. Wir haben das Amt daher gebeten, das Verfahren in der Praxis nicht anzuwenden.

Eine Person begehrte vom Bezirksamt Charlottenburg-Wilmersdorf Informationen zu mehreren Werbeanlagen, die in einem Fall auf einem Privatgrundstück, im zweiten Fall im öffentlichen Straßenland angebracht waren. Im ersten Fall ging es um eine Baugenehmigung, für die das Stadtentwicklungsamt zuständig ist. Die Akteneinsicht im Bauaktenarchiv wurde zunächst davon abhängig gemacht, dass die antragstellende Person ein Formular ausfüllt, in dem zutreffende Angaben anzukreuzen waren.[51] Auf unser Tätigwerden wurde eingeräumt, dass ein IFG-Antrag formlos gestellt werden kann. Das Formular würde aus organisatorischen Gründen genutzt, um die Terminierung vornehmen und über die Gebührenpflicht aufklären zu können. Die antragstellende Person hat schließlich die gewünschten Informationen erhalten, denn gesetzliche Ausschlussgründe lagen nicht vor.

Im zweiten Fall ging es um eine Sondernutzungserlaubnis, für die das bezirkliche Straßen- und Grünflächenamt zuständig ist. Hier wurde der Antrag zunächst mit der pauschalen Begründung abgelehnt, der Sondernutzer habe die Akteneinsicht durch Darlegung von Gründen abgelehnt. Seine Anhörung hätte allerdings vorausgesetzt, dass eine der genannten Tatbestandsvoraussetzungen (personenbezogene Daten bzw. Betriebs- oder Geschäftsgeheimnisse) vom Amt bejaht wurde und zusätzlich die gesetzlich vorgesehene Interessenabwägung erfolgt ist.[52] Dass hiernach der Verwaltungsvorgang in Gänze nach IFG schutzbedürftig und deshalb auch kein teilweiser Informationszugang (bei Schwärzung schutzbedürftiger Daten)[53] möglich sein sollte, war nicht nachvollziehbar. Nach unserer Intervention hat das Amt dem Widerspruch abgeholfen und den Informationszugang erteilt.

Die Beschwerden machen deutlich, dass in den Bezirken eine Vereinheitlichung der Akteneinsichtsverfahren erstrebenswert ist, denn die beschriebenen Fälle zeichneten sich auch dadurch aus, dass sich die beschwerdeführenden Personen bei gleicher Sachlage mit unterschiedlichen Vorgehensweisen in den Bezirken

[51] Z. B. „Eigentümer/in, Verwalter/in, Bevollmächtigte/r, Architekt/in, Rechtsanwalt/-wältin, Notar/in, Student/in, Makler/in, Mieter/in mit Vollmacht des Eigentümers, Sachverständige/r“.
[52] Siehe § 14 Abs. 2 IFG.
[53] Siehe § 12 IFG.

konfrontiert sahen. Wir haben uns daher zunächst einen Eindruck verschafft, welche Art von Bauakten und Daten in den Ämtern verarbeitet wird. Gemeinsam mit der Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen als Oberste Bauaufsichtsbehörde haben wir einen Termin im Bezirksamt Charlottenburg-Wilmersdorf wahrgenommen, wo uns exem-plarisch einige Akten aus dem Bauamt bzw. dem Bauaktenarchiv und diesbezügliche Akteneinsichtsanträge gezeigt wurden. Auch das Bauaktenarchiv selbst haben wir besichtigt. Denn wer es nicht gesehen hat, vermag nicht zu ermessen, welche umfangreichen grundstücksbezogenen Papierdokumentationen dort vorgehalten werden, auf die sich zahlreiche und immer wiederkehrende Akteneinsichtsgesuche beziehen. Sie werden z. B. von Bauhistoriker:innen als wahre Datenschätze angesehen. Deshalb ist es wichtig, dass Akteneinsichtsverfahren möglichst straff und informationszugangsfreundlich gestaltet werden und gleichzeitig die Rechte derjenigen gewahrt bleiben, deren Interessen von den Zugangsanträgen berührt sind.

Die Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen beabsichtigt, zur Vereinheitlichung der bezirklichen Verfahren bei Akteneinsichten in Bauakten Vorschriften zu erarbeiten. Daraus sollen sich die spezifischen Handlungsbefugnisse für die Beschäftigten ergeben, je nachdem, zu welchen Zwecken Antragsteller:innen (wie bspw. Forschende und Architekt:innen) Akteneinsicht nehmen wollen und um wessen u. U. schutzbedürftige Daten (z. B. der Bauherr:innen) es geht. Dadurch würde die antragsgemäße Offenlegung von Informationen aus bezirklichen Bauakten nach einheitlichen und für Antragsteller:innen nachvollziehbaren Kriterien erfolgen. Wir werden uns hier aus Sicht der Informationsfreiheit und aus Sicht des Datenschutzes einbringen. Die Kriterien könnten auch ein wichtiger Schritt zur Digitalisierung der Bauakten sein, die auf der Grundlage eines ggf. zukünftig existierenden Berliner Transparenzgesetzes in einem Transparenzregister zu veröffentlichen wären.

Wir begrüßen die von der Obersten Bauaufsicht beabsichtigte Vereinheitlichung des datenschutzkonformen Informationszugangs zu Bauakten, und zwar sowohl im Hinblick auf Individualanträge als auch im Hinblick auf eine mögliche spätere proaktive Veröffentlichung in einem Transparenzregister. Durch die antragsunabhängige Bereitstellung der Informationen würde letztlich auch der Personalaufwand vermieden, der durch die Bearbeitung von Einzelanträgen entsteht.

5. Informationsfreiheit und Datenschutz

a) Eine Person beschwerte sich bei uns darüber, dass ihr IFG-Antrag auf Offenlegung eines gerichtlichen Vergleichs zwischen einer Universität und einem ihrer Professoren samt allen damit zusammenhängenden Akten vom Gericht abgelehnt worden war. Zur Begründung hatte das Gericht angeführt, dass ein Vergleich gewissermaßen ein „Vertrag" zwischen den Parteien sei, dessen Inhalt nicht für Dritte bestimmt ist.

Wir haben der Person mitgeteilt, dass wir das Anliegen in unserer Funktion als IFG-Schiedsstelle[54] nicht unterstützen können. Bei dem Prozessvergleich handelt es sich um eine Entscheidung in richterlicher Unabhängigkeit und nicht um eine Verwaltungstätigkeit des Gerichts. Nur für letztere Tätigkeiten eines Gerichts ist das IFG anwendbar.[55] Zudem würde die Offenlegung des gewünschten Dokuments inklusive der dem Vergleich zugrunde liegenden Unterlagen eine Übermittlung der personenbezogenen Daten des Professors darstellen. Dies wäre auch bei Anwendbarkeit des IFG nicht vom Gesetz gedeckt: Das IFG lässt nur in den explizit genannten wenigen Fällen eine Offenlegung von personenbezogenen Daten ohne Zustimmung des Betroffenen zu.[56]

b) Eine Person beschwerte sich bei uns darüber, dass die Feuerwehr weder auf den IFG-Antrag noch in der Einsatzberichterstattung im Internet Einzelheiten zu einer Brandbekämpfung mitteilte, die in einer konkret benannten Mietwohnung eines Wohnhauses stattgefunden hatte. Für die Person war dies unverständlich, denn sie fühlte sich als im selben Haus lebende Mieterin ebenfalls vom Brand betroffen. Später beantragte sie die Auskunft über alle Einsätze der Feuerwehr, die an dem besagten Tag in Berlin erfolgt waren. Da die Feuerwehr darauf nicht reagierte, beschwerte sich die Person erneut.

Wir haben der Person mitgeteilt, dass wir ihr Anliegen in unserer Funktion als IFG-Schiedsstelle nicht unterstützen können. Denn auf der Grundlage des IFG bestand kein Anspruch, dass ihr die gewünschten Einzelheiten zu dem konkreten Einsatz mitgeteilt werden. Nach dem IFG besteht das Recht auf Aktenauskunft u. a. nicht, soweit dadurch personenbezogene Daten veröffentlicht werden und tatsächliche Anhaltspunkte dafür vorhanden sind, dass überwiegend Privatinteressen verfolgt werden.[57] Dies war hier der Fall, denn die

[54]Nach § 18 Abs. 3 IFG ist jeder Mensch befugt, die Berliner Beauftragte für Datenschutz und Informationsfreiheit anzurufen.
[55]Siehe § 2 Abs. 1 Satz 2 IFG.
[56]Siehe § 6 IFG.
[57]§ 6 Abs. 1, 1. Alt. IFG.

gewünschten Informationen zum Feuerwehreinsatz in der konkret benannten Straße mit Hausnummer und Lage („parterre, links“) sowie die konkreten Einsatzdetails waren personenbezogen. Ein überwiegendes Informationsinteresse, das sich auf die Kontrolle staatlichen Handelns bezieht,[58] war nicht ersichtlich.

Die nachfolgende Beschwerde derselben Person über die Untätigkeit der Feuerwehr in Bezug auf ihren zweiten (allgemeiner formulierten) Antrag zielte erkennbar darauf ab, nun auf diese Art Einzelheiten zu dem Feuerwehreinsatz zu erfahren. Wir teilten der Person daher mit, dass wir das Anliegen nicht unterstützen können. Auch die Feuerwehr dazu zu bewegen, den IFG-Antrag förmlich zu bescheiden, hätte bedeutet, dass wir dies mit einem Hinweis auf unsere Rechtsauffassung verbinden.[59] Danach wäre die Offenlegung der gewünschten Informationen aus den dargestellten Gründen unzulässig gewesen.

Informationszugang und Datenschutz schließen sich nicht aus: Es handelt sich um zwei Seiten derselben Medaille, denn beides kann in Einklang gebracht werden, wie sich aus der Abwägung des Gesetzgebers in den Fällen des § 6 IFG ergibt. Für die Offenlegung von personenbezogenen Daten, die über die im Gesetz genannten Fälle hinausgehen, besteht regelmäßig keine Rechtsgrundlage.

IV. Künstliche Intelligenz

Die Ausführungen in Kapitel IV. Künstliche Intelligenz geben den Sachstand korrekt wieder. Die Zusammenarbeit zwischen der Senatskanzlei und der Berliner Beauftragten für Datenschutz und Informationsfreiheit im Rahmen der Taskforce KI und insbesondere der Unterarbeitsgruppe zum Thema Datenschutz verläuft konstruktiv und lösungsorientiert. Um hinsichtlich des Einsatzes von KI-Systemen in der Berliner Verwaltung Rechtssicherheit herzustellen, erarbeitet die Senatskanzlei aktuell eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten mittels KI. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit wurde in den Erarbeitungsprozess frühzeitig einbezogen und bringt sich mit ihrer Expertise beratend ein.

Bei der aktuell in der Testung befindlichen KI-Lösung BärGPT, die vom CityLAB Berlin in Zusammenarbeit mit der Senatskanzlei entwickelt wird, liegt ein besonderes Augenmerk auf der DSGVO-

[58] § 6 Abs. 1, 2. Alt. und § 1 IFG.
[59] Das sehen wir als Teil unserer in § 18 Abs. 2 IFG normierten Befugnis, die Einhaltung des IFG bei den öffentlichen Stellen zu kontrollieren.

Konformität. Mit diesem Ziel werden derzeit gemeinsam mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit geeignete technische und organisatorische Maßnahmen erarbeitet, um mögliche Risiken zu minimieren oder von vornherein auszuschließen.

1. Künstliche Intelligenz in der Berliner Verwaltung

Im April fand das Kick-off-Treffen der neu gegründeten Taskforce KI statt. Die Taskforce wird von der Senatskanzlei und dem IT-Dienstleistungszentrum Berlin (ITDZ) gemeinsam geleitet und befasst sich mit Projekten der Verwaltung zu Künstlicher Intelligenz (KI). Ein erstes Arbeitsergebnis ist eine Orientierungshilfe zum Umgang mit auf großen Sprachmodellen basierten Chatbots (LLM-basierte Chatbots)[60] für Verwaltungsmitarbeitende. Wir bringen uns mit juristischer sowie technischer Expertise ein.

Nach dem Haushaltsgesetz 2024/25 ist die Berliner Verwaltung aufgefordert, eine Taskforce KI einzurichten. Sie soll die aktuellen Entwicklungen im Bereich Künstlicher Intelligenz beobachten, bewerten und Empfehlungen für den weiteren Umgang und die Nutzung von KI-Anwendungen im Land Berlin geben. Dazu haben sich verschiedene Akteur:innen aus den Hauptverwaltungen, der Wissenschaft, dem CityLab (Berlins öffentliches Innovationslabor) und dem ITDZ mehrmals in diesem Jahr getroffen. Wir haben uns ebenfalls eingebracht. Aufgabe der Taskforce wird es künftig sein, Beratung für die Verwaltung z. B. durch die Erarbeitung von Handlungsempfehlungen und Leitfäden anzubieten, ressortübergreifende KI-Vorhaben und zukünftige Pilotprojekte zu begleiten sowie den Wissenstransfer zu fördern.

Erste Arbeitsergebnisse der Taskforce KI sind die im September veröffentlichte Orientierungshilfe zum Umgang mit LLM-basierten Chatbots im Land Berlin sowie der Leitfaden für effektives Prompting[61]. Beide Dokumente hat die Senatskanzlei als Anlagen zu einem Rundschreiben zum Umgang mit generativen KI-Anwendungen in der Verwaltung veröffentlicht.[62] Die Handlungsanleitungen richten sich an Führungskräfte sowie Verwaltungsmitarbeiter:innen, die auf dem Markt verfügbare KI-Chatbots nutzen, und geben Hinweise zum verantwortungsbewussten Umgang damit. Gleichzeitig dienen sie der Sensibilisierung für die

[60]LLM-basierte Chatbots sind Programme, die mit großen Mengen von Textdaten trainiert werden, um natürliche Gespräche zu führen und auf eine Vielzahl von Fragen zu antworten.
[61]Der sog. Prompt ist ein Anweisungssignal oder eine Eingabe, die an ein KI-System gerichtet ist, um eine Antwort oder Aktion zu initiieren.
[62]Abrufbar unter https://www.berlin.de/politik-und-verwaltung/rundschreiben/download.php/4329261 und https://www.berlin.de/politik-und-verwaltung/rundschreiben/download.php/4329264.

rechtlichen Rahmenbedingungen. Wir haben uns bei der Erarbeitung der Orientierungshilfe beteiligt und die datenschutzrechtlichen Aspekte eingebracht.

Ferner haben wir die Teilnehmenden der Taskforce KI zu datenschutzrechtlichen Fragestellungen im Zusammenhang mit der Entwicklung und dem Einsatz von KI sensibilisiert. So gelten die Vorschriften der Datenschutz-Grundverordnung (DSGVO), wenn personenbezogene oder personenbeziehbare Daten verarbeitet werden. Sollen KI-Systeme mit personenbezogenen Daten trainiert werden, obwohl diese nicht zum Training, sondern für einen anderen Zweck erhoben wurden, bedarf es hierfür einer separaten (noch zu schaffenden) Rechtsgrundlage. Zum einen scheidet eine Verarbeitung personenbezogener Daten auf der Grundlage eines berechtigten Interesses i. S. d. Art. 6 Abs. 1 Satz 1 lit. f DSGVO im öffentlichen Bereich als Rechtsgrundlage aus.[63] Zum anderen ist fraglich, ob gegenüber der Verwaltung erteilte Einwilligungen wirksam sein können. Ob und welche Folgen es hat, wenn ein KI-Modell mit personenbezogenen Daten trainiert wurde und die Rechtmäßigkeit der Datenverarbeitung in der Trainingsphase zweifelhaft ist, muss im Rahmen einer Risikoprüfung im Einzelfall analysiert werden.

Die Einordnung, dass KI-Modelle nicht generell als anonym angesehen werden, sondern personenbezogene Daten enthalten können,[64] wirft für die Verwaltung noch zu klärende Fragen hinsichtlich der Zulässigkeit des Einsatzes verschiedener gängiger KI-Modelle auf. Die Verwaltung benötigt für die datenschutzkonforme Entwicklung und den datenschutzkonformen Einsatz von KI-Modellen Unterstützung in Form konkreter Lösungsansätze.

Zukünftig wird sich die Taskforce KI vor allem mit konkreten KI-Projekten im Land Berlin befassen. Angesichts der hohen Datenschutzrelevanz des Einsatzes von KI-Anwendungen für Bürger:innen und Beschäftigte werden wir uns weiterhin in der Taskforce KI dafür einsetzen, dass der Schutz personenbezogener Daten von vornherein Berücksichtigung findet. Hierfür soll innerhalb der Taskforce eine Unterarbeitsgruppe zum Datenschutz eingerichtet werden, an der interessierte Verwaltungsvertreter:innen mitwirken können. Unabhängig davon werden wir – sowohl in Abstimmung mit den übrigen deutschen als auch mit den eu-

[63]Siehe Art. 6 Abs. 1 Satz 2 DSGVO; Erwägungsgrund (ErwGr.) 47 Satz 5 DSGVO.
[64]Siehe Europäischer Datenschutzausschuss (EDSA), Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_de.

ropäischen Aufsichtsbehörden – auf Klärung bisher ungeklärter Rechtsfragen hinwirken und Vorschläge für konkrete Lösungsansätze erarbeiten.

2. Erste Erkenntnisse aus großen Prüfverfahren zu Künstlicher Intelligenz

Die Überwachung und die Durchsetzung der DSGVO im KI-Bereich findet mehr und mehr Eingang in unsere alltägliche Aufsichtspraxis. In ersten Prüfverfahren von Amts wegen im nicht-öffentlichen Bereich haben wir bereits einige Datenschutzverstöße ausmachen können, die es in der Zukunft zu vermeiden bzw. abzustellen gilt.

Die praktischen Einblicke in die KI-Anwendungsszenarien einiger Unternehmen haben erste Problemstellungen aufgezeigt. Hier ging es zumeist um Techniken des maschinellen Lernens, die häufig eine große Anzahl personenbezogener Trainingsdaten voraussetzen. Sowohl das Training der KI-Modelle als auch der Einsatz der auf den KI-Modellen basierenden KI-Systeme können dabei datenschutzrechtliche Relevanz aufweisen. Inhaltlich haben wir uns zunächst auf die wesentlichen Fragen der Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten bei der Entwicklung und dem Einsatz von KI[65] sowie auf die dazugehörige Transparenz gegenüber den betroffenen Personen[66] konzentriert.

Die DSGVO geht von deterministischen Verarbeitungssystemen aus, d. h. es gibt konkrete Zwecke für die Verarbeitung, an der die Erforderlichkeit der personenbezogenen Datenverarbeitung gemessen werden kann. Bei der Verwendung von KI-Modellen und -Systemen haben wir es aber regelmäßig mit Mitteln zu tun, die einen probabilistischen Ansatz verfolgen: Sie beruhen auf Wahrscheinlichkeiten und nicht auf gänzlich vorgefertigten Regeln, was die Entdeckung von Zusammenhängen in verschiedensten Anwendungsbereichen ermöglicht. Die Verwendungszwecke von personenbezogenen Daten im KI-Kontext können daher sehr allgemein bzw. unspezifisch sein, d. h. so unspezifisch, dass die KI nicht als Verarbeitungsmittel zur Erreichung eines bestimmten Zwecks zu betrachten ist, sondern etwa beim Einsatz generativer KI zum Selbstzweck wird. Vor diesem Hintergrund fehlt es ggf. an der Beziehung zwischen Zweck und Verarbeitung, die bisher den Rahmen für die Erforderlichkeitsprüfung setzt. Darüber hinaus werden ggf. Daten verwendet, die zu einem anderen Zweck erhoben wurden und nun

[65] Siehe Art. 6 Abs. 1 DSGVO.

[66] Siehe Informationspflichten bei der Direkterhebung personenbezogener Daten nach Art. 13 Abs. 1 und 2 DSGVO und bei der nicht unmittelbar bei den betroffenen Personen erfolgten Datenerhebung nach Art. 14 Abs. 1 und Abs. 2 DSGVO.

zweckändernd für das Training von KI-Modellen bzw. -Systemen eingesetzt werden sollen. Wie bei der Datenerhebung zum Zwecke des KI-Trainings bedarf es auch für die zweckändernde Weiterverarbeitung von Daten zu diesem Zweck einer Rechtsgrundlage und die Anforderungen des Zweckvereinbarkeitstests des Art. 6 Abs. 4 DSGVO müssen erfüllt sein.

Im nicht-öffentlichen Bereich kann als Rechtsgrundlage Art. 6 Abs. 1 Satz 1 lit. f DSGVO herangezogen werden. Danach ist die Rechtmäßigkeit davon abhängig zu machen, dass die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und keine schutzwürdigen Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen.[67] Im Rahmen dieser Interessenabwägung kann die Verarbeitung von Trainingsdaten auch risikoabhängig untersucht werden. Dabei wäre Folgendes zu berücksichtigen:

- ob vor dem Hintergrund der Datenminimierung eine Verarbeitung mit anonymisierten bzw. pseudonymisierten Daten ausreichend sein kann
- in welchem Kontext die Datenverarbeitung erfolgt
- welche Konsequenzen die Datenverarbeitung für die betroffenen Personen hat bzw. ob abschätzbar ist, welche Konsequenzen sie haben kann
- ob es sich um Daten handelt, die von dem Unternehmen direkt bei der betroffenen Person erhoben oder von Dritten beschafft wurden
- welche Art von Daten in welcher Intensität verarbeitet werden
- welche Schutzbedarfe die personenbezogene Datenverarbeitung hat
- welche Erwartungshaltung die betroffenen Personen in Bezug auf die Verarbeitung ihrer Daten haben
- welche Einwirkungsmöglichkeiten auf die Verarbeitung den betroffenen Personen zur Verfügung stehen

Auffällig war bei unseren Prüfungen, dass viele Unternehmen die betroffenen Personen bisher entweder gar nicht oder nicht ausreichend über ihre Datenverarbeitung im Zusammenhang mit ihren KI-Systemen informieren. Dies kann auch für die Frage der Rechtmäßigkeit der Datenverarbeitung unmittelbare Konsequenzen haben. Gerade wenn sich Verantwortliche auf die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen[68] berufen, gehen wir nach der

[67] Siehe auch EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Rn. 12 ff., abrufbar unter https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_de.
[68] Siehe Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

EuGH-Rechtsprechung[69] davon aus, dass dies unzulässig ist, wenn betroffenen Personen nicht einmal das berechtigte Interesse[70] mitgeteilt wird, auf das sich der Verantwortliche beruft. Dieser Verstoß gegen die Mitteilungspflichten nach Art. 13 bzw. Art. 14 DSGVO wirkt sich dann unmittelbar auf die Rechtmäßigkeit der Datenverarbeitung aus. Unabhängig davon kann eine über die gesetzlichen Vorgaben herausgehende Transparenz gegenüber den betroffenen Personen (z. B. durch eine Zusammenstellung häufig gestellter Fragen (FAQ) zu den KI-Systemen) ein wichtiger Faktor bei der Prüfung der Zulässigkeit im Rahmen der Interessenabwägung[71] sein.

Insofern haben wir den Eindruck gewonnen, dass viele Unternehmen unabhängig von ihrer Größe aufgrund des derzeitigen KI-Enthusiasmus erste Schritte mit KI-Systemen wagen, ohne dabei die etablierten Compliance-Prozesse für den Datenschutzbereich einzuhalten. Vielfach haben wir bspw. KI-Chatbots auf Websites ohne Informationen zur damit einhergehenden Verarbeitung personenbezogener Daten vorgefunden. Bei einem Unternehmen, das ein KI-basiertes Forderungsmanagement anbietet, haben wir vor Ort überprüft, ob hinsichtlich seiner KI-Modelle die vorgebliche Anonymisierung der Daten der Schuldner:innen vor dem bestärkenden Lernen (sog. Reinforcement Learning) tatsächlich als wirksam einzustufen ist. Da das Unternehmen seine KI-Systeme einsetzt, um eine personalisierte Kundenansprache zur erfolgreicheren Eintreibung von Forderungen zu ermöglichen, haben wir uns zusätzlich auf die Profilbildung einzelner Schuldner:innen und eine etwaig damit zusammenhängende verbotene automatisierte Einzelentscheidung[72] über die Einleitung gerichtlicher Schritte des Unternehmens gegen die Schuldner:innen fokussiert.

In einem weiteren Fall prüften wir eine kommerzielle Fotoplattform, die nach unserer derzeitigen Kenntnis bereits ins Internet hochgeladene Fotos, die zumindest zum Teil als personenbezogen einzustufen waren, Unternehmen gegen Bezahlung auch für das Training von KI-Modellen anbot. Dieses Vorgehen war nur teilweise in der Datenschutzerklärung der Plattform abgebildet. Bei einer Immobilienvermittlungsplattform ist uns im Rahmen eines Beschwerdeverfahrens aufgefallen, dass der Betreiber die abgeschlossene und neu hinzukom-

[69]Europäischer Gerichtshof (EuGH), Urteil vom 9. Januar 2025, C-394/23, Rn. 52; EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 126 (Meta Platforms); Generalanwalt beim EuGH, Schlussanträge vom 11. Juli 2024, C-394/23, Rn. 53 ff.
[70]Siehe Art. 13 Abs. 1 lit. d und Art. 14 Abs. 2 lit. b DSGVO.
[71]Siehe Art. 6 Abs. 1 Satz 1 lit. f DSGVO.
[72]Art. 22 Abs. 1 DSGVO.

mende Kommunikation mit Kund:innen für das Training eines KI-Systems zur effizienteren Bearbeitung von Kundenanfragen nutzte, ohne jedoch die Kund:innen auf diese Verarbeitung hinzuweisen.

Zu einer Nachrichtenseite eines anderen Unternehmens wurde uns berichtet, dass der auf der Website eingesetzte KI-Chatbot widersprüchliche Aussagen zur Datenschutzerklärung der Website gemacht hat. So hat der Chatbot auf die Frage, welche personenbezogene Daten verarbeitet werden, ausgegeben, dass keine Daten gespeichert und verarbeitet werden, was aber im Widerspruch zur Datenschutzerklärung auf der Website stand. LLM-Chatbots können fehlerhafte oder erfundene Antworten geben, die plausibel klingen, was oft als „Halluzination“ bezeichnet wird. Der Datenschutzgrundsatz der Richtigkeit personenbezogener Daten[73] und die Vorgaben zum Datenschutz durch Technikgestaltung[74] gebieten es, eine Reihe von an das jeweilige KI-System angepassten Maßnahmen zur Erhöhung der Korrektheit der Antworten von KI-Chatbots zu ergreifen.[75]

Die Entwicklung und der Einsatz von KI-Systemen bringen häufig die Verarbeitung einer großen Menge personenbezogener Daten mit sich. Unsere ersten Prüfverfahren zeigen, dass insbesondere die Transparenz bei KI-Anwendungen vielfach noch nicht auf dem notwendigen Niveau angekommen ist. Auch wenn KI-Systeme einen schnellen Effizienzgewinn und neue Einnahmequellen für Unternehmen versprechen, ist es im Hinblick auf die damit einhergehenden datenschutzrechtlichen Risiken wichtig, die Rechtsabteilung und die betrieblichen Datenschutzbeauftragten bei deren Einführung frühestmöglich einzubeziehen. In den nächsten Jahren werden wir unseren KI-Prüffokus stetig erweitern, insbesondere im Hinblick auf die Umsetzung von Betroffenenrechten (wie z. B. Auskunfts-, Löschungs- und Widerspruchsrechte) sowie auf mit Verzerrungen einhergehende Diskriminierungen (sog. Bias). Auf nationaler sowie europäischer Ebene findet ein intensiver Austausch unter den Aufsichtsbehörden zu den datenschutzrechtlichen Fragen der Entwicklung und des Einsatzes von KI statt.[76]

[73] Art. 5 Abs. 1 lit. d DSGVO.
[74] Art. 25 Abs. 1 DSGVO.
[75] Z. B. durch Techniken wie Prompt Engineering und Retrieval-Augmented Generation.
[76] Siehe dazu B.II.6 und C.I.4.

V. Inneres und Justiz

1. Einsatz von Gesichtserkennungssystemen ohne Rechtsgrundlage

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert klare gesetzliche Regelungen für Gesichtserkennungssysteme.[77] Den Einsatz solcher Technologien durch die Staatsanwaltschaft Berlin haben wir zur Prüfung der Rechtmäßigkeit in den Fokus genommen.

Im Frühjahr wurde uns bekannt, dass bei der Staatsanwaltschaft in verschiedenen Verfahrenskomplexen ein Gesichtserkennungssystem eingesetzt wurde. Dabei handelte es sich um ein System von fest installierten sowie mobil auf Kraftfahrzeugen betriebenen Kameras, das Bilder von Personen und Fahrzeugen erstellen und biometrisch abgleichen kann. Der Einsatz erfolgte unter Nutzung von Sach- und Personalmitteln, die in Amtshilfe zur Verfügung gestellt wurden.[78] Die Staatsanwaltschaft stützt die Datenverarbeitungen auf die §§ 100h, 163f Strafprozessordnung (StPO) für die längerfristige Observation und die Aufzeichnung von Bildern auf öffentlichen Straßen und auf § 98a StPO für den Abgleich der erhobenen Daten mittels automatisierter Gesichtserkennung.

Alle drei Rechtsgrundlagen regeln jeweils nur Teilbereiche des Einsatzes von biometrischer Gesichtserkennung, aber auch gemeinsam gelesen ergibt sich daraus keine rechtliche Grundlage für den Einsatz solcher Fernidentifikationssysteme. Die Regelungen sprechen weder speziell den Einsatz solcher Systeme an, noch erfüllen sie die verfassungsrechtlichen Anforderungen für derart erhebliche Eingriffe in die informationelle Selbstbestimmung, wie sie der verfassungsrechtliche Bestimmtheitsgrundsatz erfordert.

§ 98a StPO regelt die Rasterfahndung. Diese gesetzliche Bestimmung ermöglicht den Strafverfolgungsbehörden, umfangreiche maschinelle Datenabgleiche vorzunehmen, um Personen, die bisher als Zielperson unbekannt waren, zu identifizieren. Bei dieser Methode der Überprüfung wird anders vorgegangen als bei herkömmlichen verdeckten Ermittlungstechniken: Zunächst wird ein großer Datenbestand mit Informationen zu vielen Personen, die nicht im Fokus von Verdächtigungen stehen, anhand spezifischer Kriterien analysiert. Das Ziel dieser Maßnahme ist es, diesen Personenkreis durch eine fortschreitende Selektion anhand

[77] Siehe B.II.2.

[78] Siehe Abgeordnetenhaus von Berlin, Schriftliche Anfragen vom 4. März 2024 und 1. August 2024, Abghs.-Drs. 19/18461 und 19/19879.

von auf die Täterin oder den Täter vermutlich zutreffenden Prüfungsmerkmalen schrittweise zu verkleinern. Auf diese Weise sollen unverdächtige Personen ausgeschlossen oder weitere ermittlungsrelevante Merkmale ausgemacht werden.

Die biometrische Fernidentifizierung ist hingegen eine Technologie, die es – in aller Regel verdeckt – ermöglichen soll, Personen, die sich im öffentlichen Raum aufhalten, in Echtzeit aus der Ferne zu identifizieren, indem biometrische Merkmale wie Gesichtszüge gleichzeitig oder zeitnah mit Personenbildern aus Datenbanken abgeglichen werden. Die Zielpersonen sind in diesem Fall bekannt; die Datenerhebung erfolgt aber als laufende Aufnahme aus dem letztlich „dynamischen" Datenbestand des öffentlichen Raums, aus dem vollkommen unvorhersehbar in Art und Umfang eine Vielzahl von biometrischen Informationen, Verhaltens- und Standortdaten erfasst wird. Nur mittels einer weiteren technischen Anwendung können dann die Lichtbilder und Videos in einer Form zusammengeführt und analysiert werden, die einen Abgleich ermöglicht. Diese technische Verarbeitung ist Voraussetzung, um erhobene Bilder aus dem öffentlichen Straßenland zu verwenden, da sich diese Daten in Format und Struktur von den Abgleichsobjekten unterscheiden. Auch dieser Verarbeitungsvorgang benötigt eine rechtliche Grundlage, die in § 98a StPO nicht hinreichend bestimmt ist.

Zwar erlaubt § 100h StPO unter bestimmten Voraussetzungen auch heimliche Überwachungsmaßnahmen mit technischen Mitteln, die hier vorgesehene Art der Verarbeitung von biometrischen Daten geht aber über den erlaubten Anwendungsbereich hinaus. Auch § 163f StPO, der die längerfristige Observation erlaubt, kann nicht als Rechtsgrundlage dienen. Biometrische Daten sind aufgrund ihrer einzigartigen Natur zudem besonders schützenswert und ihre Verarbeitung erfordert daher strengere Auflagen als andere Arten personenbezogener Daten.[79] Eine ausreichende Rechtsgrundlage müsste den Einsatz dieser Systeme spezifisch erlauben und genauer umschreiben.

Das Bundesverfassungsgericht (BVerfG) hat die verfassungsrechtlichen Anforderungen an entsprechende Vorschriften zur automatisierten Datenanalyse konkretisiert.[80] § 98a StPO genügt diesen Voraussetzungen im

[79]Art. 10 Richtlinie 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 (JI-Richtlinie).
[80]BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20.

Hinblick auf den Einsatz von Gesichtserkennungssystemen nicht. Auch ist im vorliegenden Fall fraglich, ob die Maßnahmen angesichts der Vielzahl an betroffenen unverdächtigen Personen überhaupt verhältnismäßig durchgeführt wurden. Die Staatsanwaltschaft konnte zu entsprechenden Zahlen keine belastbaren Angaben machen. Auch die erforderliche Datenschutz-Folgenabschätzung[81] konnte sie nicht vorlegen.

Die von der Staatsanwaltschaft herangezogenen Rechtsgrundlagen sehen jeweils eine richterliche Anordnung der einzelnen Maßnahmen vor. Mangels Zuständigkeit für die justizielle Tätigkeit der Gerichte erfasst unsere rechtliche Würdigung nicht die richterlichen Anordnungen der Maßnahmen in der Vergangenheit.[82] Wir haben allerdings die Staatsanwaltschaft gewarnt, dass weitere entsprechende Anträge in der Zukunft gegen Datenschutzrecht verstoßen würden.[83]

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit überschreitet mit ihrer Kritik an der Tätigkeit der Staatsanwaltschaft ihre Befugnisse in eklatanter Weise. Gegenstand ihrer Kritik sind von mindestens sechs verschiedenen Ermittlungsrichtern und Ermittlungsrichterinnen des Amtsgerichts Tiergarten erlassene Beschlüsse zum Einsatz von Gesichtserkennungssystemen. Aufgrund des grundgesetzlichen Schutzes der richterlichen Unabhängigkeit (Art. 97 Abs. 1 GG) nimmt § 8 Abs. 3 BlnDSG die rechtsprechende Tätigkeit der Gerichte von der Kontrolle durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit explizit aus.

Auch die DSK hat sich mit dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden befasst und in einer Entschließung[84] klargestellt, dass der einschlägige Rechtsrahmen und die Freiheitsrechte der Betroffenen – also potenziell aller Menschen – nicht hinreichend beachtet werden, wenn Behörden automatisierte biometrische Gesichtserkennungssysteme im öffentlichen Raum einsetzen und sich dabei auf unspezifische strafprozessuale Normen berufen. Die bestehenden Regelungen in der StPO bieten nach Ansicht der DSK für biometrische Gesichtserkennung im öffentlichen Raum keine Grundlage.

Der Versuch der Berliner Beauftragten für Datenschutz und Informationsfreiheit, ihre Kritik ausdrücklich nur auf die staatsanwaltschaftliche Antragstellung und nicht die antragsgemäße Entscheidung des Amtsgerichts Tiergarten verstanden wissen zu wollen, geht fehl und vermag keine andere Bewertung zu rechtfertigen. Denn angesichts des Umstands, dass für beides dieselben Rechtsvorschriften gelten, stellt ihre Kritik an der Antragsstellung der Staatsanwaltschaft Berlin eine offensichtliche Umgehung des Gesetzes und einen massiven und unzulässigen Eingriff in die richterliche Unabhängigkeit dar.

Der Einsatz von Gesichtserkennungssystemen durch Strafverfolgungsbehörden greift intensiv in das Recht auf informationelle Selbstbestimmung ein. Die bestehenden Regelungen in der StPO bieten für biometrische Gesichtserkennung im öffentlichen Raum keine ausreichende Grundlage. Sie erfüllen insoweit die verfassungsrechtlichen Anforderungen nicht, da sie schon nicht bestimmt genug sind, die umfassenden Möglichkeiten biometrischer Fernidentifikation zu erfassen. Sofern nach der KI-Verordnung und dem Verfassungsrecht Regelungsspielraum für den nationalen Gesetzgeber verbleibt und er den entsprechenden Einsatz als

Die Behauptung, die Staatsanwaltschaft hätte einen rechtswidrigen Beschluss beantragt, enthält untrennbar die unzulässige Feststellung, der vom Gericht antragsgemäß erlassene Beschluss sei rechtswidrig. In einer auf der 64. Jahrestagung der Präsidentinnen und Präsidenten der Oberlandesgerichte, des Kammergerichts und des Bundesgerichtshofs gefassten Entschließung heißt es:

„Alle im Rahmen von strafrechtlichen Ermittlungsverfahren ergehenden richterlichen Maßnahmen

[81] § 500 StPO i. V. m. § 67 Bundesdatenschutzgesetz (BDSG).
[82] § 8 Abs. 3 Berliner Datenschutzgesetz (BlnDSG).
[83] Siehe § 13 Abs. 2 Satz 4 BlnDSG.
[84] Siehe B.II.2.

zwingend erforderlich betrachtet, bedarf es einer tiefgehenden verfassungsrechtlichen Auseinandersetzung. Dann kann ein angemessener Ausgleich zwischen dem staatlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung der Menschen hergestellt werden.

gehören zum Kernbereich der richterlichen Unabhängigkeit und sind daher jeder Überprüfung durch andere Staatsgewalten - auch durch die Datenschutzbeauftragten - von vornherein entzogen. Dies gilt wegen des untrennbaren Zusammenhangs auch dann, wenn die Datenschutzbeauftragten nicht unmittelbar die gerichtliche Entscheidung, sondern den Antrag der Staatsanwaltschaft auf Erlass der richterlichen Entscheidung überprüfen oder gar beanstanden…. Die von den Datenschutzbeauftragten beanspruchten Kompetenzen verschieben die im Grundgesetz und in den Verfassungen der Länder vorgegebene Balance der drei Staatsgewalten in verfassungswidriger Weise. Die Dritte Staatsgewalt schützt die Grundrechte der Bürger wirkungsvoll."

2. Zu weitreichende Videoüberwachung der Polizeiwache am Kottbusser Tor

Wir haben die Videoüberwachung der Polizeiwache am Kottbusser Tor vor Ort geprüft und dabei festgestellt, dass die Datenerhebungen ohne ausreichende Rechtsgrundlage erfolgen und unverhältnismäßig in die Grundrechte von Passant:innen und Verkehrsteilnehmer:innen eingreifen. Wir haben daher eine Mangelfeststellung ausgesprochen.

Die Polizei hat seit Anfang 2023 eine neue Wache am Kottbusser Tor im Zentrum Kreuzbergs eingerichtet. Die Dienststelle befindet sich in einem Gebäuderiegel über der Adalbertstraße. Zur Sicherung der Wache werden in der Unterführung Videokameras eingesetzt, die sowohl die Fußwege als auch die Fahrbahn der Adalbertstraße erfassen. Zusätzlich wird der Eingangsbereich auf der Fußgängerterrasse videoüberwacht.

Die implementierte Videoüberwachung findet keine Stütze in § 24a Allgemeines Sicherheits- und Ordnungsgesetz Berlin (ASOG), der von der Polizei als Erlaubnisnorm herangezogen wird. Eine Polizeiwache stellt kein gefährdetes Objekt im Sinne dieser Vorschrift dar, da nicht jedes Gebäude zur Erfüllung öffentlicher Aufgaben von der Norm erfasst wird. Der Gesetzgeber wollte mit § 24a ASOG den Schutz bestimmter Objekte wie Religionsstätten oder Denkmäler erhöhen, nicht aber die allgemeine Videoüberwachung öffentlicher Räume bzw. öffentlicher Gebäude regeln. Diese unterfällt vielmehr § 20 BlnDSG, der nur einen sehr begrenzten Einsatz von Videokameras zur Wahrung des Hausrechts erlaubt. Nach Berliner Rechtsprechung muss der unverpixelte Erfassungsbereich der

Nach Auffassung des Senats können auch Dienstgebäude der Polizei Berlin zu den gefährdeten Orten nach § 24a Absatz 1 ASOG zählen. Das ist auch aus § 21 Abs. 2 Nr. 3 ASOG Bln ersichtlich, wonach die Polizei die Identität einer Person feststellen kann, wenn sie sich u. a. in einem Amtsgebäude oder einem anderen gefährdeten Objekt befindet, wenn Tatsachen die Annahme recht-fertigen, dass an oder in einem Objekt dieser Art Straftaten begangen werden sollen und weitere Voraussetzungen erfüllt sind. Es bedarf daher keines Rückgriffs auf § 20 BlnDSG.

Kameras auf etwa einen Meter zur Gebäudefassade begrenzt und für Passant:innen deutlich markiert werden.[85]

Die Polizei hatte den Einsatz der Kameras u. a. mit befürchteten Angriffen auf die Wache begründet; die Videoüberwachung soll daher der präventiven Gefahrenabwehr dienen. Allerdings werden die Aufnahmen zeitlich begrenzt gespeichert. Die Speicherung der Daten ist zum Zwecke der Gefahrenabwehr nicht erforderlich, da die Wache durchgehend besetzt ist und die Mitarbeiter:innen im Gefahrenfall sofort reagieren können. Seit Beginn der Überwachung wurden nur wenige Straftaten, darunter Sachbeschädigungen, aufgezeichnet. Die Speicherung der Aufnahmen geht damit über den Zweck hinaus und zielt offenbar auf die Strafverfolgungsvorsorge, also eine Sicherung von Beweisen für etwaige zukünftige Strafverfahren, ab. Eine solche Zweckänderung ist jedenfalls dort, wo die Zwecke und Verarbeitungsschritte klar getrennt werden können, rechtlich problematisch. Die Strafverfolgungsvorsorge fällt grundsätzlich in die Gesetzgebungskompetenz des Bundes.[86] Die bundesgesetzliche StPO und das BDSG sehen eine derartige Videoüberwachung jedoch nicht vor.

Die Strafverfolgungsvorsorge ist nach § 1 Absatz 3 Teil der vorbeugenden Bekämpfung von Straftaten und gehört als solche zur polizeilichen Aufgabe der Straftatenverhütung im Rahmen der Gefahrenabwehr. Daher ist die Speicherung der Aufnahmen zu diesem Zweck zulässig.

Die Überwachung ist im Übrigen unverhältnismäßig: Die Unterführung am Kottbusser Tor ist ein zentraler Verkehrsknotenpunkt von bezirksübergreifender Bedeutung. Sie wird täglich von tausenden Menschen als wichtiger Verkehrsweg genutzt und verbindet die Bezirke Mitte und Kreuzberg. Die Verkehrsteilnehmenden haben dabei wenig Möglichkeiten, der Videoüberwachung auszuweichen. Eine ausreichende Prüfung von milderen Mitteln wie baulichen Sicherungen oder Einsatz von Personal konnten wir nicht feststellen. Zwar werden die Kameras mit niedriger Auflösung eingesetzt. Dies kann den Grundrechtseingriff allein allerdings nicht kompensieren.

Die Videoüberwachung an der Polizeiwache am Kottbusser Tor ist so ausgestaltet, dass der Grundrechtseingriff verhältnismäßig ist: Gesichter von Personen und Kennzeichen der durchfahrenden Fahrzeuge werden in der Anzeige verpixelt bzw. ausgegraut; diese Verpixelung kann erst im Nachhinein bei Verdacht einer Straftat aufgehoben werden. Bestimmte Bereiche wie beispielsweise Wohnungen sind dauerhaft geschwärzt.

Besonders heikel ist die Überwachung der Fußgängerterrasse, da sich dort auch Zugänge zu anderen Einrichtungen befinden. Die Wache liegt zwischen der einzigen Treppe zur Terrasse und dem Zugang zu weiteren Einrichtungen, die u. a. Beratungsangebote für gesellschaftlich marginalisierte Gruppen anbieten. Den Hilfesuchenden muss ermöglicht werden, diese Angebote wahrzunehmen, ohne dass sie dabei gezwungen sind, sich der Videoüberwachung auszusetzen.

Wohnungen und Einrichtungen auf der anderen Seite der Adalbertstraße sind nicht ausschließlich über den Fußweg über die Terrasse an der Wache vorbei erreichbar. Es gibt Möglichkeiten, diese zu erreichen, ohne sich der polizeilichen Videoüberwachung auszusetzen. Zudem sind auch andere Einrichtungen neben solchen, die Beratung für marginalisierte Gruppen anbieten, über den Fuß-

[85]Siehe Amtsgericht (AG) Berlin-Mitte, Urteil vom 18. Dezember 2003, 16 C 427/02.

[86]Siehe BVerfG, Urteil vom 27. Juli 2005, 1 BvR 668/04, Rn. 99: „Die Verfolgungsvorsorge erfolgt in zeitlicher Hinsicht präventiv, betrifft aber gegenständlich das repressiv ausgerichtete Strafverfahren. Die Daten werden zu dem Zweck der Verfolgung einer in der Zukunft möglicherweise verwirklichten konkreten Straftat und damit letztlich nur zur Verwertung in einem künftigen Strafverfahren, also zur Strafverfolgung, erhoben."

weg erreichbar, sodass keineswegs eindeutig geschlussfolgert werden kann, mit welchem Ziel die von der Videoüberwachung erfassten Personen den Fußweg benutzen.

Der Einsatz von Videoüberwachung zur Sicherung öffentlicher Gebäude greift in das Recht auf informationelle Selbstbestimmung der Bürger:innen ein. Die Maßnahme muss daher auf einer Rechtsgrundlage beruhen, die den verfassungsrechtlichen Bestimmtheitsanforderungen genügt, und zudem verhältnismäßig sein. Polizeiwachen unterfallen regelmäßig nicht dem Schutz besonders gefährdeter Objekte nach dem ASOG. Die räumliche Ausdehnung der Überwachung ist auf den erlaubten Zweck und das erforderliche Maß zu begrenzen und darf insbesondere nicht den Zugang zu anderen Einrichtungen erschweren. Die Sicherheitsbehörden sollten alternative Konzepte in Betracht ziehen, die einen schonenden Ausgleich zwischen Sicherheitsinteressen und Freiheitsrechten ermöglichen.

Der Senat begrüßt es, dass mit dem Antrag der Koalitionsfraktionen über ein Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin (Drucksache 19/2553) eine Klarstellung im Wortlaut von § 24 a ASOG erfolgen soll, die ausdrücklich auch Amts- und Dienstgebäude als mögliche gefährdete Objekte nennt.

3. Zuverlässigkeitsüberprüfungen bei Großveranstaltungen: Grenzen der polizeilichen Befugnisse

Die Polizei führte im Berichtszeitraum bei mehreren Großveranstaltungen Zuverlässigkeitsüberprüfungen nach § 45a ASOG durch. Dabei traten sowohl beim Umfang der Überprüfungen zum Christopher Street Day (CSD) als auch bei den Überprüfungen beim Verfassungsschutz zur UEFA-Europameisterschaft datenschutzrechtliche Fragen auf. Wir haben die Behörde auf die Grenzen der gesetzlichen Ermächtigung und die Besonderheiten des Versammlungsrechts hingewiesen.

Bei der Organisation von Großveranstaltungen nutzen die Veranstalter:innen häufig die Möglichkeit von Zuverlässigkeitsüberprüfungen nach § 45a ASOG über die Polizei. Diese Überprüfungen betreffen vor allem Personen mit Tätigkeiten in sicherheitsrelevanten Bereichen. Dabei ergaben sich in zwei Fällen datenschutzrechtliche Fragestellungen: Beim CSD sollten auf Bitten der Veranstalter:innen die Fahrer:innen der Paradewagen überprüft werden, bei der UEFA-Europameisterschaft wurde mit den Datensätzen der überprüften Mitarbeitenden an den Veranstaltungsorten eine Regelanfrage u. a. bei den Verfassungsschutzbehörden durchgeführt.

Die Zuverlässigkeitsüberprüfung der CSD-Fahrer:innen wirft die grundlegende Frage zum Verhältnis von Gefahrenabwehrrecht und Versammlungsfreiheit auf. Versammlungsrechtliche Vorfeldmaßnahmen sind nach dem ASOG vor Beginn der Versammlung grundsätzlich zulässig, soweit sie nicht die Wahrnehmung

Die Fahrerinnen und Fahrer von LKW und Trucks anlässlich des CSD, der dem Versammlungsrecht unterlag, wurden vom Veranstalter gegen Entgelt für diese Tätigkeit aquiriert; in dieser Funktion wurden sie nach sorgfältiger Abwägung der betroffenen Rechte von der Polizei einer Zuverlässigkeitsüberprüfung unterzogen. Die Überprüfung

der Versammlungsfreiheit erschweren. Da Fahrer:innen nach einer Ablehnung aufgrund einer Zuverlässigkeitsüberprüfung auch als Fußgänger:innen an der Versammlung teilnehmen können, dürfte ihr Grundrecht auf Versammlungsfreiheit insgesamt auch nur am Rande betroffen sein. Dennoch muss die Überprüfung der Fahrer:innen auf einer objektiven Gefahrenlage basieren[87] – die Zustimmung der Versammlungsleitung ist hingegen unerheblich, da sie nicht über die personenbezogenen Daten der Fahrer:innen selbständig verfügen kann.

war vor dem Hintergrund einer entsprechenden Gefährdungslage-Bewertung des BKA, der zufolge zumindest die abstrakte Gefahr der Begehung eines islamistischen Terroranschlags bestand, rechtlich zulässig und geboten; insbesondere war die potenzielle, in der Vergangenheit bereits realisierte Gefährdung, die von einem Lastwagen ausgehen kann, der durch eine große Menge von Personen fährt, zu berücksichtigen. Ein Eingriff in das Grundrecht aus Art. 8 GG lag nicht vor, da – wie die Berliner Beauftragte für Datenschutz und Informationsfreiheit selbst ausführt - auch bei Ablehnung als Fahrerin oder Fahrer eine Teilnahme am CSD als Fußgänger möglich gewesen wäre.

Die Regelanfrage beim Verfassungsschutz im Rahmen der UEFA-Spiele überschreitet dagegen die Grenzen des § 45a ASOG. Der Gesetzgeber hat in § 45a ASOG den Umfang der Überprüfungen abschließend geregelt.[88] Ein Rückgriff auf die polizeiliche Generalklausel[89] scheidet aufgrund des Vorrangs der spezielleren Norm aus. Das Gleiche gilt für die im ASOG vorgesehene allgemeine Regelung zur Datenübermittlung innerhalb des öffentlichen Bereichs.[90]

In § 45a ASOG ist der Umfang der Überprüfungen gerade nicht abschließend geregelt. De lege lata ist dort lediglich die Übermittlung des Ergebnisses der Zuverlässigkeitsüberprüfung an öffentliche und nicht-öffentliche Stellen normiert (§ 45a Absatz 1 Satz 2 in Ver-bindung mit Satz 1), nicht jedoch das Verfahren der Überprüfung selbst, die diesem Ergebnis vorgeschaltet ist. Diesbezüglich ist da-her - unter der in § 45a Absatz 1 Satz 1 ASOG geregelten Prämisse der Erforderlichkeit einer Zuverlässigkeitsüberprüfung wegen besonderer Gefahren bei Großveranstaltungen - der Rückgriff auf die allgemeinen polizeilichen Befugnisse zur Datenverarbeitung zulässig. Es entspricht dem Sinn und Zweck des § 45a ASOG, dass die Polizei eine Prüfung in dem Umfang vornimmt, der mit der konkreten Gefahrenlage der Veranstaltung korrespondiert und geeignet ist, Sicherheitsbedenken weitestgehend auszuschließen.

Nach der Rechtsprechung des BVerfG bedarf jeder Eingriff in das Recht auf informationelle Selbstbestimmung einer klaren und bestimmten gesetzlichen Grundlage.[91] Dies gilt umso mehr bei einer Datenübermittlung zwischen Polizei und Nachrichtendiensten: Das informationelle Trennungsprinzip zwischen diesen Behörden ergibt sich aus ihren grundlegend verschiedenen Aufgaben und Befugnissen. Während die Polizei konkrete Gefahren abwehrt und dabei an enge rechtliche Voraussetzungen gebunden ist, betreiben die In-

Der Senat hält die anlässlich der UEFA-Spiele durchgeführte Regelanfrage beim Verfassungsschutz für rechtlich zulässig; das informationelle Trennungsprinzip zwischen Polizei und Nachrichtendiensten wurde nicht verletzt. Letzteres gilt nicht absolut, vielmehr sehen die Verfassungsschutzgesetze des Bundes und der Länder Übermittlungsbefugnisse zwischen den Verfassungsschutzbehörden und der Polizei zur jeweiligen Aufgabenerfüllung ausdrücklich unter bestimmten Voraussetzungen vor. So hat der Verfassungsschutz

[87]Siehe § 45a Abs. 1 Satz 1 ASOG: „Soweit […] wegen besonderer Gefahren bei Großveranstaltungen erforderlich“.
[88]Siehe zur Sperrwirkung der Spezialermächtigung gegenüber der Generalklausel etwa Oberverwaltungsgericht (OVG) Bremen, Urteil vom 24. März 1998, 1 BA 27/97.
[89]§§ 17, 18 ASOG.
[90]§ 44 Abs. 2 ASOG.
[91]BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 u. a. (sog. Volkszählungsurteil).

landsgeheimdienste eine weitreichende Vorfeldaufklärung mit nachrichtendienstlichen Mitteln.[92] Eine routinemäßige Verschränkung dieser unterschiedlichen Aufgabenbereiche durch Datenaustausch und eine weitreichende Zweckänderung der erhobenen Daten unterläuft die verfassungsrechtlich gebotene Trennung zwischen Polizei und Nachrichtendiensten. Wie das BVerfG feststellt,[93] können die weitreichenden Überwachungsbefugnisse der Verfassungsschutzbehörden verfassungsrechtlich nur gerechtfertigt werden, wenn die aus der Überwachung gewonnenen Informationen nicht ohne Weiteres an andere Behörden mit operativen Anschlussbefugnissen übermittelt werden dürfen.

nach § 5 Verfassungsschutzgesetz Berlin (VSG Bln) u.a. auch die Aufgabe, die zuständigen staatlichen Stellen und die Öffentlichkeit über Gefahren für die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder zu unterrichten, um diesen zu ermöglichen, rechtzeitig die erforderlichen Maßnahmen zur Abwehr dieser Gefahren zu ergreifen. Dazu gehört zweifellos auch die Verhinderung extremistisch motivierter Straftaten, wie sie im Vorfeld der EURO 2024 explizit u.a. vom „Islamischen Staat“ angedroht wurden. Die regelhafte Einbindung des Verfassungsschutzes in die Zuverlässigkeitsüberprüfung durch die Polizei war somit aufgrund der besonderen Gefahrenlage der in Rede stehenden internationalen, medial im besonderen Fokus der Öffentlichkeit stehenden Großveranstaltung rechtlich zulässig und auch geboten. Die Befugnis der Verfassungsschutzbehörde zur Übermittlung von Sicherheitsbedenken an die Polizei ergibt sich aus § 22 Absatz 2, Alt.1 VSG Bln.

Im Falle der Regelabfrage bei den Verfassungsschutzbehörden haben wir daher eine Mangelfeststellung ausgesprochen.

Diese Einzelfälle zeigen, dass Zuverlässigkeitsüberprüfungen bei Großveranstaltungen einer sorgfältigen rechtlichen Vorprüfung bedürfen. Bei Versammlungen muss die Polizei besonders zurückhaltend vorgehen, da bei der Überprüfung einzelner Teilnehmender im Vorfeld Auswirkungen auf die Versammlungsfreiheit nicht von vornherein ausgeschlossen werden können. Zudem darf der gesetzlich vorgesehene Rahmen für die Datenverarbeitung bei Zuverlässigkeitsüberprüfungen nicht durch einen Rückgriff auf die Generalklausel umgangen werden.

Der Senat begrüßt es, dass mit dem Antrag der Koalitionsfraktionen über ein Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin (Drucksache 19/2553) eine grundlegende Überarbeitung des § 45a im Sinne einer rechtssicheren Durchführung von Zuverlässigkeitsüberprüfungen erfolgen soll.

4. Automatisierte Datenabrufe einzelner Personen aus dem Melderegister durch Behörden

Eine betroffene Person wandte sich an uns, weil eine Behörde ihre personenbezogenen Daten aus dem Melderegister abgerufen hatte, ohne dass hierfür ein nachvollziehbarer Anlass ersichtlich war. Auf unsere Nachfrage teilte die Behörde mit, dass über das automatisierte Abrufverfahren eine namensgleiche Person im Melderegister gesucht worden war und der Abruf damit versehentlich erfolgte. Es stellte sich heraus, dass in der Suchmaske der Melderegisterabfrage nicht alle der Behörde vorliegenden Angaben zu der gesuchten Person eingegeben worden waren.

[92] BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07 (sog. ATDG-Urteil).
[93] BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 120.

Eine öffentliche Stelle darf personenbezogene Daten aus dem Melderegister über ein automatisiertes Verfahren der Meldebehörde abrufen, soweit die Daten der abrufenden Stelle zur Erfüllung ihrer Aufgaben bekannt sein müssen.[94] Ein automatisierter Abruf der Daten ist nicht erforderlich, wenn die betreffende öffentliche Stelle die Daten mit wenig Aufwand selbst erheben kann, indem sie diese etwa von der anwesenden betroffenen Person direkt erfragt.

Zu einer konkreten, namentlich bekannten Person dürfen alle in § 34 Abs. 1 Satz 1 BMG aufgeführten Daten abgerufen werden. Dies sind bspw. das Geburtsdatum und der Geburtsort, die derzeitigen Staatsangehörigkeiten sowie aktuelle und frühere Anschriften. Allein Sicherheitsbehörden und Gerichten ist es erlaubt, weitere Melderegisterdaten zu einer gesuchten Person automatisiert abzurufen.

Bei der Suche bzw. dem Abruf von Melderegisterdaten zu einer namentlich bekannten Person darf die abrufende Stelle nur bestimmte Auswahldaten verwenden.[95] Demnach muss sie mindestens drei gesetzlich genannte Informationen über die jeweilige Person kennen. Hinsichtlich des Namens kommen z. B. der aktuelle Familienname und mindestens ein Vorname oder der eingetragene Künstlername in Betracht. Zusätzlich zum Namen muss die abrufende öffentliche Stelle entweder die derzeitige oder eine frühere vollständige Anschrift (bestehend aus Wohnort, Straßenangabe und Hausnummer) oder – sofern ihr die exakte Anschrift nicht bekannt ist – neben dem Wohnort ein weiteres Kriterium (z. B. Geburtsdatum, Geburtsort oder Geschlecht) in die Suche eingeben.

Die abrufende Behörde oder eine andere öffentliche Stelle muss stets alle bekannten Auswahldaten für den automatisierten Abruf verwenden.[96] Hierdurch wird gewährleistet, dass die gesuchte Person so exakt wie möglich bestimmt werden kann und keine Daten anderer Personen abgerufen werden bzw. große Trefferlisten entstehen. Durch geeignete technische und organisatorische Maßnahmen muss eine abrufberechtigte Stelle daher auch u. a. sicherstellen, dass nur die Daten abgerufen werden, die für ihre Aufgabenerfüllung erforderlich sind.[97]

[94] Sog. einfache Behördenauskunft; siehe § 34 Abs. 1 und 2 Nr. 1 Bundesmeldegesetz (BMG) i. V. m. § 34a Abs. 1 BMG.
[95] Siehe § 38 Abs. 1 BMG.
[96] Siehe Nr. 38 Allgemeine Verwaltungsvorschrift zur Durchführung des Bundesmeldegesetzes (BMGVwV).
[97] § 39 Abs. 1 BMG.

In unserem Beschwerdefall wäre zwar zur Bearbeitung eines Antrags der Abruf zur antragstellenden Person erforderlich gewesen, nicht aber der Abruf zur namensgleichen Person unseres Beschwerdeführers. Ursache für diesen unbefugten Abruf war, dass nicht die exakte derzeitige Wohnanschrift als Auswahldatum in die Suchmaske eingegeben wurde, obwohl diese der Behörde bekannt war. Hierdurch wurden neben der tatsächlich gesuchten Person auch die Daten der beschwerdeführenden Person angezeigt. Die Behörde hat uns zugesichert, nochmals alle Dienstkräfte entsprechend den gesetzlichen Vorschriften zum Datenabruf zu belehren, um zukünftig Mehrfachauskünfte bzw. Trefferlisten zu vermeiden.

Jeder Abruf von Melderegisterdaten durch Behörden und andere öffentliche Stellen ist ein rechtfertigungsbedürftiger Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Personen. Die Behörden müssen vor jedem automatisierten Abruf prüfen, ob die personenbezogenen Daten zu ihrer Aufgabenerfüllung unerlässlich sind. Ferner müssen alle bekannten Auswahldaten bei der Suche eingegeben werden, um die Entstehung von Trefferlisten zu vermeiden. Die öffentlichen Stellen sind verpflichtet, entsprechende technisch-organisatorische Maßnahmen zu ergreifen. Dies kann insbesondere durch die Erstellung verbindlicher Handlungsleitfäden und Schulung der Dienstkräfte, die zum Melderegisterdatenabruf befugt sind, erfolgen.

VI. Digitalisierung in der -Verwaltung

1. Quo vadis? Wie ist Berlins Digitalstrategie für die Zukunft?

Die Digitalpolitik soll in Berlin u. a. an dem Grundsatz der Digitalen Souveränität ausgerichtet werden.[98] Aus Datenschutzsicht setzt dies voraus, dass IT-Lösungen in der Lage sind, alle Datenschutzvorgaben – allen voran die Anforderungen der Datenschutz-Grundverordnung (DSGVO)–, aber auch die der einschlägigen landesrechtlichen Regelungen einzuhalten. Digitale Souveränität umfasst darüber hinaus auch die Erfüllung begleitender Kriterien, die die Einhaltung der datenschutzrechtlichen Pflichten effektiv, nachprüfbar und dauerhaft sicherstellen.[99] Bei der Suche nach geeigneten Lösungen für die Verwaltungsmodernisierung sind daher auch Open-Source-Lösungen in den Blick zu

[98]Koalitionsvertrag 2023–2026, S. 15, abrufbar unter https://www.berlin.de/rbmskzl/_assets/dokumentation/koalitionsvertrag_2023-2026_.pdf?ts=1684996989.

[99]Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 11. März 2023, Kriterien für Souveräne Clouds, S. 3, abrufbar unter https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf.

nehmen, die ein hohes Maß an Transparenz versprechen und selbst geprüft und ggf. auch angepasst werden können.

Dies sieht offensichtlich auch der Senat so, denn in den Richtlinien der Regierungspolitik 2023–2026 heißt es unter dem Punkt „Verwaltungsmodernisierung“, dass die Verwendung von Open-Source-Lösungen die digitale Souveränität der Berliner Verwaltung stärkt. Der Senat hat sich darauf verständigt, bei der Suche nach geeigneten Lösungen für die Verwaltungsmodernisierung auch Open-Source-Lösungen einen besonderen Raum einzuräumen und bestehende Kooperationen zu Open Source zu verstärken und zu erweitern.[100] Im Bericht zur Open-Source-Strategie für das Jahr 2024 kündigt der Senat nun an, bestrebt zu sein, rechtzeitig zum Bericht für das Jahr 2025 eine entsprechende Strategie für das Land Berlin entwickelt und verabschiedet zu haben.[101] In der Praxis der Verwaltungsdigitalisierung können wir noch nicht erkennen, welche konkreten Schritte der Senat in Richtung einer tatsächlichen Realisierung einer solchen Strategie unternommen hat. Obwohl der Senat ein Open-Source-Kompetenzzentrum beim IT-Dienstleistungszentrum Berlin (ITDZ) eingerichtet und auch beschlossen hat, einen „Open Source BerlinPC“ zu entwickeln, der als Referenz für alle entsprechenden Ausschreibungen dienen soll,[102] haben wir bisher keine Informationen über konkrete Fortschritte in diese Richtung erhalten. Vielmehr findet derzeit wegen des auslaufenden Supports für das Client-Betriebssystem Windows 10 eine Migration der IKT-Arbeitsplätze auf das Betriebssystem Windows 11 statt. Offenbar sind viele der in der Berliner Verwaltung zum Einsatz kommenden IT-Fachverfahren noch immer auf einen Microsoft Client angewiesen.

Wir haben die IKT-Steuerung[103] im Rahmen unserer Beratung darauf hingewiesen, dass wir es vor dem Hintergrund der Festlegung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zum Einsatz von Microsoft 365[104] für erforderlich halten, Alternativen in den Blick zu nehmen, die ein datenschutzkonformes Handeln der Verwaltung sicherstellen können. Im Rahmen der strategischen Überlegungen muss berücksichtigt werden, dass auch

[100]Richtlinien der Regierungspolitik 2023–2026, „Verwaltungsmodernisierung“.
[101]Abghs.-Drs. 19/2136, S. 6, abrufbar unter https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/DruckSachen/d19-2136.pdf.
[102]Ebd., S. 4.
[103]Die bei der Senatskanzlei angesiedelte zentrale Steuerung der landesweit genutzten Informations- und Kommunikationstechnologie (IKT).
[104]Siehe DSK, Festlegung vom 24. November 2022, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf; siehe zum Einsatz von Microsoft 365 in Schulen auch JB 2023, A.IV.4.

Datenschutznachteile durch die Abhängigkeit von einzelnen Unternehmen und Lock-in-Effekte entstehen können.

Auf dem Weg zu einer digitalen Souveränität der Berliner Verwaltung ist es unerlässlich, dass der Senat im Rahmen einer Digitalstrategie einen konkreten Zeitplan für den Umstieg auf datenschutzgerechte Lösungen aufstellt und die im Koalitionsvertrag und in den Richtlinien der Regierungspolitik aufgestellten Ziele (etwa Open-Source-Lösungen einen besonderen Raum einzuräumen) auch tatsächlich praktisch umgesetzt werden. Wichtig ist es dabei, die gesamte Verwaltung in den Blick zu nehmen und einheitliche Lösungen anzubieten.

2. Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben

Mit der zunehmenden Digitalisierung der Verwaltung sind die an unsere Behörde gerichteten Beratungsanfragen in den letzten Jahren stark gestiegen. Eine datenschutzkonforme Umsetzung der Verwaltungsdigitalisierung setzt in der Verwaltung den Aufbau von fachlicher Kompetenz in Datenschutzfragen voraus. Als Grundlage dafür haben wir in diesem Jahr den Standardprozess Datenschutz für öffentliche Digitalisierungsvorhaben veröffentlicht,[105] den wir zusammen mit dem ITDZ entwickelt haben.

Die Digitalisierung der Verwaltung bringt eine zunehmend vollständig automatisierte Verarbeitung der personenbezogenen Daten der Bürger:innen und Beschäftigten im öffentlichen Dienst mit sich. Zum Schutz der Rechte und Freiheiten der Personen, deren Daten verarbeitet werden, müssen die verantwortlichen Behörden angemessene technische und organisatorische Maßnahmen ergreifen.[106] Dazu müssen sie über ausreichende Datenschutzexpertise verfügen und die Risiken analysieren können. Die Bewertung etwaiger Datenschutzrisiken setzt zudem vertiefte Kenntnisse der tatsächlich in der jeweiligen Behörde stattfindenden Verwaltungsprozesse und Datenverarbeitungen voraus. Die datenschutzrechtlichen Prüfungen der Verwaltungen können daher nicht ohne Weiteres auf externe Beratungsunternehmen ausgelagert werden. Diesen fehlen regelmäßig die erforderlichen Kenntnisse der internen Verwaltungsprozesse. In jedem Fall benötigt die verantwortliche Behörde eigene Expertise, auch um bewerten zu können, ob extern durchgeführte Prüfungen tatsächlich brauchbar sind. Darüber hinaus ist die Risi-

[105] Abrufbar unter https://www.datenschutz-berlin.de/themen/behoerden/standardprozess/.
[106] Siehe JB 2023, A.IV.1.

kobewertung bei den zentralisierten und standardisierten Projekten der Verwaltungsdigitalisierung, wie etwa der Einführung von IKT-Basisdiensten oder großen IT-Fachverfahren, komplex, da eine Vielzahl öffentlicher und privater Stellen einbezogen ist und oft umfangreich personenbezogene Daten verarbeitet werden.[107]

Wir stellen immer wieder fest, dass bereits sehr grundsätzliche Fragen, z. B. ob überhaupt personenbezogene Daten betroffen sind, nicht ausreichend geklärt werden. Darüber hinaus zeigt sich, dass die Beachtung der Vorgaben des Datenschutzes häufig nicht rechtzeitig in den Blick genommen wird. Dies kann dann im weiteren Verlauf der Projektumsetzung zu einem Problem werden oder Verzögerungen hervorrufen. Häufig besteht auch Unklarheit darüber, wer in einem Projekt für die Umsetzung der Anforderungen des Datenschutzes verantwortlich ist. Dabei ist weder die Rolle der behördlichen Datenschutzbeauftragten der Verwaltungen noch unsere Rolle ausreichend bekannt.

Der Standardprozess Datenschutz orientiert sich vor diesem Hintergrund an dem verbindlichen Projektmanagementhandbuch[108] der Berliner Verwaltung und formuliert dreizehn konkrete Schritte zu den Anforderungen des Datenschutzes, die den einzelnen Prozessschritten des Projektmanagementhandbuchs zugeordnet sind. Dabei zeigt sich, dass ein modernes Projektmanagement viele Ansatzpunkte für die Umsetzung des Datenschutzes bietet. So sind z. B. die Vorgaben der DSGVO als sachliche Umfeldfaktoren bereits in die zu Beginn des Projekts durchzuführende Projektumfeldanalyse und Machbarkeitsprüfung einzustellen. Ferner können die verantwortlichen Behörden die Risikoanalyse aus Sicht des Datenschutzes bereits in das während der Planungsphase zu implementierende Chancen- und Risikomanagement integrieren. Diese Orientierung an den Standards des Projektmanagements gewährleistet, dass die verantwortlichen Behörden die Vorgaben des Datenschutzes strukturiert und vor allem rechtzeitig umsetzen.

Flankiert wird der Standardprozess Datenschutz durch eine Rollenmatrix, die einen Überblick darüber bietet, wann welche Rollen der Datenschutzaufsicht, insbesondere die behördlichen Datenschutzbeauftragten, einzubeziehen sind. Schließlich stellen wir der Verwaltung drei Handreichungen (I bis III) zu den wichtigsten Prozessschritten des Standardprozesses Datenschutz zur Verfügung, die fachliche Antworten auf die immer

[107] Ebd.

[108] Abrufbar im Innennetz der Berliner Verwaltung unter https://www.berlin.de/rbmskzl/skzl-intern/artikel.351090.php. Der Standardprozess Datenschutz wird als Anlage in das Projektmanagementhandbuch aufgenommen.

wieder im Zusammenhang mit Digitalisierungsvorhaben gestellten Fragen geben.

- So fasst Handreichung I die acht typisch-relevanten Fragen zum Datenschutz zusammen, die bereits im Rahmen der Projektumfeldanalyse und der Machbarkeitsprüfung zu klären sind, und gibt Hilfestellungen zur Beantwortung. Es ist z. B. zu prüfen, ob in dem geplanten Projekt überhaupt eine Verarbeitung personenbezogener Daten i. S. d. DSGVO[109] erfolgt. Ferner müssen die zuständigen Behörden feststellen, welche der beteiligten Stellen für die konkrete Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich ist[110] und welche Stellen die personenbezogenen Daten nur im Auftrag[111] verarbeiten. Ist eine Verarbeitung personenbezogener Daten geplant, müssen die verantwortlichen Behörden als Teil der Machbarkeitsprüfung feststellen, ob diese Verarbeitung rechtmäßig ist[112] oder ob ggf. eine entsprechende Rechtsgrundlage durch Anpassung des Fachrechts erst geschaffen werden müsste.
- Handreichung II gibt den Behörden einen Überblick, welche Aspekte aus Sicht des Datenschutzes im Rahmen eines möglichen Vergabeverfahrens zu berücksichtigen sind.
- Handreichung III gibt sodann, aufbauend auf Handreichung I, eine konkrete Methodik zur Durchführung der Risikobewertung vor. Daraus ergeben sich klare Leitlinien zur Datenschutzprüfung, die dann auch die Erstellung von Rahmendatenschutz- und Datenschutzkonzepten sowie Datenschutz-Folgenabschätzungen ermöglichen.

Die Handreichungen stützen sich auf die Standards der DSK, wie etwa auf das Standard-Datenschutzmodell[113] oder die Kurzpapiere 5 (Datenschutz-Folgenabschätzung nach Art. 35 DSGVO) und 18 (Risiko für die Rechte und Freiheiten natürlicher Personen)[114], und bieten einen Zugang zu diesen Ressourcen.

Der Standardprozess Datenschutz dient der Verwaltung als „Hilfe zur Selbsthilfe“. Durch die klare Strukturierung der Anforderungen des Datenschutzes in Prozessschritten, die auf das ohnehin für Digitalisierungsprojekte der Verwaltung zu verwendende Projektmanagementhandbuch zugeschnitten sind, können die ver-

[109]Siehe Art. 4 Nr. 1 und 2 DSGVO.
[110]Siehe Art. 4 Nr. 7 DSGVO.
[111]Siehe insbesondere Art. 28 Abs. 3 DSGVO.
[112]Siehe Art. 6 Abs. 1 DSGVO.
[113]Abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/SDM-Methode-V31.pdf.
[114]Alle DSK-Kurzpapiere sind abrufbar unter https://www.datenschutz-berlin.de/infothek/publikationen-der-dsk/kurzpapiere/.

antwortlichen Behörden Digitalisierungsprojekte effektiver umsetzen und gleichzeitig fachliche Kompetenzen zum Datenschutz aufbauen. Wir werden den Standardprozess gemeinsam mit der Verwaltung weiterentwickeln und ständig evaluieren. Innerhalb der DSK setzen wir uns zudem für eine Standardisierung der Umsetzung des Datenschutzes bei länderübergreifenden Digitalisierungsvorhaben ein.

3. Digitale Akte als Testlauf für den Standardprozess Datenschutz

Wir begleiten den Prozess der Einführung der Digitalen Akte in der Berliner Verwaltung seit mehreren Jahren.[115] Wir haben uns in diesem Zusammenhang mit der IKT-Steuerung[116] verständigt, die Anwendung des von uns entwickelten Standardprozesses Datenschutz bei öffentlichen Digitalisierungsvorhaben[117] anhand des Projekts Basisdienst Digitale Akte zu pilotieren und den Standardprozess einem Praxistest zu unterziehen.

Da der Basisdienst Digitale Akte in der gesamten Berliner Verwaltung zum Einsatz kommen soll, handelt es sich um einen Dienst von besonderer Bedeutung. Seit mehreren Jahren beraten wir die IKT-Steuerung in diesem Verfahren. So haben wir frühzeitig darauf hingewirkt, dass die IKT-Steuerung, die die Verfahrensverantwortung für den Dienst trägt, ein Rahmendatenschutzkonzept entwickelt, das von den die Digitale Akte nutzenden Stellen nachgenutzt werden kann. Diese müssen dann darüber hinausgehend lediglich noch die Risiken prüfen, die sich aus den spezifischen Besonderheiten der jeweiligen Verwaltung ergeben, und in einem eigenen Datenschutzkonzept dokumentieren.

Die IKT-Steuerung wird seit Beginn des Jahres in dem Projekt zur Einführung der Digitalen Akte durch ein externes Beratungsunternehmen unterstützt. Das Rahmendatenschutzkonzept soll mit dessen Hilfe neu gefasst werden. Für dieses Rahmendatenschutzkonzept soll die Methodik des Standardprozesses Datenschutz bei öffentlichen Digitalisierungsvorhaben angewendet werden. Wir beraten und begleiten diesen Prozess, um Erfahrungen zu sammeln, wie der Standardprozess noch weiter auf die konkreten Bedürfnisse der Verwaltung abgestimmt werden kann.

Die im Rahmen des Projekts Digitale Akte gesammelten Erfahrungen zur Praxistauglichkeit des Standardprozesses werden wir evaluieren. Wir werden den Stan-

[115] Siehe JB 2023, A.IV.1.
[116] Siehe §§ 20 ff. E-Government-Gesetz Berlin (EGovG Bln).
[117] Siehe A.VI.2.

dardprozess auf Grundlage dieser und weiterer Praxiserfahrungen kontinuierlich weiterentwickeln. Wichtig ist uns dabei der regelmäßige Austausch mit der Verwaltung, den wir in einem ersten Vernetzungstreffen der Digitalisierungsmanager:innen in den Verwaltungen bereits angestoßen haben.

VII. Schule und Bildung

1. Fortschritte bei der Schuldigitalisierung

Bereits im vergangenen Jahr haben wir begonnen, in einem regelmäßigen Austausch auf der Fach- und Leitungsebene die mit der Schuldigitalisierung verbundenen datenschutzrechtlichen Herausforderungen zu erörtern. Bei einigen Projekten konnten durch unsere frühzeitige Einbindung Datenschutzbelange bereits von vornherein Berücksichtigung finden.

Wir haben uns mit der Bildungsverwaltung zur Weiterentwicklung der Berliner Lehrkräfte-Unterrichts-Schul-Datenbank (LUSD)[118] ausgetauscht. Die Bildungsverwaltung stellte dabei geplante Änderungen und neue Entwicklungen in dem IT-Fachverfahren in regelmäßigen Treffen vor, um etwaige Datenschutzfragen bzw. -risiken gemeinsam mit uns in den Blick zu nehmen. Inhaltlich richtete sich unsere Beratung in erster Linie auf die Erweiterung der Funktionalitäten des Berliner Schulportals[119] und der damit verbundenen Erweiterung von Schnittstellen zur LUSD. Beim Ausbau der digitalen Bildungsinfrastruktur kommt dem Berliner Schulportal eine besondere Bedeutung zu. Es handelt sich um ein von der Bildungsverwaltung als Schulaufsichtsbehörde betriebenes Fachverfahren, über welches Lehrkräfte, pädagogische Beschäftigte und perspektivisch auch Erziehungsberechtigte sowie Schüler:innen digitale Werkzeuge, digitale Lehr- und Lernmittel sowie weitere digitale Dienste nutzen können. Mit der jüngsten Novellierung des Schulgesetzes (SchulG) hat der Gesetzgeber nun auch die notwendige gesetzliche Grundlage für die Datenverarbeitung geschaffen.[120] Das Berliner Schulportal wird stetig um neue Funktionalitäten erweitert.

Wir haben die Erweiterung des Berliner Schulportals um einen webbasierten Noteneingabeklienten und die Digitalisierung des Verfahrens zur Erstattung von Schulversäumnisanzeigen begleitet. Mit dem Noteneingabeklienten steht den Lehrkräften erstmals eine zentrale und webbasierte Möglichkeit zur Eingabe von

[118] Siehe auch JB 2022, 4.4.6; JB 2023, A.IV.3.
[119] Siehe JB 2022, 4.4.2.
[120] Siehe A.VII.2.

Jahresabschlussnoten zur Verfügung. Die Noten können unmittelbar digital in die LUSD übertragen werden. Die Übernahme der Noten in die LUSD und der sich daran anschließende Ausdruck von Zeugnissen wird damit erheblich vereinfacht. Wir haben die Bildungsverwaltung hinsichtlich der einzuhaltenden sicherheitstechnischen Anforderungen bei der Schnittstellenimplementierung und Netzwerkarchitektur entsprechend beraten. Die Bildungsverwaltung hat unsere Hinweise umgesetzt und die entwickelten Implementierungen auch für das Verfahren der digitalen Umsetzung der Schulversäumnisanzeigen genutzt.

Diese Beratungen betrafen bisher einzelne Bereiche bzw. Anwendungen des Schulportals. Im Hinblick auf die in den vergangenen Jahren entwickelte Gesamtarchitektur des Berliner Schulportals und damit auch der IT-sicherheitstechnischen Gegebenheiten sind allerdings noch wesentliche Fragen offen. Dies haben wir gegenüber der Bildungsverwaltung in unseren Gesprächen angemahnt und beabsichtigen, die Gesamtarchitektur in den nächsten Monaten prioritär in den Blick zu nehmen. Parallel dazu begleiten wir die Bildungsverwaltung bei der Durchführung weiterer Digitalisierungsprojekte, wie etwa der Einführung eines digitalen Klassenbuchs.

Das Datenflussmodell des Berliner Schulportals befand sich im Jahr 2024 in der Erarbeitungsphase und wurde zwischenzeitlich im Rahmen des gemeinsamen strukturierten Austauschs der Berliner Beauftragten für Datenschutz und Informationsfreiheit vorgestellt.

Im Herbst haben wir aus der Presse erfahren, dass die Bildungsverwaltung den Lehrkräften über das Schulportal die KI-Anwendung Microsoft Copilot zur Verfügung stellt. Vor dem Hintergrund der zahlreichen komplexen Fragen zum Umgang mit personenbezogenen Daten bei der Nutzung von KI-Anwendungen im Schulkontext haben wir ein formelles Verfahren eröffnet und die Bildungsverwaltung zunächst um Stellungnahme gebeten.

Es ist zutreffend, dass pädagogische Beschäftigte über ihr dienstliches mobiles Endgerät (MEG) sowie über das Berliner Schulportal (BSP) Zugang zu Microsoft Copilot erhalten, allerdings erst nach erfolgter Authentifizierung. Diese Authentifizierung gewährleistet, dass Microsoft Copilot im sogenannten „Enterprise data protection“-Modus (Unternehmensdatenschutz) betrieben wird.
In diesem Modus werden Eingabeaufforderungen und Antworten ausschließlich innerhalb der Microsoft 365-Dienstgrenzen verarbeitet. Die von Microsoft Copilot bereitgestellten Antworten basieren ausschließlich auf öffentlich zugänglichen Internetdaten. Personenbezogene Nutzenden- und Organisationsdaten bleiben geschützt.
Weder Prompts noch Antworten werden zur Weiterentwicklung oder zum Training der zugrundeliegenden großen Sprachmodelle verwendet. Zudem sind alle Chatdaten, die im Rahmen des Unternehmensdatenschutzes übertragen werden, sowohl während der Übertragung als auch im Ruhezustand verschlüsselt.
Die Senatsverwaltung für Bildung, Jugend und Familie (SenBJF) hat ergänzend zu den bestehenden technischen Maßnahmen auch organisatorische Vorkehrungen zur datenschutzkonformen Nutzung

von Microsoft Copilot getroffen. Es ist den Nutzenden ausdrücklich untersagt, personenbezogene Daten in den Dienst einzugeben. Ebenso ist der Einsatz von Copilot für Bewertungen oder zur Kontrolle von Prüfungsleistungen unzulässig.
Zur weiteren Sensibilisierung der Nutzenden plant die SenBJF, die organisatorischen Maßnahmen auszuweiten.
Darüber hinaus befindet sich die SenBJF in Gesprächen mit Microsoft mit dem Ziel, den bestehenden Auftragsverarbeitungsvertrag an die Anforderungen der Datenschutzkonferenz anzupassen.

Durch den mittlerweile etablierten und strukturierten Austausch mit der Bildungsverwaltung konnten wir erreichen, dass wir bei einigen neuen Projekten frühzeitig eingebunden wurden und unsere Expertise zur Verfügung stellen konnten. Dennoch lässt sich der Austausch noch weiter verbessern, insbesondere im Hinblick auf die Rückmeldungen, inwieweit unsere Empfehlungen umgesetzt wurden. Wir erwarten, dass unsere Einbindung zukünftig bei allen wesentlichen Projekten rechtzeitig erfolgt, damit wir gemeinsam mit der Bildungsverwaltung die richtigen Weichen für eine datenschutzgerechte und zukunftsgerichtete Schuldigitalisierung stellen können.

Die SenBJF zeigt sich äußerst erfreut über den konstruktiven und produktiven fachlichen Austausch mit der Berliner Beauftragen für Datenschutz und Informationsfreiheit. Die darin zum Ausdruck kommende Expertise wird von der SenBJF sehr geschätzt und als wertvolle Grundlage für die weitere Zusammenarbeit betrachtet.
Dem Schutz personenbezogener Daten wird hohe Priorität eingeräumt, um sowohl den rechtlichen Anforderungen als auch den berechtigten Erwartungen der Betroffenen gerecht zu werden. Vor diesem Hintergrund beabsichtigt die SenBJF, die bereits etablierten Formate der Kooperation weiterhin konsequent beizubehalten und auszubauen.
Im Rahmen dieser Zusammenarbeit soll die Berliner Beauftragte für Datenschutz und Informationsfreiheit auch in zukünftigen Projekten und Vorhaben frühzeitig und umfassend eingebunden werden, um datenschutzrechtliche Fragestellungen von Beginn an berücksichtigen zu können und somit eine datenschutzkonforme Umsetzung sicherzustellen.
Die SenBJF bekräftigt ihr Engagement, die von der Berliner Beauftragten für Datenschutz und Informationsfreiheit formulierten Empfehlungen ernst zu nehmen und im Rahmen ihrer Zuständigkeiten sorgfältig umzusetzen. Dadurch wird eine nachhaltige Verbesserung des Datenschutzes in den entsprechenden Fachbereichen angestrebt.

2. Novellierung schulgesetzlicher Normen

Zum Schuljahr 2024/25 ist das SchulG um eine Reihe datenschutzrechtlicher Vorschriften ergänzt worden.[121] *Wir haben die Bildungsverwaltung bereits im Vorfeld des Gesetzgebungsverfahrens beraten und auch schriftlich Stellung genommen. Viele der von uns unterbreiteten Vorschläge wurden übernommen und haben Eingang in das novellierte Gesetz gefunden.*

[121] Zweites Gesetz zur Änderung des Schulgesetzes und weiterer Rechtsvorschriften vom 10. Juli 2024, GVBl. 2024, S. 465 ff.

Wir begrüßen, dass mit der Novellierung der schulgesetzlichen Vorschriften eine Rechtsgrundlage für das Berliner Schulportal geschaffen worden ist. Mit dem Berliner Schulportal ermöglicht die Bildungsverwaltung den Zugang zu digitalen Lehr- und Lernmitteln sowie digitalen Kommunikationswerkzeugen. Zudem soll über das Berliner Schulportal auch eine Verarbeitung der im Fachverfahren LUSD gespeicherten personenbezogenen Daten für Zwecke der Verwaltung hinsichtlich der Schüler:innen sowie der Schulorganisation ermöglicht werden. Mit § 64d SchulG wird dafür eine Norm geschaffen, die den rechtlichen Rahmen für die notwendigen Datenverarbeitungen vorgibt und insbesondere deren Zwecke beschreibt. Exemplarisch zu nennen sind neben dem Zugang zu digitalen Lehr- und Lernmitteln sowie digitalen Kommunikationsmitteln auch die Feststellung der Anwesenheit der Schüler:innen und deren Dokumentation, die Meldung und Entschuldigung von Abwesenheiten, die Dokumentation zeugnisrelevanter Informationen und Leistungsnachweise sowie weitere Zwecke der Schulorganisation wie die Kurs- und Fächerwahl. Konkret werden damit Möglichkeiten geschaffen, z. B. ein digitales Klassenbuch einzurichten oder die Notenerfassung zu erleichtern. Gleichzeitig enthält die Vorschrift Regelungen, die sicherstellen, dass ein Zugriff auf die in der LUSD gespeicherten Daten von Schüler:innen nur durch authentifizierte und autorisierte Personen erfolgen kann.

Da die gesetzliche Regelung lediglich den rechtlichen Rahmen für das Berliner Schulportal vorgeben kann, bedarf es weiterer Vorschriften für das Verfahren der konkreten Datenverarbeitung sowie der technisch-organisatorischen Maßnahmen zum Schutz der Daten. Konkret folgt daraus die Notwendigkeit, die Schuldatenverordnung (SchuldatenV) um entsprechende Regelungen zu ergänzen.

Eine weitere wichtige Neuregelung wurde mit § 58 Abs. 2 Satz 2 SchulG geschaffen. Diese Vorschrift sieht nun die Möglichkeit vor, zusätzliche Ausfertigungen und Zweitschriften von Zeugnissen auch in elektronischer Form auszustellen. Ergänzt wird die Vorschrift durch eine Änderung des § 2 Abs. 2 Satz 2 Gesetz über das Verfahren der Berliner Verwaltung (VwVfG Bln), der bislang lediglich die Papierform zuließ.

Mit der Novellierung des SchulG ebnet der Gesetzgeber den Weg für eine weitere Fortentwicklung der Schuldigitalisierung und nimmt die praktischen Bedürfnisse der Schulen nach weiteren Funktionalitäten

in den Blick. Die untergesetzlichen Umsetzungsvorschriften müssen jetzt zügig angepasst werden. In diesem Rahmen ist es notwendig, auch die bereits zum Schuljahr 2023/24 mit der SchuldatenV und der Digitalen Lehr- und Lernmittelverordnung (DigLLV)[122] in Kraft getretenen Regelungen zum Umgang mit personenbezogenen Daten in der Schule hinsichtlich ihrer Praxistauglichkeit auf den Prüfstand zu stellen. Wir stehen der Bildungsverwaltung mit unserer Expertise beratend zur Seite.

VIII. Jugend und Soziales

1. Berliner Datenschutzwegweiser für Kitas

Die Senatsverwaltung für Bildung, Jugend und Familie (SenBJF) hat einen digitalen „Berliner Datenschutzwegweiser für Kitas“ veröffentlicht.[123] Das Angebot richtet sich an Kitafachkräfte und Träger, bietet praxisnahe Unterstützung und schafft mehr Transparenz bei Datenschutzfragen im Kitaalltag. Wir haben bei den fachlichen Inhalten des Angebots mitgewirkt. Die neue Website ist eine Ergänzung zur etablierten Broschüre „Datenschutz bei Bild-, Ton- und Videoaufnahmen – Was ist in der Kindertageseinrichtung zu beachten?“ des Landes Berlin, die sich als wertvolles Nachschlagewerk bewährt hat und die wir gemeinsam mit der Senatsverwaltung verfasst haben.

Von Fotos bei Veranstaltungen über digitale Medien bis hin zur Dokumentation – im Kitaalltag spielen die Daten von Kindern eine wichtige Rolle. In diesem Zusammenhang kommen bei den Fachkräften immer wieder Fragen zum Datenschutz auf. So erhalten wir bspw. seit vielen Jahren zahlreiche Anfragen zum Umgang mit Bild-, Video- und Tonaufnahmen.[124] Gemeinsam mit der zuständigen Senatsverwaltung entstand daher die Idee, eine praktische Handlungshilfe für die Erzieher:innen in Kindertageseinrichtungen und auch für den Bereich der Kindertagespflege zu entwickeln.[125] Die Broschüre „Datenschutz bei Bild-, Ton- und Videoaufnahmen – Was ist in der Kindertageseinrichtung zu beachten?“ liegt nunmehr in der 2. Auflage vor.[126]

Um die gängigen datenschutzrechtlichen Fragen auch in einer digitalisierten Form aufzubereiten, hat SenBJF nun eine multimediale Plattform entwickelt. Eine Arbeitsgruppe sammelte Fragen von Praktiker:innen und

[122] Siehe JB 2023, A.I.2.
[123] https://www.datenschutzwegweiser-kita.de/home.
[124] Siehe z. B. JB 2019, 5.1; JB 2020, 4.2; JB 2022, 4.3.
[125] Siehe JB 2018, 5.4; JB 2020, 4.2.
[126] Abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/broschueren/2020-BlnBDI-Datenschutz_Bild_Ton_Video.pdf.

formulierte Antworten. Dabei orientierte sie sich vor allem an den praktischen Bedürfnissen. Kernstück des neuen Onlineangebots sind daher die umfangreichen FAQ, die gezielt häufig gestellte Fragen zum Thema Datenschutz beantworten. Diese wurden speziell für den pädagogischen Alltag entwickelt. Der Fokus liegt darauf, die Informationen einfach und verständlich zu vermitteln, sodass Fach- und Leitungskräfte sowie Träger rasch Antworten auf dringende Fragen finden, aber auch Eltern sich gut informieren können. Die Beantwortung der Fragen haben wir mit unserer fachlichen Expertise unterstützt.

Der multimediale Wegweiser soll die Kitas dabei unterstützen, die Datenschutzbestimmungen kompetent umzusetzen und die Rechte der Kinder konsequent zu wahren. Als Berliner Datenschutzaufsicht haben wir uns an der Entwicklung des Wegweisers beteiligt, um Kitafachkräften den rechtssicheren Umgang mit Daten von Kindern zu erleichtern.

2. Kinder- und Jugendschutz als zentrales Anliegen

Im Rahmen mehrerer Beratungen haben wir SenBJF und die Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung (SenASGIVA) bei der Erarbeitung von verschiedenen Handlungsleitfäden und Konzepten zum Kinderschutz unterstützt. In diesen Leitfäden geht es in erster Linie um praktische Anweisungen an freie Träger aus dem Jugend- und Sozialbereich, wie bei einem Verdacht auf eine Kindeswohlgefährdung zu verfahren ist.

Zum Schutz von betroffenen Kindern und Jugendlichen ist es von erheblicher Bedeutung, dass Fachkräfte bei Einrichtungen der freien Jugendhilfe und bei sozialen Trägern erkennen können, ob eine Kindeswohlgefährdung vorliegt, und wissen, wie in solchen Fällen zu verfahren ist. Um Unsicherheiten der meist gesetzlich zur Verschwiegenheit verpflichteten Fachkräfte zu beseitigen, erarbeiten SenBJF und SenASGIVA derzeit verschiedene Handlungsleitfäden und Konzepte. Wir unterstützen die Verwaltungen dabei.

In Fällen des Verdachts auf eine Kindeswohlgefährdung ist es besonders wichtig, dass die Fachkräfte die einzelnen Schritte kennen, die diesbezüglich gesetzlich vorgesehen sind, und auch wissen, unter welchen Voraussetzungen personenbezogene Daten weitergegeben werden dürfen.[127] Werden Fachkräften in Ausübung ihrer beruflichen Tätigkeit gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder Jugendlichen bekannt, so sollen sie gemeinsam mit dem Kind

[127]Siehe § 4 Gesetz zur Kooperation und Information im Kinderschutz (KKG).

oder Jugendlichen und den Erziehungsberechtigten die Situation erörtern und, soweit erforderlich, bei den Erziehungsberechtigten auf die Inanspruchnahme von Hilfen hinwirken. Dabei darf der wirksame Schutz des Kindes oder Jugendlichen nicht in Frage gestellt werden. Zur fachlichen Einschätzung der Kindeswohlgefährdung haben die Fachkräfte außerdem einen Anspruch auf Beratung durch eine „insoweit erfahrene Fachkraft“[128].

Zum Zwecke der Beratung dürfen die Fachkräfte die dafür erforderlichen Daten an die insoweit erfahrene Fachkraft übermitteln. Die Daten sind allerdings vor einer Übermittlung zu pseudonymisieren.[129] Scheidet eine Abwendung der Gefährdung durch die Fachkräfte der Jugendhilfeeinrichtungen oder anderer sozialer Einrichtungen aus oder bleibt die Erörterung mit den Familien und das Bemühen, auf die Inanspruchnahme von Hilfen hinzuwirken, erfolglos, so dürfen die Fachkräfte das Jugendamt informieren. Dies setzt voraus, dass die Fachkräfte ein Tätigwerden des Jugendamts für erforderlich halten, um eine Gefährdung des Wohls eines Kindes oder eines Jugendlichen abzuwenden.[130] Die Fachkräfte sollen die Kinder und Jugendlichen sowie die Erziehungsberechtigten vorab auf eine Meldung an das Jugendamt hinweisen, es sei denn, dass damit der wirksame Schutz des Kindes oder Jugendlichen in Frage gestellt wird.[131] Den Fachkräften ist die Weitergabe der notwendigen Informationen an das Jugendamt in solchen Fällen gesetzlich erlaubt. Nachdem das Jugendamt von einer Fachkraft informiert wurde, soll es ihr zeitnah eine Rückmeldung geben, ob es die gewichtigen Anhaltspunkte für die Gefährdung des Wohls des Kindes oder Jugendlichen bestätigt sieht und ob es zum Schutz des Kindes oder Jugendlichen tätig geworden ist bzw. noch tätig ist.[132]

Mit den Handlungsleitfäden sollen Unsicherheiten der Fachkräfte bei der Abwendung und Verhinderung von Kindeswohlgefährdungen in der Praxis beseitigt werden. Den Fachkräften wird damit die notwendige Rechtssicherheit gegeben, welche konkreten Schritte zu befolgen sind und wann welche Informationen an das Jugendamt weitergegeben werden dürfen.

[128]Eine „insoweit erfahrene Fachkraft“ ist die gesetzlich festgelegte Bezeichnung für die beratende Person zur Einschätzung des Gefährdungsrisikos bei einer vermuteten Kindeswohlgefährdung. Die insoweit erfahrene Fachkraft zeichnet sich durch eine Zusatzausbildung und besondere Expertise aus.
[129]§ 4 Abs. 2 KKG.
[130]§ 4 Abs. 3 KKG.
[131]Ebd.
[132]§ 4 Abs. 4 KKG.

3. Multiinstitutionelle Fallkonferenzen in Hochrisikofällen

Unter Verweis auf den Berliner Landesaktionsplan zur Umsetzung des Übereinkommens des Europarats zur Bekämpfung und Verhütung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention) vom 18. Oktober 2023[133] plant SenASGIVA u. a. die Einrichtung multiinstitutioneller, interdisziplinärer Fallkonferenzen. Unter Federführung der Senatsverwaltung hat eine bereits vor einigen Jahren eingesetzte institutionsübergreifende Arbeitsgruppe, bestehend aus Vertreter:innen der Polizei, der Justiz und weiterer Behörden sowie des Frauenhilfesystems, ein Konzept zur Durchführung entsprechender Fallkonferenzen in Hochrisikofällen bei häuslicher Gewalt und Trennungsstalking erarbeitet.

Bei den multiinstitutionellen Fallkonferenzen sollen mehrere Institutionen, die mit dem Schutz der betroffenen Frauen und ggf. ihrer Kinder sowie der Gefahrenabwehr bzw. Strafverfolgung befasst sind, wie etwa Frauenhäuser, Beratungsstellen, Polizei und Jugendamt, gemeinsam an einem Tisch sitzen und einen Austausch zu konkreten Einzelfällen durchführen. Das von der Arbeitsgruppe erarbeitete Konzept sieht mangels eigener gesetzlicher Grundlage für die Durchführung solcher multiinstitutioneller Fallkonferenzen in Hochrisikofällen vor, diese auf Einwilligungserklärungen der betroffenen Frauen zu stützen. Ein behörden- und institutionsübergreifender Austausch personenbezogener Daten berührt jedoch in besonderer Weise datenschutzrechtliche Grundpositionen und ist daher rechtlich genau zu betrachten.

Im Rahmen von multiinstitutionellen Fallkonferenzen sollen personenbezogene Daten der betroffenen Frauen und von Dritten zwischen allen an der Konferenz beteiligten Institutionen ausgetauscht werden. Für jede einzelne dieser Datenübermittlungen zwischen den an der Konferenz Beteiligten muss ein datenschutzrechtlicher Erlaubnistatbestand vorliegen, der jeweils die Übermittlung der personenbezogenen Daten an alle beteiligten Institutionen zulässt. So muss es bspw. zulässig sein, wenn ein Frauenhaus im Rahmen einer Fallkonferenz Daten gleichzeitig an die Polizei, das Jugendamt oder das Gesundheitsamt weitergibt. Entsprechende Regelungen zu einem solchen ressortübergreifenden Austausch sehen das Datenschutzrecht und das jeweilige Fachrecht im Regelfall jedoch nicht vor. Vielmehr ist es nach den gesetzlichen Regelungen jeweils im Einzelfall zu prüfen, mit welchen Institutionen welche Informationen ausgetauscht werden dürfen.

[133] Abghs.-Drs. 19/1248.

Dass entsprechende gesetzliche Regelungen zum ressortübergreifenden Austausch nicht gegeben sind, liegt daran, dass die beteiligten Institutionen unterschiedliche Ziele verfolgen: Während Frauenhäusern und Beratungseinrichtungen daran gelegen ist, für die betroffenen Frauen Sicherheit und Unterstützung anzubieten, verfolgt das Jugendamt zuvorderst den Schutzauftrag bei Kindeswohlgefährdung; gesetzliche Aufgabe der Gesundheitseinrichtungen ist es, das Wohl und die Gesundheit ihrer Patient:innen zu schützen. In allen diesen Institutionen wird ein hoher Stellenwert der Vertraulichkeit eingeräumt, die durch eine entsprechende gesetzliche Schweigepflicht der Beschäftigten flankiert wird. Die Polizei und Staatsanwaltschaft wiederum unterliegen dem Legalitätsprinzip und sind daher verpflichtet, ein Ermittlungsverfahren zu eröffnen, sofern zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen.[134]

Daraus folgt, dass die Weitergabe bzw. der Austausch personenbezogener Daten zwischen einzelnen Institutionen zwar im konkreten Einzelfall aufgrund der bestehenden gesetzlichen Befugnisse zulässig sein kann – nicht jedoch zwangsläufig eine Datenweitergabe an alle an der Fallkonferenz beteiligten Institutionen. Die von SenASGIVA als rechtliche Grundlage für die Fallkonferenzen in den Blick genommene Einwilligung der Frauen in eine Weitergabe an alle Institutionen birgt rechtliche Hürden und führt zu Rechtsunsicherheit. Es ist nicht vorhersehbar, welche Informationen im Verlauf einer Fallkonferenz zusammengeführt werden und welche Folgen sich daraus ergeben können. Dies gilt insbesondere im Hinblick auf eine Beteiligung der Strafverfolgungsbehörden und der Jugendämter, die bei zureichenden tatsächlichen Anhaltspunkten für eine Straftat oder eine Kindeswohlgefährdung zum Tätigwerden verpflichtet sind. Die Entscheidung hierüber steht daher nicht zur Disposition der Frauen. Da eine Einwilligung jedoch nur wirksam ist, wenn sie informiert und transparent erfolgt, halten wir sie in diesem Kontext nicht für geeignet. Daten dürfen keinesfalls hinter dem Rücken der betroffenen Frauen ausgetauscht werden.

Wir haben SenASGIVA seit Jahresbeginn mehrfach unsere Beratung angeboten. Erst nach Medienberichten im Sommer hat SenASGIVA unser Beratungsangebot angenommen und im Oktober ein erstes Konzept vorgelegt. Wir mussten feststellen, dass es erhebliche Mängel aufweist und von uns nicht mitgetragen werden kann.

[134] § 152 Abs. 2 Strafprozessordnung (StPO).

So fehlte im Konzept bspw. eine Beschreibung der Szenarien, bei denen eine Fallkonferenz eingesetzt werden soll, und eine Beschreibung, wann und aus welchen Gründen welche Institutionen an einer Fallkonferenz teilnehmen sollen. Zudem fehlte es an unbedingt erforderlichen praxisbezogenen Handlungsleitfäden, bspw. dazu, wie die Fachkräfte die Frauen hinreichend aufklären und eine Einwilligung rechtssicher einholen können. Auch sah das Konzept vor, dass die betroffenen Frauen nicht an der Fallkonferenz teilnehmen dürfen. Nicht ausreichend beleuchtet war auch das Verhältnis von Einwilligung und nicht zur Disposition stehenden gesetzlichen Befugnissen. -SenASGIVA konnte uns zudem nicht beantworten, welche konkreten Informations-defizite trotz bestehender gesetzlicher Möglichkeiten des Informationsaustauschs in der Vergangenheit entstanden sind und wie diese Defizite zu verminderten Möglichkeiten der Verhinderung von Gewalteskalation geführt haben. Auf unsere Nachfrage wurde uns mitgeteilt, dass SenASGIVA keine Aufarbeitung der Fälle von Frauentötungen der letzten Monate und Jahre im Hinblick auf diese Fragestellungen durchgeführt hat. Eine Antwort, wie die vorgeblichen Defizite durch Fallkonferenzen gelöst werden können, konnte SenASGIVA ebenfalls nicht geben. Im Wesentlichen wurde deutlich, dass die Fallkonferenz der Bündelung von Kompetenzen und Fachwissen dienen soll.

Bei uns ist der Eindruck entstanden, dass die in der Praxis wahrgenommenen Pro-bleme darauf zurückzuführen sind, dass Behörden und Fachkräften oftmals die datenschutzrechtlichen Befugnisse zum Austausch mit anderen Behörden (die ihnen in solchen Hochrisikofällen ohnehin häufig bereits aufgrund der bestehenden gesetzlichen Regelungen zur Verfügung stehen) nicht bekannt sind und daher nicht ausreichend genutzt werden. Vielmehr wurde pauschal auf angebliche Hindernisse durch den Datenschutz hingewiesen, ohne dass SenASGIVA bzw. die anderen Beteiligten der Arbeitsgruppe dies untermauern konnten. Wir haben daher vorgeschlagen, gemeinsam mit der Senatsverwaltung praxisbezogene Handlungsleitfäden für die einzelnen Institutionen zu erarbeiten, um Fachkräften die notwendige Sicherheit in Bezug auf die bestehenden Befugnisse geben und ausloten zu können, an welcher Stelle ggf. Defizite bestehen könnten. Auf dieses Angebot ist SenASGIVA nicht eingegangen. Vielmehr haben SenASGIVA und die Senatsverwaltung für Inneres und Sport (SenInnSport) in einer gemeinsamen Presseerklärung mitgeteilt, die multiinstitutionellen Fallkonferenzen einzuführen.[135] Offen bleibt, wie das

[135]Pressemitteilung vom 22. November 2024, abrufbar unter https://www.berlin.de/sen/asgiva/presse/pressemitteilungen/2024/pressemitteilung.1505927.php.

von SenASGIVA uns gegenüber benannte Ziel, datenschutzrechtliche Bestimmungen bei den Fallkonferenzen unbedingt einzuhalten, trotz der bestehenden Mängel am Konzept und der rechtlichen Hürden erreicht werden soll.

Die Durchführung multiinstitutioneller, interdisziplinärer Fallkonferenzen wirft zahlreiche rechtliche Fragen auf. Dass datenschutzrechtliche Bestimmungen bei der Durchführung von Fallkonferenzen eingehalten werden, ist unabdingbar. Ein mit rechtlichen Mängeln behaftetes Verfahren birgt die Gefahr von Verwertungsverboten in Strafverfahren gegen potenzielle Täter:innen und von Verstößen gegen gesetzliche Verschwiegenheitspflichten mit strafrechtlicher Relevanz. Wir werden die weitere Entwicklung und Umsetzung des Konzepts durch SenASGIVA aufmerksam verfolgen.

IX. Forschung und Gesundheit

1. Hilfestellung bei der KIS-Beschaffung

Der Hersteller eines verbreiteten Krankenhausinformationssystems (KIS) kündigte seinen Rückzug aus dem entsprechenden Marktsegment und die Einstellung des Supports an. Dies zwingt Krankenhäuser, die Systeme dieses Herstellers einsetzen, dazu, in absehbarer Zeit neue Systeme zu beschaffen. Auch die Charité gehört zu den betroffenen Unternehmen. Wir unterstützen das Universitätsklinikum darin, beim anstehenden Wechsel datenschutzrechtliche Aspekte zu berücksichtigen.

Im Herbst 2022 kündigte der Hersteller das Ende der Verfügbarkeit seiner Systeme und damit einhergehend das Ende der laufenden Wartungs- und Supportverträge bis spätestens 2030 an. Betroffene Krankenhäuser stehen nun vor der Aufgabe, ein neues KIS anzuschaffen. Bereits bei den entsprechenden Ausschreibungen müssen auch datenschutzrechtliche Anforderungen beachtet werden, um eine Nutzung des Systems nach der Datenschutz-Grundverordnung (DSGVO) zu ermöglichen.

Im Rahmen regelmäßiger Gespräche mit der Charité boten wir unsere Unterstützung bei der Ausgestaltung der Ausschreibungstexte in Bezug auf datenschutzrechtliche Anforderungen an. Bereits in der ersten uns übersandten Fassung des Ausschreibungstextes hatte die Charité wesentliche Teile der sich aus dem Datenschutzrecht ergebenden Anforderungen berücksichtigt. Insbesondere die von uns herausgestellten Punkte der Zugriffssteuerung und -protokollierung, der Bereitstel-

lung eines Verfahrens zur Unterstützung der Gewährung der Betroffenenrechte sowie von Funktionalitäten für eine fristgemäße Löschung von Patientenakten nach der Krankenhaus-Verordnung (KhsVO) fanden sich wieder.

Darüber hinaus regten wir an, in der Finalisierung des Ausschreibungstexts weitere Aspekte aufzunehmen. Zum einen sollte das KIS Funktionalitäten zur nachträglichen Überprüfung von Zugriffen auf Patientendaten aufweisen. Diese sollen automatisierte Prüfungen von Zugriffsberechtigungen umfassen, aber auch eine stichprobenhafte Kontrolle von Zugriffen ermöglichen, bei denen über die Zulässigkeit des Zugriffs nicht automatisiert entschieden werden konnte. Zum anderen sollten die Anforderungen zum Rollen- und Berechtigungskonzept berücksichtigen, dass es sich bei einem Krankenhausbetrieb um ein hochdynamisches Umfeld handelt. Es sind daher Mechanismen und Funktionalitäten nötig, die es ermöglichen, eine solche Dynamik insbesondere bei einer Erweiterung der an der Behandlung von Patient:innen Beteiligten ohne gesteigerten Aufwand für die medizinischen Fachkräfte abzubilden. Hier empfahlen wir der Charité, sich an den Verfahren für häufig auftretende Szenarien zu orientieren, die in der von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereitgestellten Orientierungshilfe beschrieben sind.[136]

Wir begrüßen sehr, dass im Ergebnis auch diese von uns vorgebrachten Empfehlungen berücksichtigt wurden. Der konstruktive Dialog führte damit dazu, dass sich wichtige datenschutzrechtliche Anforderungen im Ausschreibungstext für die Beschaffung eines neuen KIS wiederfinden. Nur die Erfüllung dieser Anforderungen durch die im Ausschreibungsverfahren erfolgreichen Hersteller:innen oder Anbieter:innen des zu beschaffenden Systems wird das Klinikum in die Lage versetzen, das neue KIS datenschutzkonform einzusetzen.

Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte bereits bei öffentlichen Ausschreibungen Rechnung getragen werden.[137] Dies gilt sowohl für die im Ausschreibungstext niedergelegten Anforderungen als auch für die Entscheidung über den Zuschlag: Nur solche Produkte, Dienste und Anwendungen können später eingesetzt werden, die unter Berücksichtigung des

[136]Orientierunghilfe KIS, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/201403_oh_krankenhausinformationssysteme.pdf.
[137]Siehe Erwägungsgrund (ErwGr.) 78 Satz 4 DSGVO.

Stands der Technik so gestaltet wurden, dass der Verantwortliche in der Lage ist, seinen Datenschutzpflichten nachzukommen.

2. Aufsichtszuständigkeit für Unternehmen zur Onlinebuchung von Arztterminen (Fortsetzung)

Verarbeiten Verantwortliche personenbezogene Daten grenzüberschreitend, ist diejenige Aufsichtsbehörde federführend zuständig, in deren Hoheitsgebiet die Hauptniederlassung oder die einzige Niederlassung des Verantwortlichen liegt.[138] Entscheidet eine Konzernmutter, die Tochterunternehmen in mehreren Mitgliedstaaten der Europäischen Union (EU) hat, über die Zwecke und Mittel bestimmter Verarbeitungen und handelt es sich bei diesen um grenzüberschreitende Verarbeitungen, ist die Aufsichtsbehörde desjenigen Mitgliedstaats, in dem die Konzernmutter ihren Sitz hat, federführend zuständig.

In der Datenschutzinformation[139] und dem Verarbeitungsverzeichnis[140] eines Unternehmens, das eine Internetplattform zur Buchung von Arztterminen betreibt, war ein Tochterunternehmen mit Sitz in Berlin als Verantwortliche für die Datenverarbeitungen, die im Zusammenhang mit der deutschen Internetplattform erfolgen, angegeben. Auf unsere Nachfrage hin bestätigte uns das Tochterunternehmen, über das wir bereits berichtet haben,[141] seine Stellung als Verantwortliche, vertrat uns gegenüber aber wiederholt die Ansicht, nicht wir, sondern die Aufsichtsbehörde des Mitgliedstaats, in dem die Muttergesellschaft ihren Sitz hat, sei zuständige Aufsichtsbehörde.[142] Diese Auffassung zur Zuständigkeit war nicht nachvollziehbar.[143] Denn Art. 56 Abs. 1 DSGVO setzt das Vorliegen einer grenzüberschreitenden Verarbeitung des Verantwortlichen voraus und knüpft die Zuständigkeit der Aufsichtsbehörde insbesondere an den Sitz der Hauptniederlassung des Verantwortlichen.

Wir suchten auch den Kontakt mit der von der deutschen Niederlassung des Unternehmens als zuständig angesehenen Aufsichtsbehörde in dem anderen Mitgliedstaat. Diese Aufsichtsbehörde wandte sich an die Konzernmutter, die erklärte, dass sie selbst Verantwortliche für die betroffenen Datenverarbeitungen durch die deutsche Tochtergesellschaft sei und es sich

[138] Art. 56 Abs. 1 DSGVO.
[139] Siehe Art. 13 DSGVO.
[140] Siehe Art. 30 Abs. 1 DSGVO.
[141] Siehe JB 2023, A.VI.1.
[142] Ebd.
[143] Ebd.

bei diesen insoweit um grenzüberschreitende Verarbeitungen handele.[144] Da die DSGVO keine parallele Verantwortung für ein- und dieselbe Verarbeitung kennt, sondern nur eine gemeinsame Verantwortung,[145] widerspricht dies der Information zur Verantwortlichkeit in der Datenschutzerklärung und den Erklärungen der deutschen Tochtergesellschaft, die sich uns gegenüber als Verantwortliche bezeichnet hatte.

Für unsere Beschwerdeverfahren hat dies zur Folge, dass Beschwerden von Menschen, die grenzüberschreitende Datenverarbeitungen der verantwortlichen Konzernmutter betreffen, nunmehr federführend im Rahmen des Kooperationsverfahrens[146] von der Aufsichtsbehörde in dem anderen Mitgliedstaat bearbeitet werden. Im Rahmen dieses Verfahrens hat die federführende Aufsichtsbehörde uns ihren Beschlussentwurf zur Stellungnahme vorzulegen und unserer Stellungnahme zu dem Beschlussentwurf gebührend Rechnung zu tragen.[147] Der endgültige Beschluss wird grundsätzlich von der federführenden Aufsichtsbehörde erlassen und dem Verantwortlichen mitgeteilt. Die Unterrichtung der beschwerdeführenden Person über das Ergebnis der Ermittlung erfolgt durch uns, sofern die Beschwerde in Deutschland eingereicht wurde.[148]

Laufende oder zukünftige Prüfungen von Amts wegen, die grenzüberschreitende Datenverarbeitungen betreffen, für die die Konzernmutter verantwortlich ist, werden nun federführend von der Aufsichtsbehörde in dem Mitgliedstaat, in dem der Verantwortliche seine Hauptniederlassung hat, geführt.

Für Unternehmen, die Datenverarbeitungen in mehreren Mitgliedstaaten der EU vornehmen, kann der in der DSGVO vorgesehene sog. One-Stop-Shop-Mechanismus zur Anwendung gelangen. Nach diesem unterliegen die von einem Verantwortlichen (oder Auftragsverarbeiter) durchgeführten grenzüberschreitenden Datenverarbeitungen federführend der Aufsicht derjenigen Aufsichtsbehörde, die für die Hauptniederlassung oder die einzige Niederlassung des Verantwortlichen (oder Auftragsverarbeiters) zuständig ist. Erklärt ein Unternehmen in seiner Datenschutzinformation, dass eine Tochterniederlassung in Deutschland Verantwortliche ist, kann nicht die Behörde eines anderen Mitgliedstaats, in dem die dann nicht verantwortliche Muttergesellschaft ihren Hauptsitz hat, federführende Behörde sein. Stellt sich allerdings heraus, dass

[144] Siehe Art. 4 Nr. 23 lit. a DSGVO.
[145] Siehe JB 2023, A.VI.1.
[146] Nach Art. 60 DSGVO.
[147] Siehe Art. 60 Abs. 3 Satz 2 DSGVO.
[148] Siehe Art. 60 Abs. 7 DSGVO.

tatsächlich nicht das Tochterunternehmen, sondern die Muttergesellschaft über die Mittel und Zwecke bestimmter Datenverarbeitungen entscheidet und damit selbst Verantwortliche ist, hat der Verantwortliche seine Informationspflichten[149] nicht erfüllt. Unternehmen sind verpflichtet, zutreffende Angaben zum Verantwortlichen für die Datenverarbeitung zu machen.

3. Prüfung einer Website zur Bestellung ärztlicher Verordnungen

Bei der Überprüfung eines Internetportals, über welches Rezeptverordnungen bei Ärzt:innen bestellt werden können, entdeckten wir zahlreiche datenschutzrechtliche Mängel. Das Unternehmen haben wir verwarnt.

Die Betreiberin des Portals verarbeitete Kontaktdaten von Ärzt:innen aus dem gesamten Bundesgebiet, damit diese über das Portal von Patient:innen zur Bestellung einer ärztlichen Verordnung kontaktiert werden konnten. Dabei wurden auch Daten von solchen Ärzt:innen auf der Plattform bereitgestellt, bei denen eine Rezeptbestellung gar nicht möglich war, da sie nicht mit der Plattform kooperierten.

Eine Rechtsgrundlage für diese Datenverarbeitungen war nicht ersichtlich. Insbesondere ließ sich die Verarbeitung der Kontaktdaten der Ärzt:innen nicht auf die Rechtsgrundlage der Interessenabwägung stützen.[150] Zwar stellt der Betrieb einer legalen Onlineplattform zur Vermittlung von Rezeptverordnungen als gewerbliches Interesse grundsätzlich auch ein berechtigtes Interesse i. S. d. DSGVO dar. Die konkrete Datenverarbeitung muss aber zur Wahrung des berechtigten Interesses auch tatsächlich erforderlich sein. Voraussetzung hierfür ist, dass kein milderes, gleich effektives Mittel zur Verfügung steht, um das Interesse zu wahren. Die Plattformbetreiberin verfolgte mit der Anzeige der bisher nicht mit ihr kooperierenden Ärzt:innen auf ihrer Plattform offenbar den Zweck, diesen die Plattform bekannt zu machen. Patient:innen sollten animiert werden, über das Portal eine Rezeptbestellung vorzunehmen, und so die Ärzt:innen zur Kooperation mit dem Unternehmen bewegen. Zur Bewerbung der Geschäftsidee gegenüber den Ärzt:innen hätte das Unternehmen jedoch weniger einschneidende Werbemaßnahmen ergreifen können, ohne personenbezogene Daten der Ärzt:innen ohne deren Zustimmung im Kontext der Plattform zu veröffentlichen und eine weitere Verarbeitung der Daten durch die Kontaktaufnahme der

[149] Siehe Art. 13 Abs. 1 lit. a DSGVO.
[150] Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

Patient:innen zu veranlassen. Zudem war davon auszugehen: Es entsprach nicht den vernünftigen Erwartungen der Ärzt:innen, dass ihre Kontaktdaten – wenn auch beruflicher Natur – zu Geschäftszwecken von der Plattformbetreiberin verwendet werden, ohne dass ein Geschäftsverhältnis besteht. Vor diesem Hintergrund überwogen auch die schutzwürdigen Interessen der Ärzt:innen, dass ihre Daten nicht entsprechend verarbeitet werden.

Für die Verarbeitungen der Gesundheitsdaten auf der Plattform, die Personen bei der Bestellung von ärztlichen Verordnungen der Betreiberin der Plattform zwangsläufig offenbarten, fehlte es ebenfalls an einer ausreichenden Rechtsgrundlage. Eine wirksame Einwilligung der Bestellenden wurde nicht eingeholt. Auch eine andere Rechtsgrundlage für die Verarbeitung der Gesundheitsdaten kommt nicht in Betracht. Insbesondere kann sich das plattformbetreibende Unternehmen nicht auf Art. 9 Abs. 2 lit. h sowie Abs. 3 DSGVO stützen, weil es sich bei der Plattformbetreiberin nicht um eine Angehörige eines Gesundheitsberufs handelt.

Darüber hinaus war die rechtlich vorgeschriebene Datenschutzinformation[151] der Website unpräzise und unvollständig. Wir haben gegen die Betreiberin der Plattform eine Verwarnung ausgesprochen.

Unternehmen, die über ihre Website personenbezogene Daten verarbeiten möchten, müssen vor Inbetriebnahme und auch bei jeder Änderung der Website prüfen, ob die beabsichtigten Verarbeitungen im Einklang mit der DSGVO stehen. Die Veröffentlichung personenbezogener Drittdaten zur Vermittlung von Diensten an Endnutzer:innen wird regelmäßig nicht den vernünftigen Erwartungen der Dritten entsprechen, wenn diese in keinerlei (Geschäfts-)Beziehung zu dem Verantwortlichen stehen.[152] Vor diesem Hintergrund stehen solchen Verarbeitungen regelmäßig schutzwürdige Interessen entgegen. Die Verantwortlichen sind zudem verpflichtet, sämtliche Datenverarbeitungen vollständig, transparent und präzise zu beschreiben und eine entsprechende Datenschutzinformation auf ihrer Website bereitzustellen. Kommen Unternehmen diesen Pflichten nicht nach, müssen sie mit einer aufsichtsrechtlichen Überprüfung und der Verhängung von Sanktionen einschließlich Bußgelder rechnen.

[151] Siehe Art. 13 und Art. 14 DSGVO.

[152] Siehe Europäischer Datenschutzausschuss (EDSA), Guidelines 1/2024 on processing of personal data based ohn Article 6 (1)(f) GDPR, Version 1.0, Rn. 54 und Example 6, abrufbar unter https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en.

X. Mobilität und -Daseinsvorsorge

1. Einsatz von Bodycams durch die Berliner Verkehrsbetriebe

Die Berliner Verkehrsbetriebe (BVG) haben im März dieses Jahres begonnen, den Einsatz von Bodycams durch ihr Sicherheitspersonal in einem Pilotprojekt zu erproben. Das Projekt ist auf zunächst zwölf Monate angelegt. Wir haben die BVG vor der Umsetzung beraten.

Die von den Sicherheitskräften getragenen Bodycams sind standardmäßig ausgeschaltet. Gerät eine Person mit Bodycam in eine Situation, bei der es wahrscheinlich ist, dass es zu einem körperlichen Übergriff auf sie kommt, kündigt sie an, dass sie die Bodycam aktivieren wird. Nach Angaben der BVG soll der betroffenen Person zugleich ein Informationsflyer mit datenschutzrechtlichen Informationen übergeben werden.[153]

Sofern sich die Situation nicht bereits beruhigt hat, wird sodann die Bodycam zunächst in Form des sog. Pre-Recording aktiviert. Dabei überschreibt sich die Aufzeichnung fortlaufend alle 120 Sekunden. Zugleich aktiviert sich der Bildschirm der Bodycam, sodass sich die von der Aufzeichnung betroffene Person selbst live sieht. Sollte die Situation weiter eskalieren, wird der eigentliche Aufnahmemodus gestartet. Kommt es zur Deeskalation der Situation, wird das Pre-Recording bzw. der Aufnahmemodus ausgeschaltet bzw. gar nicht erst gestartet. Aufnahmen, bei denen der Aufnahmemodus aktiviert wurde, werden automatisch nach 48 Stunden gelöscht, falls sie nicht zuvor auf Anforderung an Strafverfolgungsbehörden übermittelt wurden. Tonaufnahmen finden nicht statt. Die Beschäftigten, die eine Bodycam tragen sollen, werden zuvor intensiv datenschutzrechtlich geschult.

Die Rechtmäßigkeit der Videoaufnahmen richtet sich nach § 20 Abs. 1 und 4 Berliner Datenschutzgesetz (BlnDSG). Anders als bei den Bodycams der Polizei, Feuerwehr und Rettungsdienste, die im Einsatz ständig angeschaltet sind,[154] befinden sich die Bodycams der BVG-Mitarbeiter:innen zunächst in ausgeschaltetem Zustand. Entscheidend ist dann, ob in einer Situation eine Deeskalation erforderlich und die Aktivierung der Kamera dafür notwendig ist. Wir haben gegenüber der BVG u. a. deutlich gemacht, dass die Bodycams grundsätzlich nur als letztes Mittel eingesetzt werden dürfen, wenn körperliche Übergriffe tatsächlich wahrschein-

[153] Siehe Art. 13 Abs. 1 und 2 Datenschutz-Grundverordnung (DSGVO).
[154] Siehe JB 2023, A.V.3.

lich sind, nicht etwa bei Beleidigungen, Beweissicherungen bei Fahrten ohne Tickets oder Sachbeschädigungen wie Graffiti. Zudem haben wir Hinweise zur Erkennbarkeit der Personen mit Bodycams und zum Inhalt des Informationsflyers für die Betroffenen erteilt. Beispielsweise haben wir darauf hingewiesen, dass die getragenen Armbinden auch sichtbar Piktogramme und das Wort „Bodycam“ enthalten sollten und dass im Informationsblatt die Strafverfolgungsbehörden als mögliche Empfängerinnen der Videoaufnahmen zu nennen sind.[155] Die BVG hat zugesagt, unsere Hinweise umzusetzen.

Der Einsatz von Bodycams durch das Sicherheitspersonal der BVG kann zur Eigensicherung zulässig sein, solange keine dauerhaften, anlasslosen Aufzeichnungen stattfinden und die Aktivierung der Kamera im konkreten Fall zur Deeskalation erforderlich ist. Wir lassen uns fortlaufend von der BVG über den Verlauf des Pilotprojekts berichten. Nach dem Ende des Projekts werden wir uns dann über den Erfolg der Maßnahmen und die Erfahrungen mit dem Verfahren zur Übergabe des Informationsflyers informieren lassen. Die BVG hat zudem zugesagt, uns in die anschließende Entscheidung über einen Regelbetrieb einzubinden.

2. Einführung des Deutschlandsemestertickets

Berliner Studierende hatten in einer Übergangsphase die Möglichkeit, bei Zahlung eines Aufpreises ihr Semesterticket um ein Deutschlandticket zu erweitern. Zum Sommersemester dieses Jahres wurde das Verfahren umgestellt, sodass alle Studierenden ein Deutschlandsemesterticket erhalten. Das digitale Ticket wird von der BVG in Zusammenarbeit mit den Studierendenschaften der Hochschulen angeboten. Wir haben uns im Rahmen einer Anfrage einer Studierendenschaft mit den rechtlichen Rahmenbedingungen befasst.

Für die Bereitstellung des digitalen Deutschlandsemestertickets werden personenbezogene Daten der Studierenden von der jeweiligen Studierendenschaft an die BVG übermittelt. Anschließend wird das Deutschlandsemesterticket im Auftrag der BVG über eine eingesetzte Dienstleisterin als Auftragsverarbeiterin ausgestellt. Die Studierendenschaften, die nach dem Hochschulgesetz für die Ausgabe des Semestertickets zuständig sind, verarbeiten die Daten der Studierenden dabei in gemeinsamer Verantwortung mit der BVG und haben hierzu mit dieser in einer Vereinbarung festge-

[155] Siehe Art. 13 Abs. 1 lit. e DSGVO.

legt, wer welche Verpflichtung nach der DSGVO erfüllt.[156] So stellt die Studierendenschaft etwa den Studierenden die datenschutzrechtlichen Informationen zur Verfügung und dient ihnen als Hauptansprechpartnerin für Betroffenenrechte wie Auskunfts- oder Löschungsersuchen,[157] während die BVG bspw. die notwendigen Verträge mit Auftragsverarbeiter:innen schließt und diese überwacht.

Die Verarbeitung der personenbezogenen Daten der Studierenden durch die Studierendenschaften und die BVG als gemeinsam Verantwortliche ist datenschutzrechtlich zulässig. Sie dient dem Zweck, dass die BVG das Deutschlandsemesterticket für die Studierenden ausstellen kann. Die Nutzung eines Semestertickets zu ermöglichen, stellt eine gesetzliche Aufgabe der Studierendenschaften dar.[158] Um diese Aufgabe erfüllen zu können, bedarf es der Verarbeitung der personenbezogenen Daten der Studierenden, die grundsätzlich zum Erwerb des Tickets verpflichtet sind. Zugleich sind aber auch nur die Studierenden zur Erlangung des Tickets berechtigt. Da das Ticket unmittelbar durch die BVG ausgestellt wird und nicht durch die jeweilige Studierendenschaft,[159] besteht die Notwendigkeit, dass sich die BVG über die bestehende Berechtigung für den Erwerb eines Deutschlandsemestertickets vergewissern kann. Erst dann kann sie dieses ausstellen.

Für die Prüfung der Legitimation sollte das sog. Shibboleth-Verfahren verwendet werden. Beim Shibboleth-Verfahren erfolgt der Datenabgleich zur Berechtigung auf Seiten der Hochschule, der die personenbezogenen Daten der Studierenden ohnehin vorliegen. Die BVG erhält erst dann Zugriff auf die Daten zur Ausstellung des Semestertickets, wenn die Studierenden sich erfolgreich auf der Website der Hochschule angemeldet und somit ihre Berechtigung nachgewiesen haben. So wird gewährleistet, dass der Zugriff der BVG auf die Daten davon abhängt, dass die Studierenden dies selbst veranlasst haben.

Die Verarbeitung personenbezogener Daten der Studierenden durch die Studierendenschaft und die BVG als gemeinsam Verantwortliche zur Ausstellung des Deutschlandsemestertickets mit dem sog. Shibboleth-Verfahren ist zulässig.

[156] Siehe Art. 26 DSGVO.
[157] Siehe Art. 13–21 DSGVO.

[158] § 18a Berliner Hochschulgesetz (BerlHG).
[159] Nach § 6 Abs. 1 Satz 2 des Gemeinsamen Tarifs der im Verkehrsverbund Berlin–Brandenburg zusammenwirkenden Verkehrsunternehmen (Stand: 1. Januar 2025) werden Fahrausweise im Namen und für Rechnung der Verkehrsunternehmen ausgegeben.

3. Verlängerung der Speicherdauer von Videoaufnahmen der Berliner Verkehrsbetriebe

Die Ansprechperson der Landesregierung Berlin für die Akzeptanz sexueller und geschlechtlicher Vielfalt[160] hat uns wegen einer möglichen Verlängerung der gesetzlich festgelegten[161] maximalen Speicherdauer für Videoaufnahmen in U-Bahnen und Bussen der BVG kontaktiert. Um evidenzbasierte Erkenntnisse zur Frage der Erforderlichkeit einer Verlängerung der Speicherdauer zu gewinnen, haben wir hier zunächst die Polizei Berlin und die BVG gebeten, uns die vorliegenden Fallzahlen zur Verfügung zu stellen. Auch die Senatsverwaltung für Inneres und Sport (SenInnSport) hat uns konkrete Pläne zu einer Verlängerung der Speicherdauer von 48 auf 96 Stunden vorgestellt.

Die Bestrebungen zur Verlängerung der Speicherdauer wurden damit begründet, dass in der Vergangenheit Videoaufnahmen schon gelöscht gewesen seien, obwohl sie ggf. zur Strafverfolgung benötigt worden wären. Dies sei vor allem der Fall, wenn Geschädigte Anzeigen verzögert oder lückenhaft stellen oder sich ein Bezug zur BVG erst im Verlauf polizeilicher Ermittlungen ergeben hat.

Es ist für uns grundsätzlich nachvollziehbar, dass die Polizei Videoaufnahmen in solchen Fällen nicht mehr rechtzeitig anfordern kann. Entscheidend für die Rechtfertigung einer Verlängerung der Speicherfrist ist insbesondere deren objektive Erforderlichkeit. Eine Verdoppelung der Speicherfrist von zwei auf vier Tage wäre länger als in den meisten anderen deutschen Großstädten. Wir haben die BVG und die Polizei daher gebeten, uns mitzuteilen, in wie vielen Fällen die Polizei im letzten Jahr wegen zu großer zeitlicher Verzögerung kein Übermittlungsersuchen mehr an die BVG gestellt hat bzw. diese ein Übermittlungsersuchen nicht mehr bearbeiten konnte.

Die BVG und die Polizei haben übereinstimmend mitgeteilt, keine entsprechenden Statistiken zu führen. Vonseiten der Polizei wurden einige Fallbeispiele geschildert, in denen keine Videoaufnahmen mehr vorlagen. Festzustellen war, dass in diesen Fällen der Tatort mehrfach nicht im Bus- oder U-Bahn-Bereich lag, sondern vielmehr das Vor- oder Nachtatverhalten der Täterin bzw. des Täters für die Polizei relevant war. Bei der Bewertung ist jedoch zu berücksichtigen, dass die Strafverfolgung gerade nicht zu den gesetzlichen Aufgaben der BVG gehört. Die BVG darf personenbezo-

Die Fraktionen der CDU und der SPD haben mit der Abgeordnetenhaus-Drucksache 19/2553 einen Gesetzentwurf vorgelegt, der u. a. eine Verlängerung der Speicherdauer für personenbezogene Daten aus der Videoüberwachung der öffentlich zugänglichen Räume des Öffentlichen Personennahverkehrs (ÖPNV) auf 72 Stunden vorsieht.

Ohne den Entscheidungen des Gesetzgebers vorzugreifen, unterstützt der Senat die mit dem Gesetzentwurf intendierte Regelung.

Diese Erweiterung ist notwendig, weil die Praxis gezeigt hat, dass es möglich sein muss, länger als bisher auf ggf. vorhandene Beweismittel zurückzugreifen. Insofern kann auf die Begründung zu oben genannter Abgeordnetenhaus-Drucksache 19/2553 verwiesen werden, der dazu auf den Seiten 372 ff. folgende Ausführungen zu entnehmen sind:

„[…] Gerade wenn Geschädigte zunächst zögern, Anzeige zu erstatten, oder wenn sich erst im Verlauf polizeilicher Ermittlungen eine Spur ergibt, die zu einem ÖPNV-Bezug führt, hat die bislang geltende Speicherfrist von 48 Stunden häufig zur Folge, dass erfolgversprechendes Videomaterial bereits gelöscht ist. Weitere Gründe, die bislang zu einem Beweismittelverlust geführt haben, können beispielsweise auch sein:

- Sachverhalte werden in einer Internetanzeige nur lückenhaft geschildert und können durch Rückfragen nicht rechtzeitig ergänzt werden, da der Anzeigenerstatter oder die Anzeigenerstatterin nicht durchgehend erreichbar ist.
- Sachverhalte stellen sich erst zu einem späteren Zeitpunkt als Straftat dar, etwa wenn in einem Vermisstenfall zunächst keine Anzeichen auf eine Entführung hindeuten.

160 Ansprechperson Queeres Berlin.

161 § 20 Abs. 4 Satz 2 BlnDSG.

gene Daten mittels Videoüberwachung vielmehr lediglich zur Abschreckung in ihren Fahrzeugen und Bahnhöfen und zur Wahrnehmung ihres Hausrechts erheben.[162] Die Aufklärung außerhalb des öffentlichen Personennahverkehrs begangener Straftaten gehört nicht zu diesen Aufgaben. Die BVG darf zwar auch in diesen Fällen bereits angefertigte Videoaufnahmen übermitteln,[163] jedoch lässt sich die Erforderlichkeit der Verlängerung der Speicherfrist der Videoaufnahmen für die Aufgabenerfüllung der Polizei nicht damit begründen. Vielmehr müsste die Polizei in solchen Fällen nach Maßgabe der für sie geltenden Vorschriften Videoüberwachungsmaßnahmen selbst einsetzen.[164]

Mit den uns von BVG und Polizei vorgelegten Informationen lässt sich der Bedarf für eine gesetzliche Verlängerung der Speicherdauer für Videoaufnahmen in Bussen und U-Bahnen nicht ohne Weiteres begründen. Insbesondere fehlt es an empirischen Nachweisen. Die Erforderlichkeit einer Verlängerung der Speicherdauer ist für uns daraus nicht erkennbar.

- Zeitverluste können an Wochenenden und oder an Feiertagen eintreten, da Fachdienststellen und sachbearbeitende Dienststellen zu diesen Zeiten nur mit einem Bereitschaftsdienst besetzt sind.
- Nach der Erstsichtung ist bislang eine Nachsicherung von Videodaten meistens nicht mehr möglich, da das Zeitfenster von bislang 48 Stunden dann bereits abgelaufen ist.

Auch mit einer Verlängerung der Speicherdauer auf 72 Stunden ist die Berliner Regelung noch äußerst restriktiv. Die meisten anderen Bundesländer haben für Video-Aufzeichnungen aus dem ÖPNV überhaupt keine gesetzliche Höchstspeicherfrist festgelegt, sondern bestimmen nur allgemein, dass personenbezogene Daten unverzüglich zu löschen sind, wenn und soweit sie nicht mehr für die Zwecke erforderlich sind, zu denen sie erhoben wurden. Das ist zugleich der Maßstab der Datenschutz-Grundverordnung: Nach Artikel 5 Absatz 1 Buchstabe e DS-GVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie dies für die Zwecke, derentwegen sie erhoben wurden, erforderlich ist. Auf dieser Grundlage kann das jeweilige Unternehmen des ÖPNV nach seinen Erfahrungen selbst einschätzen, wann es üblicherweise keine Anfragen der Polizei mehr bekommt.

Feste Höchstspeicherfristen kennen außer Berlin nur
- Baden-Württemberg, wo die Frist vier Wochen beträgt,
- Bayern, wo die Frist zwei Monate beträgt,
- Rheinland-Pfalz, wo die Frist zwei Monate beträgt und
- Sachsen, wo die Frist zwei Monate beträgt."

Im Ergebnis wird Berlin demnach auch mit einer auf 72 Stunden verlängerten Höchstspeicherfrist

[162] § 20 Abs. 1 BlnDSG.
[163] § 20 Abs. 4 Satz 1 BlnDSG.
[164] Die Polizei kann nach § 24b Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) in öffentlich zugänglichen Räumen des Personennahverkehrs offene Videoaufnahmen anlassbezogen anfertigen.

die im Bundesvergleich mit Abstand strengste Regelung behalten.

4. Fortführung der Sicherheitsmaßnahmen der Berliner Bäder-Betriebe

Die Berliner Bäder-Betriebe hatten im vergangenen Jahr nach mehreren gewalttätigen Vorfällen u. a. Ausweiskontrollen und teilweise Videoüberwachung an den Eingängen der von ihnen betriebenen Sommerbäder eingeführt und diese Maßnahmen in diesem Jahr fortgesetzt. Zudem haben sie von Juni bis August den Ticketverkauf in fünf Bädern weitestgehend auf personalisierte Onlinetickets beschränkt. Wir halten die Ausweiskontrollen und Videoüberwachung für datenschutzrechtlich unzulässig und haben dies den Berliner Bäder-Betrieben mitgeteilt. Wir stehen mit den Berliner Bäder-Betrieben dazu weiterhin im Austausch und haben unsere Bereitschaft signalisiert, die Evaluation der Maßnahmen beratend zu begleiten.

Wir hatten bereits im vergangenen Jahr über die Einführung von Ausweiskontrollen und Videoüberwachung durch die Berliner Bäder-Betriebe sowie unsere diesbezügliche Bewertung berichtet.[165] Entgegen unserer Bewertung und unserer Hinweise[166] haben die Berliner Bäder-Betriebe ihre Maßnahmen in dieser Sommersaison fortgesetzt. Dass die Ausweiskontrollen und die Videoüberwachung für eine Verbesserung der Sicherheit zumindest mitursächlich sind, haben die Berliner Bäder-Betriebe auch in diesem Jahr nicht plausibel dargelegt. Die Ausweiskontrollen bewerten wir weiterhin als rechtswidrig, da diese zur Erfüllung der Aufgabe der Berliner Bäder-Betriebe, die Sicherheit ihrer Gäste und ihrer Beschäftigten zu gewährleisten, weder geeignet noch erforderlich sind. Auch hinsichtlich der Maßnahmen zur Videoüberwachung haben die Berliner Bäder-Betriebe nicht den notwendigen Nachweis erbracht, dass diese einen messbaren Mehrwert für die Identifizierung von Straftäter:innen mit sich bringt. Seit Einführung der Videoüberwachung haben die Berliner Bäder-Betriebe im Jahr 2023 lediglich in zwei Bä-

1. Chronologie

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 (Ausweispflicht) und den Einsatz von Kameraüberwachungsanlagen in Ein- und Ausgangsbereichen ausgewählter Bäder (Videoüberwachung) sowie seit 2024 die Option zum Erwerb von personalisierten Online Tickets zum Eintritt in Freibäder.

2. Ausweiskontrolle

Der Senat vertritt weiterhin die Auffassung, dass die Ausweispflicht für den Zutritt zu den Freibädern der BBB und eine Sichtkontrolle der Identitätsnachweise zur Aufgabenerfüllung der BBB erforderlich und somit zulässig ist.

Die Sichtkontrolle, ob beim Eintritt in ein Bad ein Identitätsnachweis mitgeführt wird, berührt Datenschutzinteressen der Badegäste nur geringfügig, da bei einer Sichtkontrolle nur das Vorhandensein eines Identitätsnachweises überprüft wird. Auch findet im Anschluss an die Sichtung keine weitere Verarbeitung, insbesondere Speicherung, statt.

Im Gegenzug stärkt das Mitführen eines Identitätsnachweises die Sicherheit von Mitarbeitenden bzw. Besuchenden der Bäder, da im Fall von Gewalt- oder anderen Sicherheitsvorfällen die Wahrscheinlichkeit der Identifizierung der Tatverdächtigen sehr hoch ist. Darüber hinaus hat dies bereits einen

[165] Siehe JB 2023, A.VII.3.
[166] Ebd.

dern jeweils ein einziges Mal und dieses Jahr nur insgesamt ein einziges Mal Videoaufnahmen an Strafverfolgungsbehörden übermittelt. Ob in diesen Fällen auch tatsächlich Tatverdächtige aufgrund der Videoaufnahmen ermittelt wurden, haben die Berliner Bäder-Betriebe nicht dargelegt. Auch liegen keine Auswertungen vor, ob die Ausweiskontrollen und die Videoüberwachung messbar zur Erhöhung der Sicherheit in den Sommerbädern geführt haben.

Die Berliner Bäder-Betriebe haben als weitere Maßnahme in diesem Jahr in fünf Sommerbädern in zentraler Lage den Verkauf von Bartickets eingeschränkt, sodass ein solcher nur noch bis 10 Uhr möglich war. Personen, die für die betroffenen Bäder nach 10 Uhr spontan Tickets kaufen wollten, waren de facto gezwungen, unter Angabe von u. a. Namen und E-Mail-Adresse personalisierte Onlinetickets zu kaufen. Mit dieser Maßnahme ist die Nutzung der Sommerbäder für Personen, die die Bäder erst nachmittags oder abends nutzen können, kaum noch möglich, ohne personenbezogene Daten im Rahmen des Onlineverkaufs anzugeben. Für die Inanspruchnahme der Leistungen des Schwimmbads ist es schlicht nicht erforderlich, dass die Kund:innen identifiziert werden bzw. Namen und E-Mail-Adressen angeben müssen. Vor diesem Hintergrund ist eine Evaluation dieser Maßnahme vor Beginn der nächsten Sommersaison notwendig.

präventiven abschreckenden Einfluss auf ggf. gewaltbereite Personen, die die Bäder aufsuchen.

Mit der Änderung der Tarifsatzung in 2025 für die Berliner Bäder wurden verschiedene neue Tarifmodelle und Kartenarten eingeführt, deren Gültigkeit einer Kontrolle bedarf, welche personenbezogene Daten miteinschließt. Dabei handelt es sich u. a. um die nach der Tarifsatzung und den Allgemeinen Geschäftsbedingungen der BBB zu personalisierenden Online-Tickets, die für den Eintritt in die Freibäder für ein ausgewähltes Zeitfenster erworben werden können, personalisierte Abonnement-Mitgliedschaften, die Badekarte im Ferienpass und Eintrittskarten für spezielle Aktionstarife. Auch hierfür ist das Mitführen von Identitäts- bzw. Berechtigungsnachweisen erforderlich. Eine Einschränkung der Kassenöffnungszeiten, wie sie für die Sommersaison 2024 galt, gibt es in der Saison 2025 nicht mehr.

3. Videoüberwachung

Die Videoüberwachung erfolgt in den Ein- und Ausgangsbereichen der Sommerbäder Neukölln, Pankow, Am Insulaner, Kreuzberg und im Kombibad Gropiusstadt.

Die Videoüberwachung hält der Senat weiterhin für zulässig, weil sie zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe der BBB 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.

Die Videoüberwachung hat in erster Linie einen präventiven Charakter, 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 Vor-

	handensein einer Videoüberwachung und das damit einhergehende Abschreckungspotential kann dazu führen, dass potentielle Tatpersonen vom Besuch bzw. Eintritt in einem Sommerbad abgehalten werden.
Die Berliner Bäder-Betriebe haben nach wie vor nicht nachgewiesen, dass die von ihnen eingeführten Ausweiskontrollen und Videoüberwachungsmaßnahmen zur Gewährleistung der Sicherheit in den Sommerbädern geeignet und erforderlich sind. Wir haben diese daher erneut als rechtswidrig bewertet. Auch die in dieser Sommersaison eingeführte zeitliche Beschränkung des Barticketverkaufs und die Einführung personalisierter Onlinetickets bedarf vor einer Fortsetzung der Evaluation. Wir haben bei den Berliner Bäder-Betrieben angeregt, uns an der Auswertung der Sicherheitsmaßnahmen und den Planungen für die nächste Sommersaison zu beteiligen, um gemeinsam datenschutzkonforme Lösungen zu entwickeln.	4. Fazit Die Pflicht zum Mitführen eines Identitätsnachweises (Ausweispflicht) und der ausgewählte Einsatz von Videoüberwachung sind Teile des ganzheitlichen Konzeptes aus Service, Prävention und Sicherheit, das durch weitere Maßnahmen (u. a. Verstärkung der Zaunanlagen, Deeskalationstraining, Steuerung von Besucherströmen durch Ampelsystem, betreute Sportangebote „SpOrt im Freibad“) ergänzt wird. Alle Maßnahmen können nur in ihrer Gesamtheit und in der Gesamtwirkung betrachtet werden. In der Vergangenheit kam es in den betroffenen Bädern mehrfach zu sicherheitsrelevanten Vorfällen. Nach Weiterführung des Maßnahmenbündels war in der Saison 2024 eine deutliche Beruhigung der Situation zu verzeichnen, welche sich in der statistischen Erfassung widerspiegelt: • Im Vergleich zur Sommerbadesaison 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. • In der Sommerbadesaison 2024 erteilten die BBB insgesamt 249 schriftliche Hausverbote im Vergleich zum Vorjahr mit 145 Hausverboten. Der Anstieg ist dabei auf die Ausweispflicht und die damit verbundene 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 sind wirksam und haben im Ergebnis und 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 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 Datenschutzbericht 2024 erneut gefordert - 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 weiterhin 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 der zuständigen Fachverwaltung (SenInnSport) und der BBB hiernach datenschutzrechtlich nicht zu beanstanden.

Im Jahr 2025 stehen die BBB weiterhin zu den beanstandeten Maßnahmen mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit im Austausch.

5. Es läuft: Funkwasserzähler datenschutzkonform einsetzen

Öffentliche Stellen unterliegen in Berlin strengen Voraussetzungen, was den Einsatz funkbasierter Messsysteme angeht. Dass eine datenschutzkonforme Verwendung dieser Geräte dennoch möglich ist, wenn verantwortliche Stellen sich entsprechend vorbereiten, zeigt der nunmehr anstehende Roll-out von per Funk ablesbaren Wasserzählern.

Im August veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Orientierungshilfe zur Datenverarbeitung im Zusammenhang mit funkbasierten Zählern.[167] Schon bei der Erarbeitung dieses Papiers fielen die mitunter erheblichen Unterschiede in den jeweiligen Landesgesetzen auf, die den Einsatz funkbasierter Verbrauchsmessgeräte, sog. Funkzähler, betreffen. In Berlin gilt mit § 22 BlnDSG eine Sonderregelung für die funkbasierte Erfassung von Verbrauchswerten ausschließlich für öffentliche Stellen. Danach ist die Verwendung von funkbasierten Verbrauchszählern nur mit Einwilligung der betroffenen Personen zulässig und dies auch nur, wenn die Ablesung für Betroffene erkennbar ist und abgeschaltet werden kann.

Da die Berliner Wasserbetriebe (BWB) die einzige öffentliche Stelle des Landes sind, die Verbrauchsmessungen durchführt, ist diese Regelung im BlnDSG allein im Bereich von funkbasierten Wasserzählern einschlägig. Wir standen mit den BWB in diesem Zusammenhang bereits seit 2019 im Austausch. Die BWB haben sich intensiv mit den Anforderungen der Spezialnorm auseinandergesetzt und ein Datenschutzkonzept entwickelt.

Die BWB planen einen flächendeckenden Austausch auf Zählergeräte, die sowohl funkbasiert als auch manuell ausgelesen werden können. Die Auslesung per verschlüsselter Funkverbindung erfolgt nur, wenn eine Einwilligung der betroffenen Personen erteilt wird. Ohne diese Zustimmung wird der Zähler weiterhin durch Mitarbeiter:innen der BWB vor Ort abgelesen. Die Einwilligung kann jederzeit widerrufen werden und die BWB können einen Widerruf auch direkt umsetzen. Eine Funkauslesung findet ab dem Zeitpunkt des Eingangs des Widerrufs nicht mehr statt. Personen, die einer funkbasierten Ablesung ihres Wasserverbrauchs zugestimmt haben, erhalten nach der Umstellung einen Hinweis über das digitale Kundenportal

[167] Abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/orientierungshilfen/2024-DSK-OH-Datenverarbeitung-funkbasierte-Zaehler.pdf.

oder per Briefpost, wann genau die Auslesung ihrer Verbrauchswerte erfolgt.

Wir haben den BWB mitgeteilt, dass für Personen, die einer Funkauslesung zugestimmt haben, auch außerhalb der turnusmäßigen Verbrauchsmessung zu Abrechnungszwecken jederzeit Einblick in den Datenbestand zu ihrem Wasserverbrauch gewährt werden muss. Auch Datensätze, die ausnahmsweise und nicht zu Abrechnungszwecken erhoben werden (z. B. Meldungen des Geräts zum eigenen Batteriestand oder ein Alarm wegen eines vermuteten Lecks) müssen den Betroffenen auf Anfrage zur Verfügung gestellt werden. Die BWB haben zugesagt, unsere Vorschläge umzusetzen.

Die sorgfältige Erarbeitung eines Datenschutzkonzepts gerade für komplexe Verarbeitungsvorgänge und neu auf den Markt drängende technische Lösungen wie funkbasierte Verbrauchsmessgeräte lohnt sich auch abseits der Daseinsvorsorge. Eine schrittweise Beobachtung der Datenverarbeitungsvorgänge vereinfacht das Finden datenschutzkonformer Lösungen und erspart aufwendige Anpassungen, die notwendig werden, wenn nach der Implementierung neuer Techniken datenschutzrechtliche Verstöße innerhalb miteinander verknüpfter Prozesse festgestellt werden.

XI. Arbeit und Beschäftigtendatenschutz

1. Personalakten sind nicht Teil des Bewerbungsverfahrens

Wenn im öffentlichen Dienst tätige Personen sich auf eine andere Stelle innerhalb des öffentlichen Dienstes bewerben, müssen sie häufig der Einsicht in ihre Personalakte zustimmen. Dadurch kann die ausschreibende Verwaltung Kenntnis von vielen für das Bewerbungsverfahren nicht erforderlichen Daten nehmen. Wir haben deshalb bei der für Landespersonal zuständigen Senatsverwaltung für Finanzen (SenFin) angeregt, dass auf die Übermittlung von Personalakten in Bewerbungsverfahren gänzlich verzichtet wird.

Seit langer Zeit gehört es zum Standard, von den sich bewerbenden Personen pauschal eine „Einwilligung zur Einsicht in die Personalakte“ zu fordern, wenn die Personen bereits im öffentlichen Dienst beschäftigt sind oder waren. Vielfach wurden darüber hinaus Ausdrucke der Fehlzeiten der letzten drei Jahre von den übermittelnden Behörden gefertigt und mit der Personalakte versandt. In diesem und letztem Jahr haben wir vermehrt Beschwerden und Anfragen zu dieser Verfahrensweise erhalten. Gleichzeitig hat die für Landesper-

sonal zuständige SenFin begonnen, aktualisierte Vorgaben zu Datenschutzfragen bei der Führung von Personalakten zu veröffentlichen.[168] In diesen wurden die Maßstäbe an eine solche Einwilligungserklärung und die Grenzen der Personalakteneinsicht in Bewerbungsverfahren ausdrücklich dargelegt. Das ist als Zwischenschritt sehr zu begrüßen.

Zu bedenken ist aber auch, dass eine Einwilligung eine freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung ist. Damit gibt die betroffene Person zu verstehen, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.[169] Freiwilligkeit setzt voraus, dass die betroffenen Personen eine echte Wahl haben, also eine Einwilligung verweigern oder zurückziehen können, ohne Nachteile zu erleiden.[170] In den Beschwerdeverfahren ließ sich nachweisen, dass die Personen von den Verfahren ausgeschlossen wurden, weil sie ihre Einwilligung in die Einsicht in ihre Personalakten nicht erteilt haben. Dies ist ein erheblicher Nachteil, der zeigt, dass die Einwilligungen nicht freiwillig abgegeben werden konnten.

Auch wenn dieser Ausschluss nicht stattgefunden hätte, wäre es schwer zu beurteilen, ob eine Entscheidung im Bewerbungsverhältnis freiwillig getroffen wird. Denn es besteht immer die Gefahr, dass Personen sich gezwungen fühlen, die Einwilligung zu erteilen, da sie befürchten, andernfalls schlechtere Chancen im Verfahren zu haben.

Personalakten im öffentlichen Dienst enthalten umfangreiche Datensammlungen über die Beschäftigten. Für die Beurteilung, ob eine Person für eine ausgeschriebene Stelle am besten geeignet ist, darf jedoch nur ein Teil dieser Informationen herangezogen werden. Dies sind etwa Beurteilungen und Zeugnisse, Nachweise über Weiterbildungen, aber auch Informationen über Disziplinarverfahren. Viele weitere Informationen, die sich aus der Personalakte ergeben, wie gesundheitliche Einschränkungen und Krankheitstage, Familienstand, Fotos aus den Bewerbungsunterlagen oder schlicht veraltete Informationen, dürfen für die Beurteilung nicht herangezogen werden. Diese Informationen sind nicht erforderlich, um Entscheidungen entsprechend dem Grundsatz der Bestenauslese zu treffen. Eine klare Trennung zwischen verschiedenen Personalaktenteilen findet bei den aktenführenden Stellen meist nicht statt, weshalb dann oft doch die gesamte

[168] Rundschreiben SenFin IV Nr. 23/2024. Weitere Rundschreiben sind geplant.
[169] Art. 4 Nr. 11 Datenschutz-Grundverordnung (DSGVO).
[170] Erwägungsgrund (ErwGr.) 42 Satz 5 DSGVO.

Personalakte übersandt wird, obwohl nur einzelne Teile angefordert werden.

Die ausschreibende Behörde kann alle für das Verfahren notwendigen Bewerbungsunterlagen unmittelbar von der sich bewerbenden Person verlangen. Wir streben daher an, dass Personalakteneinsichten in Bewerbungsverfahren im öffentlichen Dienst nicht mehr Teil des Bewerbungsprozesses sind, da die Einwilligung zur Einsicht in die Akte aufgrund der Abhängigkeitssituation der Bewerber:innen i. d. R. nicht freiwillig sein wird. Dies würde zu einem deutlich datenschutzfreundlicheren Bewerbungsverfahren führen, ohne dass wesentliche Nachteile für die einstellende Dienstbehörde zu befürchten sind.

2. Keine Videoaufzeichnungen von Befragungen durch Arbeitgeber:innen

In einem Fall, der uns zur rechtlichen Beurteilung vorlag, wurden mehrere Beschäftigte des Diebstahls einer erheblichen Geldsumme verdächtigt und zur Aufklärung vonseiten des Arbeitgebers nacheinander befragt. Diese Befragungen wurden ohne Wissen der Betroffenen aufgezeichnet. Die Aufzeichnung war für die Aufklärung nicht erforderlich.

In einem größeren Geschäft wurden die Bareinnahmen in einem Tresor gelagert, auf den die insgesamt sechs Schichtleitungen Zugriff hatten. Aus diesem Tresor waren die Einnahmen einer Woche verschwunden. Bei dem Versuch aufzuklären, wer das Bargeld entwendet hat, wurden alle Schichtleitungen von zwei Arbeitgebervertreter:innen verhört. Bei fünf dieser Gespräche war zusätzlich eine Person der Arbeitgeberseite über ein Videokonferenzsystem zugeschaltet. Die Gespräche wurden darüber aufgezeichnet.

Der Arbeitgeber hat erklärt: Die erste Person sei noch darauf hingewiesen worden, dass die Befragung aufgezeichnet werde; diese Person habe mündlich ihr Einverständnis erteilt. Bei den nachfolgenden Personen sei der Hinweis vergessen worden. Allerdings sei auf dem Bildschirm der zugeschalteten Person erkennbar gewesen, dass das Gespräch aufgezeichnet werde; dies hätte den befragten Beschäftigten auch auffallen müssen. Die Beschäftigten teilten mit, dies während des Gesprächs nicht bemerkt zu haben. Erst als die Aufnahme versehentlich einer der befragten Personen zugesandt wurde, hätten sie davon erfahren. Die Aufnahmen wurden mittlerweile gelöscht, der Verlust der Einnahmen konnte nicht aufgeklärt werden. Einer der befragten Personen wurde unmittelbar nach der Befragung gekündigt.

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten durch Arbeitgeber:innen nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffenen Personen im Beschäftigungsverhältnis eine Straftat begangen haben, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.[171] Die Aufnahme der Gespräche im vorliegenden Fall war eine über das gesetzliche Maß hinausgehende Datenverarbeitung, da sie zu Beweiszwecken nicht erforderlich war. Bei den Befragungen ging es darum zu klären, ob Anhaltspunkte für einen Diebstahl vorliegen und insofern ggf. auch Strafanzeige zu stellen ist. Es waren drei Zeug:innen anwesend, weshalb es keiner zusätzlichen Videoaufnahme bedurft hätte. Bei einem anschließenden Strafverfahren wäre es Angelegenheit der Strafverfolgungsbehörden gewesen, über weitere Ermittlungsmaßnahmen und Beweissicherungen zu entscheiden. Abgesehen davon ist auch die Angemessenheit einer solchen Maßnahme äußerst fragwürdig: Der in einer solchen Befragung bestehende immense Druck auf die Befragten wird durch Videoaufzeichnung unnötig erhöht, weshalb in solchen Konstellationen regelmäßig die insoweit schutzwürdigen Interessen der Beschäftigten überwiegen.

Weiterhin hatte der Arbeitgeber in mehreren Fällen nicht über die Videoaufzeichnung informiert, obwohl eine Informationspflicht[172] bestand und auch leicht zu erfüllen gewesen wäre. Eine wirksame Einwilligung ist mangels Freiwilligkeit ebenfalls regelmäßig nicht gegeben, da eine freiwillige Abgabe in solchen Konstellationen kaum denkbar ist.[173] Auch hätte diese Einwilligung dokumentiert werden müssen.[174] Eine solche Dokumentation konnte der Arbeitgeber nicht vorlegen.

Das Verfahren haben wir zur Prüfung der Einleitung eines Bußgeldverfahrens an unsere Sanktionsstelle abgegeben.

Eine Befragung von Beschäftigten kann ein zulässiges Mittel zur Aufdeckung von Straftaten sein. Vorab muss von Arbeitgeber:innen allerdings geprüft werden, ob die beabsichtigte Maßnahme das mildeste zur Verfügung stehende Mittel ist und ob sie im Verhältnis zu der begangenen Tat steht. Zudem sollten derartige Maßnahmen gut geplant sein, insbesondere muss vorher

[171] § 26 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG).
[172] Siehe Art. 13 DSGVO.
[173] Siehe § 26 Abs. 2 Satz 1 und 2 BDSG.
[174] Siehe Art. 7 Abs. 1 DSGVO.

eindeutig festgelegt werden, zu welchem Zweck die Daten verarbeitet werden sollen. Die Beschäftigten müssen bei der Befragung informiert und die Maßnahme entsprechend dokumentiert werden. Sobald sich der Verdacht einer Straftat verdichtet oder bestätigt, muss der Fall zur weiteren Verfolgung den dafür zuständigen Strafermittlungsbehörden übergeben werden.

XII. Wirtschaft und -Digitalwirtschaft

1. Onlinewerbung und Trackingrisiken

Für personalisierte Onlinewerbung wird das Verhalten von Internetnutzenden überwacht.[175] Mithilfe einer auf dem Mobilfunkanschluss basierenden Technik sollen Nutzende auch dann wiedererkennbar sein, wenn sie bspw. Cookies verweigern. Wir beteiligen uns an einem Forschungsprojekt, das die Risiken der weithin bekannten Cookiebanner untersucht und diese zu informativen und nicht manipulierenden Einwilligungsdialogen weiterentwickeln will.

Für möglichst wirksame Onlinewerbung werden im derzeit weitverbreitet eingesetzten Werbeökosystem so viele Daten wie möglich über jeden einzelnen Menschen gesammelt, um Interessen, soziodemografische Daten und – insbesondere über Smartphone-Apps – auch Aufenthaltsorte und Bewegungsmuster zu ermitteln. Einzelangaben werden dabei zum Teil mittels einer übergreifenden ID zu Profilen zusammengeführt. Diese IDs sind eindeutig der Nutzerin oder dem Nutzer zuordenbar. Vielfach werden sie (oder Daten, die sich auf sie abbilden lassen) in Cookies oder über ähnliche Mechanismen in den Geräten gespeichert, die die betroffenen Personen nutzen. Beim Zugriff auf eine Website oder bei der Nutzung einer App werden diese oder andere die betroffene Person eindeutig charakterisierende Daten den übertragenen Daten automatisch beigefügt. Die in Verbindung mit den IDs erhobenen Daten zur Person und ihren Interessen werden schließlich an die Clouddatenbanken vieler beteiligter Firmen des Werbeökosystems weitergeleitet. Hierdurch können sie zu aussagekräftigen und tiefe Einblicke in die Verhaltensmuster, Interessen und Lebensgewohnheiten der betroffenen Personen gewährenden Profilen verknüpft werden.

Ein zumindest in Deutschland neuer Ansatz für eine Person, eine derartige eindeutige ID zu generieren, ist die Verknüpfung mit dem Mobilfunkanschluss. Die jeweilige ID wird mittels kryptografischer Methoden aus der Telefon- oder Identifikationsnummer der SIM-

[175] Siehe auch JB 2020, 15.1.

Karte eines Endgeräts der Nutzenden generiert und vom Mobilfunkanbieter an den jeweilig genutzten Dienst (Website, Apps) weitergegeben. Die Nutzenden bemerken diese Übermittlung nicht, haben keine Eingriffsmöglichkeit und Selbstschutzmaßnahmen wie das Löschen von Cookies bleiben wirkungslos. Selbst wenn die Speicherung von Cookies in einem Browser unterbunden und andere entsprechende Speichermechanismen im Endgerät deaktiviert werden, kann der Mobilfunkbetreiber immer wieder die gleiche ID zu einer Person liefern und damit den App- und Websitebetreibenden und mittelbar den Werbetreibenden erlauben, die Profile in hoher Datenqualität fortzuschreiben.

Als Rechtsgrundlage für diese Datenverarbeitung kommt nur eine Einwilligung der Betroffenen in Betracht. Diese müsste aber wirksam sein und den datenschutzrechtlichen Vorgaben[176] entsprechen. Aus der Praxis sind uns hier Einwilligungsmechanismen bekannt, die neben den bereits auf vielen Websites vorhandenen Einwilligungsdialogen einen zusätzlichen Einwilligungsdialog für das Tracking mittels Mobilfunk-ID vorsehen. Den Nutzenden soll insbesondere über den zweiten Dialog ermöglicht werden, die Einwilligungen für einzelne Websites auch nachträglich individuell verwalten zu können. Die ausgegebenen IDs sind für verschiedene Publisher unterschiedlich und für einen begrenzten, aber vergleichsweise langen Zeitraum von 90 Tagen gültig. Eine Verknüpfung von Daten zur selben Person über diesen Zeitraum hinaus und über verschiedene Angebote hinweg ist Websitebetreibenden jedoch vergleichsweise einfach möglich. Auch hier zeigt sich wieder, dass eine Einwilligung als Grundlage für komplexe und eine Vielzahl von Akteur:innen beteiligende Datenverarbeitungsketten an ihre Wirksamkeitsgrenzen stößt. Da das Tracking mittels Mobilfunk-ID nach unserer Wahrnehmung stark zunimmt, werden wir dies im nächsten Jahr bei einzelnen Websitebetreibenden einer Prüfung unterziehen.

Seit Jahren beschäftigen wir uns im Rahmen unserer Tätigkeit als Aufsichtsbehörde mit dem Werbeökosystem. Eins der Grundprobleme – die derzeitige Internetwerbung beruht auf der Überwachung durch eine unüberschaubare Anzahl von Drittparteien – ist nicht gelöst. Regelmäßig steht diese Überwachung in Konflikt mit den datenschutzrechtlichen Regelungen, da eingeholte Einwilligungen aufgrund mangelnder Informa-

[176] Insbesondere die Anforderungen an eine wirksame Einwilligung zur Setzung der Cookies (§ 25 Abs. 1 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG) und zur Verarbeitung der personenbezogenen Daten im Rahmen des Trackings (Art. 6 Abs. 1 Satz 1 lit. a Datenschutz-Grundverordnung – DSGVO) nach Art. 4 Nr. 11 und Art. 7 DSGVO sowie an die Transparenzpflichten nach Art. 13 Abs. 1 und 2 DSGVO.

tion der Betroffenen nicht wirksam sind und die Datenschutzgrundsätze von Transparenz und Fairness nicht umgesetzt werden.

Im Rahmen eines Forschungsprojekts[177], an dem wir uns zusammen mit Partner:innen aus Universitäten und Industrie beteiligen, ermitteln wir die objektiv bestehenden Risiken, die den Personen, die digitale Dienste nutzen, durch die Techniken personalisierter Internetwerbung entstehen. Dabei nehmen wir verschiedene Personalisierungsverfahren in den Blick – angefangen von der überwachungsgesteuerten Werbung, die darauf basiert, das Verhalten von Individuen im Internet zu erfassen, zu dokumentieren und daraus Schlüsse für zukünftiges Verhalten zu ziehen, bis hin zu weniger invasiven Alternativen wie kontextbasierter Werbung. Ebenfalls interessant sind neuere Ansätze, die Interessensprofile nicht mehr innerhalb einer unüberschaubaren Wolke von Unternehmensdatenbanken erzeugen, speichern und nutzen, sondern potenziell datenschutzfreundlicher auf dem Endgerät unter der Kontrolle der Nutzerin bzw. des Nutzers. In einem zweiten Schritt werden wir zusammen mit den Projektpartner:innen verschiedene Varianten der Vermittlung dieser Risiken durch narrative und grafische Darstellung auf ihre Wirksamkeit untersuchen. Nur eine wirksame Vermittlung der Risiken kann zu informierter Teilhabe und Rechtskonformität der Verfahren führen.

Auch wenn das auf Daten des Mobilfunkanschlusses basierende Tracking auf einer Einwilligungslösung beruht, die Nutzenden prinzipiell die vorgeschriebenen Möglichkeiten gibt, Einwilligungen individuell pro Website zu erteilen oder zu verweigern, und diese Entscheidung auch nachträglich jederzeit revidiert werden kann, ist diese Technik riskant. Sie hat das Potenzial, die Überwachung der Nutzenden stringenter und umfassender zu gestalten und diese damit einem tieferen Eingriff in die Privatsphäre auszusetzen. Die entstehenden Profile enthalten mehr und genauere Informationen, die auch nicht nur für Werbezwecke verwendet werden können. Es gab bereits Presseberichte[178], denen zufolge Daten aus dem Werbeökosystem bspw. zur Identifikation von Militärangehörigen oder Besucherinnen von Abtreibungskliniken genutzt wurden.

2. Prüfung eines Onlinewerbeunternehmen

Wir haben dieses Jahr ein Unternehmen vor Ort geprüft, das im Bereich der Onlinewerbung als Daten-

[177]https://sid-projekt.de.

[178]Siehe https://netzpolitik.org/2024/databroker-files-firma-verschleudert-36-milliarden-standorte-von-menschen-in-deutschland/.

händler tätig ist. Für die meist sehr invasiven Verarbeitungen personenbezogener Daten, die das Unternehmen dabei durchführt, ist eine Einwilligung der betroffenen Personen erforderlich. Teilweise war bereits aus den Unterlagen des Unternehmens ersichtlich, dass keine oder keine wirksame Einwilligung erteilt worden war, teilweise konnte das Unternehmen wegen struktureller Defizite die Einwilligungen nicht nachweisen.

Das Unternehmen bietet verschiedene Dienste an. Ein Teil dieser Dienste beruht darauf, auszuwerten, welche Nutzer:innen vermeintlich bestimmte, von Werbetreibenden gewünschte Eigenschaften aufweisen. Die Werbetreibenden bzw. deren Dienstleister erhalten dann eine Rückmeldung, welche Werbe-ID-Nummern diese Eigenschaften vermeintlich aufweisen. Die Werbetreibenden bzw. deren Dienstleister können betreffenden Nutzer:innen dann gezielt auf diese Zielgruppe zugeschnittene Werbung anzeigen. Ein anderer Teil der Dienste beruht darauf, die Aufenthaltsorte von Nutzer:innen auszuwerten.

Das geprüfte Unternehmen erhebt die Daten der Nutzer:innen dabei nicht selbst, sondern kauft diese von anderen Unternehmen zu. Einige Datenlieferanten betreiben eigene Apps, einige liefern Daten, die sie wiederum von anderen Unternehmen erhalten haben. Die ursprünglichen Datenquellen wie App-Betreiber sollen für das geprüfte Unternehmen Einwilligungen in die Datenverarbeitungen einholen. Deren Prozess der Einholung der Einwilligung hat das Unternehmen zwar geprüft und wegen besonders schwerwiegender Verstöße auch einigen Datenlieferanten gekündigt. Allerdings arbeitete das Unternehmen weiterhin mit diversen Datenlieferanten zusammen, bei denen es selbst festgestellt hatte, dass datenschutzrechtliche Mängel bestanden.

Die verwendeten Einwilligungstexte basierten letztlich auf dem Transparency & Consent Framework (TCF), das vom Interactive Advertising Bureau Europe (IAB Europe) entwickelt wurde. Im Rahmen des TCF wird regelmäßig eine Einwilligung für die Verarbeitung von mehreren Hundert Akteur:innen, die in dem Werbenetzwerk von IAB Europe tätig werden, zusammen eingeholt. IAB Europe ist ein Verband ohne Gewinnerzielungsabsicht mit Sitz in Belgien, der Unternehmen der digitalen Werbe- und Marketing-industrie auf europäischer Ebene vertritt. Das Ziel des TCF besteht insbesondere darin, die Einhaltung der DSGVO zu erleichtern, wenn diese Wirtschaftsteilnehmer:innen das OpenRTB nutzen, d. h. eines der am meisten verwende-

ten Protokolle für Real Time Bidding. Real Time Bidding (RTB) ist ein System der sofortigen und automatisierten Onlineversteigerung für den Verkauf und den Kauf von Werbeplätzen im Internet. Die Gebote beruhen meist darauf, ob und für welche Werbetreibenden die den jeweiligen Nutzer:innen zugeschriebenen Eigenschaften von Interesse sind.

Neben der schieren Masse an Informationen waren die Einwilligungstexte häufig inhaltsleer bzw. unverständlich. Auch die Zwecke und verarbeiteten Daten waren nicht ausreichend klar dargestellt. Teilweise gingen die tatsächlichen Verarbeitungen zudem über den Inhalt der Einwilligung hinaus. Bei manchen Datenlieferanten wurde als vermeintliche Einwilligung gar keine Willenserklärung der Betroffenen eingeholt, bei anderen war sie versteckt und unzulässig mit wichtigen Funktionen gekoppelt. Teilweise gab es keine (benannte) oder nur eine kaum zu findende Möglichkeit zur Ablehnung der Einwilligung. Zum Teil waren Datenschutzerklärungen und Einwilligungstexte fremdsprachlich. Das Unternehmen konnte auch darüber hinaus nicht die tatsächliche Erteilung der Einwilligung nachweisen, da es nur eine abstrakte Prüfung des Einwilligungsvorgangs vorgenommen hatte. Es hatte in diesem Rahmen auch nicht getestet, ob bei verweigerter Einwilligung tatsächlich keine Datenübermittlung an das Unternehmen erfolgt. In der Praxis müssen wir häufig feststellen, dass die Verweigerung der Einwilligung von Verantwortlichen ignoriert wird und trotzdem ein umfangreiches Tracking erfolgt.

Für das Tracking des Nutzungsverhaltens auf Websites, einschließlich der Zuschreibung von Eigenschaften und Interessen, und das auf Tracking basierende Ausspielen personalisierter Werbung ist eine Einwilligung der betroffenen Person erforderlich.[179] Basiert das Tracking – wie regelmäßig – auf dem Einsatz von Cookies und vergleichbaren Technologien, dann ist auch hierfür – regelmäßig – eine Einwilligung erforderlich. Verantwortliche tragen die volle Beweislast dafür, dass sie bei der Verarbeitung personenbezogener Daten sämtliche Datenverarbeitungsgrundsätze einhalten.[180] Dazu gehört auch der Nachweis einer wirksamen Einwilligung[181] und einer den gesetzlichen Anforderungen genügenden Information der betroffenen Personen.[182]

[179]Siehe Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Orientierungshilfe für Anbieter:innen von digitalen Diensten (OH Digitale Dienste), Version 1.2, Rn. 96 ff., 107 ff., abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf.
[180]Art. 5 DSGVO; bestätigt durch ständige Rechtsprechung, z. B. Europäischer Gerichtshof (EuGH), Urteil vom 11. Juli 2024, C-757/22, Rn. 52.
[181]Art. 5 Abs. 1 lit. a Fall 1 DSGVO (Grundsatz der Rechtmäßigkeit).
[182]Art. 5 Abs. 1 lit. a Fall 3 DSGVO (Grundsatz der Transparenz).

Da das Unternehmen Daten von vielen anderen Akteur:innen zusammenführte, konnten wir einen interessanten Einblick in die Qualität der Trackingdaten erhalten. Wir haben eine Stichprobe der Datensätze untersucht. Dabei mussten wir feststellen, dass die Zuschreibungen von Eigenschaften in erheblichem Umfang widersprüchlich waren. So wurden ein und derselben Person praktisch jede Alters- und jede Einkommensklasse zugeschrieben. Datenschutzrechtliche Verstöße mussten wir bei unserer Prüfung auch in weiteren Bereichen feststellen. Wir haben vor, die festgestellten Verstöße u. a. aufgrund der hohen Zahl betroffener Personen an unsere Sanktionsstelle zur Prüfung abzugeben, ob ein Bußgeldverfahren eingeleitet werden soll.

Der Fall zeigt exemplarisch, welche Schwierigkeiten im Bereich des Trackings insbesondere im Hinblick auf die Wirksamkeit datenschutzrechtlicher Einwilligung bestehen. Auch Unternehmen in der Onlinewerbebranche, die nicht unmittelbar in Kontakt mit den betroffenen Personen stehen, müssen als Verantwortliche dafür Sorge tragen, dass sie wirksame Einwilligungen für ihre Datenverarbeitungen nachweisen können und die von ihnen zusammengeführten Datensätze eine hohe Qualität aufweisen. Allerdings nutzt auch der Nachweis einer Einwilligung nichts, wenn die Einwilligungserklärungen unwirksam sind; so regelmäßig, wenn Hunderte Akteur:innen als Datenempfänger:innen aufgeführt werden, die Datenflüsse derart komplex sind, dass diese nicht transparent gemacht werden können und die Zwecke nicht ausreichend und transparent bezeichnet sind. Zudem zeigt sich, dass Datenverarbeitungen erfolgen, die gar nicht vom Wortlaut der Einwilligung gedeckt sind, bzw. dass die von den betroffenen Personen in einem Cookiebanner getroffene Entscheidung über die Datenweitergabe im weiteren Verlauf der Datenverarbeitungskette gar nicht geprüft wird. Angesichts der Schwächen der Einwilligungslösung im Bereich des Onlinewerbetrackings[183] wäre eine über das Werbeanzeigeverbot des Data Services Act hinausgehende klarere gesetzliche Regulierung des Onlinetrackings und -profilings wünschenswert.

3. Vor-Ort-Prüfung zur Übernahme eines Wohnungsbestands

Bei der Wohnraumvermietung fallen umfangreiche Datensätze an – von den Bewerbungsunterlagen über Verbrauchswerte und Schriftwechsel während des Mietverhältnisses bis zur Kautionsrückzahlung. Bei all diesen Datenverarbeitungen sind die Prinzipien der Rechtmäßigkeit und Speicherbegrenzung einzuhalten. Die Daten dürfen also nur verarbeitet werden, wenn

[183] Art. 26 Abs. 3 und Art. 28 Abs. 2 Data Services Act, Verordnung über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, VO 2022/2065.

und solange dies zur Erfüllung des Mietvertrags erforderlich ist. Die Verarbeitungen müssen regelmäßig darauf überprüft und ggf. Daten gelöscht werden.

Bei der Prüfung eines Vermietungsunternehmens fanden wir eine Vielzahl von Informationen über aktuelle und ehemalige Mieter:innen vor, deren Verarbeitung zur Begründung oder Durchführung eines Mietverhältnisses nicht oder nicht mehr erforderlich war.

Das betroffene Unternehmen hatte uns 2022 mitgeteilt, den Datenbestand der von ihm übernommenen bzw. neu geschlossenen Mietverhältnisse zu überprüfen und zu bereinigen. Dies nahmen wir zum Anlass, den Erfolg der Maßnahmen in diesem Frühjahr in Augenschein zu nehmen. Das Unternehmen zeigte sich kooperativ und beschrieb die umfangreichen Maßnahmen, die zur Bereinigung des Datenbestands bereits ergriffen worden waren. So seien Mietverhältnisse in verschiedene Kriterien sortiert worden, um nicht oder nicht mehr erforderliche Daten einfacher identifizieren zu können. Im Anschluss seien eine hohe fünfstellige Zahl von Verträgen händisch überprüft und eine Vielzahl von Daten zur Löschung markiert worden.

Im Rahmen unseres Prüfverfahrens führten wir Stichproben durch. Teilweise hatten die von dem Unternehmen betriebenen Anstrengungen zur Bereinigung des Daten-bestands zum Erfolg geführt. In mehreren Stichproben fanden wir dennoch umfangreiche Datensätze, die nicht für die Begründung oder Durchführung eines Mietverhältnisses erforderlich sind und daher auch nicht hätten gespeichert werden dürfen (z. B. Angaben zur Staatsangehörigkeit oder Kopien von Personalausweisen). Auch Daten, die zu vor geraumer Zeit abgewickelten Mietverhältnissen gehörten, oder Daten über die religiöse Überzeugung der Mieter:innen in der Form, dass diese keine Kirchensteuer bezahlen, traten in den Stichproben zutage. Aufgrund der hohen Zahl an Betroffenen haben wir das Verfahren an unsere Sanktionsstelle zur Prüfung abgegeben, ob ein Bußgeldverfahren eingeleitet werden soll.

Unternehmen sollten bei der Übernahme von Kundendatenbeständen schon vor der Übernahme Vorkehrungen treffen, dass sie vom veräußernden Unternehmen nur diejenigen Daten erheben und speichern, die für die Fortführung des Geschäfts unbedingt notwendig sind. Unsere Vor-Ort-Prüfungen zeigen, dass die nachträgliche Bereinigung von übernommenen Mietakten i. d. R. nicht zufriedenstellend funktioniert.

4. Code-Ident-Verfahren zum Nachweis von Einwilligungen in Werbeanrufe

In den letzten Jahren haben wir zahlreiche Beschwerden zu Werbeanrufen durch Energieversorgungsunternehmen erhalten. Das Ziel der Anrufe war es, noch am Telefon Strom- und Gaslieferungsverträge abzuschließen. Ein Kontakt zwischen den Unternehmen und den angerufenen Personen bestand vorher nicht.

Werbeanrufe zur Gewinnung von Neukund:innen sind nur mit ausdrücklicher Einwilligung der betroffenen Personen zulässig.[184] In unseren Beschwerdefällen tragen diese regelmäßig vor, sie hätten weder in die Verarbeitung von auf sie bezogenen Daten zum Zweck von Werbeanrufen eingewilligt, noch wüssten sie, woher die Unternehmen ihre Daten kennen. Die Unternehmen erklärten, die betroffenen Personen hätten im Rahmen von durch Dritte durchgeführten Onlinegewinnspielen die notwendigen Einwilligungen erteilt. Sie hätten ihre Kontaktdaten in die Eingabemaske des jeweiligen Gewinnspiels eingetragen, sich sodann über das sog. Code-Ident-Verfahren verifiziert und in Werbeanrufe durch die Unternehmen eingewilligt.

Beim Code-Ident-Verfahren bestätigt die einwilligende Person mit einem ihr per SMS zugesendeten Verifikationscode, dass die angegebene Telefonnummer ihr zugeordnet ist. Zum Nachweis der Einwilligung – der für jede Datenverarbeitung, die sich auf eine Einwilligung stützt, rechtlich vorgeschrieben ist[185] – haben uns die verantwortlichen Unternehmen Screenshots der Eingabemasken der Onlinegewinnspiele vorgelegt. Die Screenshots enthielten diejenigen Daten, die die betroffenen Personen vorgeblich eingetragen hatten. Gleichzeitig legten sie uns Sendereporte zum SMS-Versand vor.

Diese Unterlagen genügten nicht, um nachzuweisen, dass die betroffenen Personen tatsächlich eingewilligt und ihre Telefonnummern bestätigt haben. Denn es ist ohne Weiteres möglich, entsprechende Unterlagen zu fälschen: Die Eingabemasken können von jeder beliebigen Person ausgefüllt und auch die Sendereporte können händisch niedergeschrieben worden sein. Aufgrund der sehr detaillierten und nachvollziehbaren Darstellung des Sachverhalts einzelner betroffener Personen konnte der durch die Unterlagen gesetzte Anschein widerlegt werden, dass diese tatsächlich Einwilligungen erteilt haben. So hatten mehrere betroffene Personen einen anderen Internetanbieter als denjenigen, dem

[184] Art. 6 Abs. 1 Satz 1 lit. a und f DSGVO i. V. m. § 7 Abs. 1 und 2 Nr. 1 Gesetz gegen den unlauteren Wettbewerb (UWG).
[185] Art. 7 Abs. 1 DSGVO.

die in den uns vorgelegten Unterlagen jeweils enthaltene IP-Adresse zugeordnet ist. Ebenso konnten betroffene Personen uns glaubhaft vortragen, dass sie zum Zeitpunkt der angeblichen Abgabe ihrer Einwilligungen mit anderen Aktivitäten befasst gewesen waren. In einem Fall schilderte uns eine betroffene Person, dass das angeführte Mobiltelefon gar nicht in der Lage sei, SMS zu empfangen. In einem weiteren Fall soll die betroffene Person bereits seit dreizehn Jahren nicht mehr unter der auf dem Screenshot angegebenen Adresse gewohnt haben. Dementsprechend müssen wir davon ausgehen, dass die Verarbeitung der Daten der betroffenen Personen durch die Unternehmen zum Zweck von Werbeanrufen rechtswidrig war.

Verantwortliche benötigen eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Stützen sie sich auf Einwilligungen, müssen sie deren Vorliegen nachweisen können. Dies gilt auch für Einwilligungen in Werbeanrufe. Das Code-Ident-Verfahren ist oftmals kein geeignetes Mittel hierfür. Wer Einwilligungen durch Dritte einholen lässt, muss sicherstellen, dass die Unterlagen, die die Einwilligungen belegen sollen, fälschungssicher sind.

XIII. Parteien und Gesellschaft

1. Datenschutz im Abgeordnetenhaus

Anfang des Jahres hat der Europäische Gerichtshof (EuGH) in einem weiteren Urteil zur Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) im parlamentarischen Raum verdeutlicht, dass auch die unmittelbare und ausschließliche parlamentarische Tätigkeit eines Untersuchungsausschusses in den Anwendungsbereich der DSGVO fallen kann.[186] Der EuGH äußert sich auch zur Frage der Zuständigkeit bei Beschwerden nach Art. 77 Abs. 1 DSGVO. Für den Fall, dass der jeweilige Mitgliedstaat „nur" eine einzige Datenschutzaufsichtsbehörde eingerichtet hat, lässt sich aus den Feststellungen des EuGH der Schluss ziehen: Dieser Aufsichtsbehörde ist auch die Zuständigkeit übertragen, über Beschwerden zur Verarbeitung personenbezogener Daten im parlamentarischen Raum zu entscheiden.

Im Jahr 2020 hat der EuGH in einer Grundsatzentscheidung festgestellt, dass der Petitionsausschuss des Hessischen Landtags als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO einzustufen ist. Also unterliegt die von einem solchen Ausschuss vorgenommene Verarbei-

[186] EuGH, Urteil vom 16. Januar 2024, C-33/22, Rn. 40.

tung personenbezogener Daten dem Anwendungsbereich der DSGVO.[187] Mit einem neuen Urteil aus dem Januar dieses Jahres hat das Gericht seine Rechtsprechung bestätigt und festgestellt, dass auch die unmittelbare und ausschließliche parlamentarische Tätigkeit eines Untersuchungsausschusses in den Anwendungsbereich der DSGVO fallen kann.[188] Die Entscheidung des EuGH bezieht sich dabei auf die Tätigkeit eines Untersuchungsausschusses, der vom österreichischen Nationalrat nach dem österreichischen Bundes-Verfassungsgesetz eingesetzt wurde. Das Gericht äußert sich dabei auch zu der Frage der Aufsichtszuständigkeit für Datenschutzbeschwerden betroffener Personen. Der EuGH kommt zu dem Ergebnis: Für den Fall, dass der Mitgliedstaat nur eine einzige Datenschutzaufsichtsbehörde eingerichtet, sie aber nicht mit der Zuständigkeit für die Kontrolle der Datenverarbeitung eines Untersuchungsausschusses ausgestattet hat, überträgt die DSGVO[189] dieser Behörde unmittelbar die Zuständigkeit, über Beschwerden betroffener Personen zu entscheiden.[190]

Die Ausführungen des EuGH in seinem aktuellen Urteil dürften auch auf andere Bereiche der parlamentarischen Tätigkeiten übertragbar sein. Umgewandelt auf die rechtliche Situation im Land Berlin bedeutet dies: Der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI), die nach § 8 Berliner Datenschutzgesetz (BlnDSG) als einzige Datenschutzaufsichtsbehörde für das Land Berlin eingerichtet ist, wird die Aufsichtszuständigkeit in diesem Bereich übertragen. Damit fallen unserer Behörde jedoch Kontrollbefugnisse im Kernbereich parlamentarischer Tätigkeiten zu, die mit den Vorgaben der Berliner Verfassung[191] und den verfassungsrechtlichen Strukturen in Deutschland nicht vereinbar sind.

Auch in dem Verfahren vor dem EuGH hatten die österreichische Datenschutzbehörde, der Präsident des Nationalrates und die österreichische Regierung darauf hingewiesen, dass im Verfassungsrang stehende Bestimmungen des österreichischen Rechts jegliche Kontrolle der Legislative durch die Exekutive verböten. Daher könne die Aufsichtsbehörde, die der Exekutive zuzurechnen sei, nicht die Anwendung der DSGVO in einem Untersuchungsausschuss überwachen, der ein

[187] EuGH, Urteil vom 9. Juli 2020, C-272/19, Rn. 74.
[188] EuGH, Urteil vom 16. Januar 2024, C-33/22, Rn. 40.
[189] Art. 77 Abs. 1 und Art. 55 Abs. 1 DSGVO.
[190] EuGH, Urteil vom 16. Januar 2024, C-33/22, Rn. 72.
[191] Art. 3 Abs. 1 Verfassung von Berlin (Gewaltenteilung), Art. 38 Abs. 4 Satz 2 Verfassung von Berlin (Auftrags- und Weisungsunabhängigkeit des Abgeordneten).

Organ der Legislative sei.[192] Das Gericht führt dazu jedoch aus, dass Art. 51 Abs. 1 DSGVO es den Mitgliedstaaten gerade mit Blick auf die Achtung ihrer verfassungsrechtlichen Strukturen freigestellt habe, mehrere Aufsichtsbehörden einzurichten.[193] Nachdem wir die Notwendigkeit der Einrichtung einer unabhängigen Kontrollstelle für die Datenschutzaufsicht nach der DSGVO bereits in unseren Jahresberichten 2020[194] und 2021[195] thematisiert hatten, haben wir das aktuelle Urteil des EuGH zum Anlass genommen, die Präsidentin und die Mitglieder des Abgeordnetenhauses von Berlin zu bitten, sich nunmehr für die Einrichtung einer unabhängigen Kontrollstelle einzusetzen.[196]

Die Wahrnehmung von Aufgaben der Datenschutzaufsicht durch uns im Kernbereich parlamentarischer Tätigkeiten ist mit der verfassungsrechtlichen Struktur des Landes nicht vereinbar. Vor dem Hintergrund der Rechtsprechung des EuGH halten wir es daher für dringend notwendig, dass für die Datenschutzaufsicht im Abgeordnetenhaus eine unabhängige Kontrollinstanz geschaffen wird.

2. Offener Brief an die im Bundestag vertretenen Parteien zum Political Targeting

Für politische Werbung, z. B. im Vorfeld von Wahlen, nutzen Parteien die Dienste der großen Onlineplattformen und sozialen Netzwerke, um ihre politischen Botschaften möglichst gezielt an Personen bzw. Personengruppen, basierend auf deren demografischen Daten, politischen Interessen oder Verhaltensweisen, auszuspielen. Die zu diesem Zwecke genutzten Targeting- und Anzeigeschaltverfahren bergen Datenschutzrisiken, auf die wir die im Bundestag vertretenen Parteien anlässlich der Wahlen zum Europäischen Parlament in diesem Jahr und der Bundestagswahl 2025 in einem offenen Brief hingewiesen haben.

In den Internetwerbenetzwerken und durch die großen Onlineplattformen werden u. a. mittels Trackingtechnologien personenbezogene Daten erhoben, ausgewertet und bestimmten Interessenkategorien zugeordnet. Dadurch entstehen umfangreiche Interessens- und Verhaltensprofile, die es den Werbenden ermöglichen, auf Websites, Onlineplattformen oder über Social-Media-

[192] EuGH, Urteil vom 16. Januar 2024, C-33/22, Rn. 67.
[193] Ebd., Rn. 68. Der EuGH verweist ferner auf Erwägungsgrund (ErwGr.) 117 DSGVO, der festhält, dass Mitgliedstaaten mehr als eine Aufsichtsbehörde errichten können sollen, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht.
[194] JB 2020, 17.1.
[195] JB 2021, 18.2.
[196] Siehe dazu Rede der BlnBDI zum Jahresbericht 2021 unter https://www.datenschutz-berlin.de/infothek/jahresberichte/rede-zum-jahresbericht-2021/.

Kanäle mithilfe von Targetingverfahren maßgeschneiderte Inhalte an ausgewählte Adressat:innen auszuspielen. Diese sollen dadurch so effektiv wie möglich mit der Werbung erreicht werden, d. h. die Instrumente sind dahingehend optimiert, die Adressat:innen so zu beeinflussen, wie von den Werbenden gewünscht.

Auch für politische Werbung werden diese Werbeinstrumente genutzt. Für die Nutzer:innen der Plattformen und Adressat:innen der Botschaften sind die genauen Vorgänge der Datenverarbeitung aber häufig nicht transparent. Das Informationsgefälle zwischen Plattform bzw. Werbenden und Adressat:innen kann dazu führen, dass es für die Adressat:innen schwer einschätzbar wird, was die Werbenden veranlasst hat, speziell sie mit dem spezifisch zugeschnittenen Inhalt anzusprechen. Bei Wahlwerbung und der Werbung mit politischen Botschaften kommt hinzu, dass sich die Adressat:innen darauf verlassen können sollten: Die Inhalte, mit denen sie angesprochen werden, spiegeln die tatsächliche Positionierung der jeweiligen politischen Akteur:innen wider und sind nicht danach ausgerichtet, was für die Adressat:innen vermeintlich am anschlussfähigsten ist. Darüber hinaus sind Informationen über die politische Haltung von Personen besondere Arten personenbezogener Daten, die datenschutzrechtlich nur mit ausdrücklicher und wirksamer Einwilligung der betroffenen Personen verarbeitet werden dürfen.[197]

Natürlich müssen Parteien die Menschen mit ihren Inhalten erreichen, sie bewerben und überzeugen können dürfen. Zentrale Aufgabe der Parteien ist es aber auch, an der politischen Willensbildung mitzuwirken, d. h. den öffentlichen Diskurs anzuregen, die vielfältigen Meinungen zu bündeln, zu Kompromissen zu führen, zu koordinieren und zu organisieren. Vor diesem Hintergrund haben wir in unserem offenen Brief Folgendes thematisiert: Bei der Nutzung von sog. Microtargetingverfahren zur Bewerbung von politischen Botschaften steht zu befürchten, dass das zielgenaue Ausspielen von politischer Werbung auf der Grundlage von umfassenden Nutzungsprofilen nicht dazu führt, den öffentlichen Diskurs anzuregen und zu fördern. Wir gehen eher davon aus, dass die Debatten in kleinteilige Gruppen verlagert und fragmentiert sowie polarisierende Inhalte ggf. verstärkt werden bzw. das vorgebliche Bild von einer „öffentlichen Meinung“ verzerrt wird. Für die Adressat:innen wird es immer schwieriger, aus den vom eigenen Interessensprofil vorgegebenen Einordnungen auszubrechen. Letztlich kann die starke Fokussierung auf die Interessensprofile auch dazu führen, dass die Adressat:innen nur noch damit konfrontiert werden,

[197] Art. 9 Abs. 1 und 2 lit. a DSGVO.

was sie vermeintlich hören möchten, und dass die Bandbreite von Positionen von Werbenden zu verschiedenen Themen sie nicht mehr erreicht.

Als Reaktion auf unseren offenen Brief nahmen die Datenschutzbeauftragten der FDP, von Bündnis90/Die Grünen, der SPD, der Linken und der CDU Kontakt mit uns auf. Intensiv erörterten wir, inwieweit es die Aufgabe der politischen Willensbildung erforderlich macht, auch die Dienste der großen Onlineplattformen zu nutzen, um die vielen Menschen zu erreichen, die sich weitestgehend über ihre Social-Media-Kanäle informieren. Dem entgegen steht aus unserer Sicht die Frage, ob die Nutzung von Werbeinstrumenten, die auf der Grundlage umfangreicher Verarbeitungen personenbezogener Daten ausgerichtet sind, Menschen so stark wie möglich zu beeinflussen, geeignete Instrumente politischer Werbung sein können. Letztendlich sind die Gefahren dieser Art von digitaler Wahlwerbung auch durch den Europäischen Gesetzgeber erkannt und aufgegriffen worden. Mit der Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO)[198] hat die Europäische Union (EU) konkrete Regelungen für das Targeting und die Anzeigenschaltung im Zusammenhang mit politischer Werbung im Internet getroffen. Diese Regelungen greifen in großen Teilen erst ab Oktober 2025 und sehen eine Zuständigkeit der Datenschutzaufsichtsbehörden[199] für die Überwachung der Vorgaben zum Targeting und zur Anzeigenschaltung im Zusammenhang mit politischer Werbung im Internet[200] vor. Sowohl der Arbeitskreis Medien der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) als auch der Europäische Datenschutzausschuss (EDSA) in der zuständigen Expertengruppe haben angefangen, an konkreten Empfehlungen zur Anwendung der Verordnung zu arbeiten.

In unserem offenen Brief haben wir über das Thema des politischen Targeting hinaus die aktuellen, ernstzunehmenden Warnungen vor Versuchen von Sicherheitsangriffen, Desinformationskampagnen und Manipulation von Parteienkommunikation thematisiert. Außerdem haben wir die Parteien auf folgende Publikationen hingewiesen:

- die von der Behörde für europäische politische Parteien und europäische politische Stiftungen (APPF)

[198] Verordnung (EU) 2024/900 des europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung.
[199] Art. 22 Abs. 1 Satz 1 TTPW-VO.
[200] Art. 18 und 19 TTPW-VO.

veröffentlichte umfangreiche Studie zur Einflussnahme auf Wahlen und demokratische Prozesse in der EU[201]
- die vom Europäischen Kompetenzzentrum für die Bekämpfung hybrider Bedrohungen (Hybrid CoE) herausgegebenen Handlungsempfehlungen[202]

Vor dem Hintergrund der anstehenden Wahlen sollten sich nicht nur die Datenschutzbeauftragten einiger Parteien, sondern insbesondere die verantwortlichen Parteispitzen sowie Entscheidungsträger:innen in den Parteien mit den datenschutzrechtlichen Implikationen ihrer politischen Werbekampagnen und Auswirkungen auf demokratische Prozesse auseinandersetzen. Wir werden zusammen mit den nationalen und europäischen Aufsichtsbehörden an Empfehlungen zur Anwendung der Verordnung über die Transparenz und das Targeting politischer Werbung arbeiten.

3. Datenschutzverstöße bei politischer Werbung in sozialen Medien

Wir haben aufgrund entsprechender Beschwerden die Wahlwerbung mehrerer Parteien auf Facebook im Bundestagswahlkampf 2021 geprüft. Die verwendeten Targetingfunktionen der Plattform ermöglichen eine gezielte Ansprache von Nutzer:innen, u. a. anhand ihrer prognostizierten politischen Meinung.

Im Vorfeld der Bundestagswahl 2021 schalteten mehrere Parteien personalisierte Werbung auf Facebook. Die Plattform ermöglicht es den Werbetreibenden, ihre Zielgruppen anhand zahlreicher Merkmale auszuwählen – von demografischen Angaben wie Alter, Geschlecht und Wohnort bis hin zu individuellen Interessen, Kaufverhalten und detaillierten Verhaltensmustern. Diese als Targeting bekannte Praxis basiert auf der automatisierten Auswertung des Nutzungsverhaltens: Welche Seiten werden aufgerufen, welche Inhalte „geliked“, wie lange werden Videos angeschaut? Aus diesen Daten erstellt Meta als Unternehmen hinter Facebook detaillierte Persönlichkeitsprofile, die auch Rückschlüsse auf die politische Meinung der Nutzer:innen zulassen.

Das Geschäftsmodell von Meta basiert dabei auf der Verknüpfung verschiedener Datenquellen: Neben den Informationen, die Nutzer:innen bei ihrer Registrierung direkt angeben, werden Nutzungsdaten aus allen Meta-

[201] Abrufbar unter https://www.appf.europa.eu/appf/en/other-information/Studies.
[202] Abrufbar unter https://www.hybridcoe.fi/publications/hybrid-coe-research-report-10-preventing-election-interference-selected-best-practices-and-recommendations/ und https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/.

Diensten (Facebook, Instagram, WhatsApp) zusammengeführt. Zusätzlich erfasst Meta auch Daten von Besuchen konzernfremder Websites, die ihre Analysetools einsetzen. Die daraus resultierenden Profile ermöglichen eine präzise Vorhersage von Konsumverhalten, Interessen und politischen Neigungen.

Die Verarbeitung bestimmter, einem besonderen Schutz unterliegender Daten wie der politischen Meinung ist nach der DSGVO grundsätzlich verboten.[203] Ausnahmen, die eine Verarbeitung erlauben würden – wie eine ausdrückliche Einwilligung oder ein erhebliches öffentliches Interesse – konnten bei unseren Überprüfungen nicht nachgewiesen werden. Im Gegenteil: Das gezielte Ausspielen unterschiedlicher Wahlwerbung an verschiedene Wählergruppen steht dem öffentlichen Interesse eher entgegen, da die Gefahr besteht, dass dies fairen und unbeeinflussten Wahlen entgegenwirkt. Auch der Umstand, dass Nutzer:innen bestimmte Interaktionen teilöffentlich vornehmen, rechtfertigt nicht die systematische Analyse und Kategorisierung ihres politischen Profils.

Da Meta und die jeweils werbende Partei als Verantwortliche die Zwecke und Mittel der Datenverarbeitung gemeinsam festlegen, hätten sie zudem in einer transparenten Vereinbarung ihre jeweiligen datenschutzrechtlichen Pflichten regeln und diese den betroffenen Personen zugänglich machen müssen – auch dies ist nicht geschehen. Die betroffenen Nutzer:innen wurden nicht ausreichend über Art und Umfang der Datenverarbeitung informiert.

Das systematische Microtargeting zur Anzeige politischer Werbung in sozialen Medien wirft grundlegende Fragen für den demokratischen Prozess auf. Wenn Parteien ihre Botschaften gezielt an bestimmte Wählergruppen anpassen können, droht eine Fragmentierung des politischen Diskurses. Statt eines offenen Austauschs von Argumenten können digitale Echokammern entstehen, in denen die Wähler:innen nur noch auf sie zugeschnittene politische Botschaften erreichen. Dies kann die Polarisierung der Gesellschaft verstärken und den demokratischen Willensbildungsprozess beeinträchtigen.

Vier der fünf betroffenen Parteien haben unsere Fragen beantwortet und an der Aufklärung der Sachverhalte mitgewirkt. Eine Verantwortliche ist gegen unsere Aufforderung zur Auskunft gerichtlich vorgegangen. Das Verfahren ist insoweit noch offen.

[203] Siehe Art. 9 DSGVO.

Die gezielte Ansprache von Wähler:innen anhand ihrer mutmaßlichen politischen Meinung durch Targeting-verfahren in sozialen Medien verstößt gegen datenschutzrechtliche Vorgaben: Ohne ausdrückliche Einwilligung der Betroffenen ist die Verarbeitung dieser besonders geschützten Daten unzulässig. Die kürzlich verabschiedete EU-Verordnung über die Transparenz politischer Werbung sieht ab Oktober 2025 strenge Vorgaben für das politische Targeting vor. Künftig müssen Parteien die verwendeten Targetingmethoden offenlegen und dürfen Datenkategorien wie die politische Meinung nicht mehr für das Profiling zur Zielgruppenauswahl nutzen. Dabei geht es nicht nur um den Schutz personenbezogener Daten, sondern auch um die Wahrung demokratischer Grundprinzipien. Die Nutzung digitaler Dienste im Wahlkampf, die mit algorithmischen Empfehlungssystemen und gezielter Werbung für alle denkbaren Produkte und Dienste Geld verdienen, darf nicht zu einer Aushöhlung der informationellen Selbstbestimmung und der Grundvoraussetzungen demokratischer Wahlen führen.

XIV. Betroffenenrechte

1. Unzulässiges Erschweren der Geltendmachung von Löschungsansprüchen

Im Rahmen einer Beschwerde prüften wir die Umsetzung des Löschrechts durch den Betreiber einer Zyklus-App. Das Unternehmen erschwerte die Ausübung des Löschrechts mit einem unnötig komplizierten Prozedere: Die Nutzerinnen mussten ihre Daten zunächst speichern und dann den Auftrag zur Löschung erneut bestätigen. Wir konnten erreichen, dass das Unternehmen das Verfahren ändert.

Betroffene Personen haben das Recht, von den Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden. Die Verantwortlichen sind verpflichtet, diesem Ersuchen nachzukommen, sofern keine Ausnahmetatbestände vorliegen.[204] Es widerspricht dieser Pflicht zur unverzüglichen Datenlöschung, wenn betroffenen Personen auf ihren Löschantrag hin zunächst aufgegeben wird, ihre Daten zu speichern, und sie sich danach noch einmal an die Verantwortlichen wenden müssen, um den Löschantrag erneut zu bestätigen. Darüber hinaus haben Verantwortliche betroffenen Personen die Ausübung ihrer Betroffenenrechte, also auch ihres Rechts auf Datenlöschung, zu erleichtern.[205] Dazu müssen sie

[204] Art. 17 Datenschutz-Grundverordnung (DSGVO).
[205] Art. 12 Abs. 2 Satz 1 DSGVO.

Modalitäten festlegen, die eine einfache unentgeltliche Beantragung der Löschung ermöglichen.[206]

Wir haben das Unternehmen auf die Rechtslage hingewiesen. Daraufhin hat das Unternehmen den Löschprozess angepasst und nimmt jetzt auf Löschanträge der Nutzerinnen eine unmittelbare Löschung von deren Daten vor. Darüber, dass eine Datenlöschung nicht rückgängig gemacht werden kann und daher eine vorherige Speicherung der Daten – diese können die Nutzerinnen über eine Back-up-Funktion in der App selbst vornehmen – sinnvoll sein kann, informiert das Unternehmen nunmehr in den FAQ (häufig gestellte Fragen) der App.

Geht ein Löschantrag bei einem Verantwortlichen ein, hat dieser unverzüglich zu prüfen, ob die Daten der Antragstellerin bzw. des Antragstellers gelöscht werden können. Ist dies der Fall, muss die Löschung sofort erfolgen. Es ist nicht zulässig, der betroffenen Person aufzugeben, ein eindeutig formuliertes Löschungsersuchen noch einmal zu bestätigen. Verantwortliche sind zudem verpflichtet, betroffenen Person Informationen über die auf ihren Löschantrag ergriffenen Maßnahmen grundsätzlich unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags, zur Verfügung zu stellen.[207]

2. Datenminimierender Nachweis der Auskunftserteilung

Verantwortliche müssen nachweisen können, dass sie Auskunftsersuchen nach Art. 15 DSGVO rechtzeitig und korrekt beantwortet haben. Hierfür ist es allerdings nicht nötig und daher auch nicht zulässig, die erteilten Auskünfte standardmäßig vollständig aufzubewahren. Mittels technischer und organisatorischer Maßnahmen kann der Nachweis auch unter Beachtung des Grundsatzes der Datenminimierung so geführt werden, dass nur wenige Daten vorgehalten werden.

Jeder Mensch hat das Recht, Auskunft über die zur eigenen Person verarbeiteten Daten zu erhalten.[208] Das Auskunftsrecht ist Bestandteil des Grundsatzes der Transparenz.[209] Die Beweislast für die Erfüllung des Auskunftsanspruchs liegt bei den Verantwortlichen, die nachweisen können müssen, dass die Datenschutzgrundsätze eingehalten werden.[210] Doch wie der Nachweis konkret zu führen ist, ist gesetzlich nicht geregelt.

[206] Erwägungsgrund (ErwGr.) 59 DSGVO.
[207] Art. 12 Abs. 3 Satz 1 DSGVO.
[208] Art. 15 DSGVO.
[209] Art. 5 Abs. 1 lit. a DSGVO.
[210] Art. 5 Abs. 2 DSGVO (sog. Rechenschaftspflicht).

Dies führt zu Unsicherheiten in der Praxis und so mancher Überlegung, die erteilten Auskünfte vollständig über Jahre zu speichern.

Da die Auskünfte personenbezogene Daten enthalten, muss für ihre Speicherung eine Rechtsgrundlage bestehen.[211] Als Rechtsgrundlage kommt die rechtliche Verpflichtung der Verantwortlichen in Betracht, die Einhaltung der Datenschutzgrundsätze nachzuweisen.[212] Auch könnte die Aufbewahrung im berechtigten Interesse des Verantwortlichen stehen.[213] Allerdings muss die Verarbeitung in beiden Fällen auch erforderlich sein, um die rechtliche Verpflichtung zu erfüllen bzw. die berechtigten Interessen zu wahren. Die Erforderlichkeit ist nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) im Zusammenhang mit dem Grundsatz der Datenminimierung[214] zu prüfen. Sobald die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, sind sie zu löschen.[215] Zulässig ist die Speicherung damit, wenn sie „unbedingt notwendig“[216] bzw. „objektiv unerlässlich“[217] ist, um den Nachweis zu führen. Das geht aber auch ohne konkret erteilte Auskünfte:

Bei einem normalen Risikoniveau ermöglicht die Dokumentation der verwendeten Auskunftsvorlagen, der Zeiträume ihres Einsatzes und des Verfahrens bei Auskunftsersuchen eine generelle Überprüfung der Auskunftspraxis, etwa auf Vollständigkeit und Verständlichkeit. Moniert eine betroffene Person im Einzelfall die erhaltene Auskunft, wäre diese im Beschwerdeverfahren vorzulegen. Für das auskunftserteilende Unternehmen könnte es dann darauf ankommen, überprüfen zu können, ob die vorgelegte Auskunft manipuliert ist.

Um Manipulationen nachträglich zu erkennen, gibt es verschiedene Möglichkeiten, unter denen es im Einzelfall im Rahmen der Technikgestaltung[218] auszuwählen gilt. So sollten elektronisch erteilte Auskünfte grundsätzlich mit einer digitalen Signatur[219] versehen werden. Bei Auskünften auf Papier kann die digitale Signatur für die rein textförmigen Anteile gebildet und abgedruckt werden. Einen weiteren Manipulationsschutz

[211] Art. 6 Abs. 1 DSGVO.
[212] Siehe Art. 6 Abs. 1 Satz 1 lit. c DSGVO i. V. m. Art. 5 Abs. 2 DSGVO.
[213] Art. 6 Abs. 1 Satz 1 lit. f DSGVO.
[214] Art. 5 Abs. 1 lit. c DSGVO.
[215] Art. 17 Abs. 1 lit. a DSGVO.
[216] EuGH, Urteil vom 7. Dezember 2023, C-26/22 und C-64/22, Rn. 88.
[217] EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 98.
[218] Art. 25 Abs. 1 DSGVO.
[219] Zu digitalen Signaturen allgemein JB 2019, 2.2.

bieten Farblaserdrucker, die einen kaum sichtbaren, jedoch gerätespezifischen Code[220] auf das Papier drucken, der die Seriennummer des Druckers enthält. Gegen die Entnahme einzelner Seiten helfen Seitenzahlen auf der Auskunft. Auskünfte auf Briefpapier, auf ungewöhnlichem Papier oder Papier derselben Marke machen Fälschungen aufwendiger. Wenn nur wenige Auskünfte erteilt werden, helfen auch manuelle Maßnahmen wie Stempeln oder Paraphieren der einzelnen Blätter. Ungewöhnliche Stempel-, Stift- oder Druckfarben erschweren Manipulationen zusätzlich.

Ferner sollte der Vorgang der Beauskunftung als solcher mit Zeitangabe und ggf. den beauskunfteten Datenkategorien (idealerweise revisionssicher) protokolliert werden, um eine tatsächlich stattgefundene Auskunftserteilung darlegen zu können. Im Rahmen dieser Protokollierung sollte jeder Datensatz anstelle der beauskunfteten personenbezogenen Daten mit einem eindeutigen Pseudonym verknüpft werden. Das Ziel ist hier, das Risiko einer unbefugten Offenlegung identifizierender Informationen gegenüber internen oder externen Stellen zu reduzieren und zugleich eine Wiederherstellung des Personenbezugs zu einer erteilten Auskunft unter bestimmten Bedingungen zu ermöglichen.[221] Ein möglicher Ansatz für die Erzeugung eines solchen Pseudonyms – im Anbetracht eines normalen Risikoniveaus – ist bspw. die Anwendung einer Einwegfunktion auf eine kleine normalisierte[222] Untermenge personenbezogener Daten (z. B. E-Mail-Adresse, Vor- und Nachname sowie Postleitzahl).

Nach erfolgter Auskunftserteilung mit Speicherung eines pseudonymisierten Protokolldatensatzes kann der Auskunftsdatensatz gelöscht werden. Erst mit Kenntnis der Untermenge der personenbezogenen Daten – die i. d. R. von der betroffenen Person bereitgestellt werden kann – kann zu einem späteren Zeitpunkt dargelegt werden, dass die Auskunft für die betroffene Person erteilt wurde. Aus dem Ergebnis der Einwegfunktion dagegen lassen sich die Ursprungsdaten praktisch nicht zurückrechnen. Bei erhöhten Risiken bietet es sich zusätzlich an, Zufallswerte in die Einwegfunktion einfließen zu lassen. Der Zufallswert bzw. das erzeugte Pseudonym sollte anschließend in verschlüsselter Form abgelegt werden, sodass es nur durch eine Treuhandstelle entschlüsselt werden kann.

[220] Sog. Machine Identification Code.

[221] Siehe Europäischer Datenschutzausschuss (EDSA), Guidelines 1/2025 on Pseudonymi-sation vom 16. Januar 2025, Rn. 27, abrufbar unter https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en.

[222] Durch die Normalisierung werden die Daten in eine einheitliche Form gebracht, bei der je nach konkretem Anwendungsfall bspw. kleinere Abweichungen in der Schreibweise wie Groß- und Kleinbuchstaben, Umlaute oder deren Ersetzung durch ASCII-Zeichen, Leerzeichen usw. irrelevant sind.

Als Versandnachweis beim Versand per E-Mail sollte Folgendes protokolliert werden:

- der Zeitstempel der E-Mail
- die Message-ID der E-Mail
- der sendende Server
- der empfangende Server (MX-Record)
- der Zeitstempel des Erhalts des SMTP-Quittungscodes 250
- die Bestätigungsnachricht (SMTP-Reply mit 250-Code und ggf. weiteren Informationen)

Bei postalischem Versand per Einschreiben sollte Folgendes protokolliert werden:

- das Datum des Schreibens
- die Sendungsnummer
- der Zustellstatus
- das Zustelldatum
- der Auslieferungsnachweis

Auch normale Briefe lassen sich über die Sendungsnummer bzw. den Matrixcode der Briefmarke heutzutage beschränkt nachverfolgen, sodass diese Daten neben Zustellstatus und Datum der voraussichtlichen Zustellung laut Sendungsverfolgung protokolliert werden sollten.

Die dargestellten Verfahren sorgen dafür, dass nur diejenigen Daten gespeichert bleiben, die tatsächlich erforderlich sind, um den Nachweiszweck zu erfüllen. Eine längerfristige vollständige Speicherung der erteilten Auskunft dagegen würde den Datenbestand zum Auskunftszeitpunkt verstetigen, auch wenn etwa die verarbeiteten Daten rechtswidrig verarbeitet wurden oder eine sehr kurze Aufbewahrungsfrist besteht. Eine solche dauerhafte Vorratsdatenspeicherung wäre übermäßig und nicht gerechtfertigt.

Beim Versand einer Auskunft per E-Mail sind nicht nur die Anforderungen des Art. 32 Abs. 1 DSGVO zu beachten.[223] Der E-Mail-Server sollte zudem so konfiguriert werden, dass im Fall eines Zustellfehlers die vollständige E-Mail zurückgesendet wird. Die Auskunft kann dann nochmals versandt werden.

[223]Siehe auch Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ vom 27. Mai 2021, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/orientierungshilfen/2021-DSK_OH-E-Mail-Verschluesselung.pdf.

Die Verantwortlichen haben die Antragstellenden allgemein über die Verarbeitung ihrer Daten zum Zwecke des Auskunftsnachweises zu informieren.[224] Bei Löschanträgen sind die Antragstellenden zusätzlich in der gesetzlich vorgeschriebenen Löschbestätigung[225] über die Gründe der Vorhaltung des Auskunftsnachweises[226] und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, zu informieren.[227] Der datenreduzierte Auskunftsnachweis darf im Hinblick auf etwaige drohende zivilrechtliche Ansprüche[228] grundsätzlich entsprechend der regelmäßigen zivilrechtlichen Verjährungsfrist für drei Jahre ab dem Ende des Jahres, in dem der Auskunftsantrag gestellt wurde – zuzüglich einer angemessenen Frist von bis zu drei Monaten für die Zustellung einer eventuellen Klage –, gespeichert werden.[229] Die tatsächliche Einhaltung dieser Frist sollten Verantwortliche durch ein wirksames Löschkonzept[230] sicherstellen.

Der Nachweis der Auskunftserteilung bei gleichzeitiger Einhaltung des Grundsatzes der Datenminimierung erfordert ein durchdachtes Konzept. Gezielt eingesetzte technische und organisatorische Maßnahmen machen es den Verantwortlichen möglich, ihrer Rechenschaftspflicht nachzukommen, ohne Klardaten oder gar die gesamte Auskunft aufbewahren zu müssen.

3. Wann sind Anträge von Betroffenen „exzessiv“?

In der Praxis kommt es vor, dass sich Verantwortliche ggf. über einen gewissen Zeitraum mit einer Vielzahl von DSGVO-Anträgen, z. B. auf Auskunft oder Löschung, konfrontiert sehen. Manchmal argumentieren die Verantwortlichen, dass diese Anträge exzessiv seien und sie sich deshalb zu Recht weigern können, die Anträge zu bearbeiten.

Häufig erreichen uns in unserer Aufsichtsarbeit Beschwerden von Bürger:innen, deren Betroffenenrechte nach Art. 15 ff. DSGVO von datenschutzrechtlich verantwortlichen Unternehmen, Behörden oder Vereinen verweigert werden. Einer der meist genannten Gründe für diese Verweigerung der Verantwortlichen ist die Erklärung, die betroffenen Personen würden ihre Anträge rechtsmissbräuchlich stellen, weil sie z. B. häufig hintereinander Anträge stellen. Oder sie stünden in einem zivilrechtlichen Streit mit dem Verantwortlichen

[224] Art. 13 Abs. 1 und 2 DSGVO.
[225] Art. 12 Abs. 3 Satz 1 DSGVO.
[226] Z. B. zur Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO gem. Art. 17 Abs. 3 lit. b DSGVO.
[227] Art. 12 Abs. 4 DSGVO.
[228] Z. B. nach Art. 82 Abs. 1 DSGVO.
[229] Siehe §§ 195, 199 Abs. 1 Bürgerliches Gesetzbuch (BGB).
[230] Siehe Art. 5 Abs. 1 lit. e i. V. m. Art. 25 Abs. 1 DSGVO.

und die Ausübung der Betroffenenrechte würde dementsprechend nicht dem Datenschutz dienen, sondern sei nur ein Vorwand, um die Verantwortlichen unter Druck zu setzen.

So ging in einem unserer Aufsichtsfälle eine Onlineplattform von Rechtsmissbrauch aus, weil eine große Zahl unzufriedener Kund:innen fast 100 Auskunftsersuchen gegenüber dem Unternehmen geltend gemacht hatte. Die Anträge erreichten das Unternehmen, nachdem in einem Onlineforum dazu aufgerufen wurde, entsprechende Auskunftsersuchen bei dem Unternehmen zu stellen, um Druck wegen finanzieller Forderungen gegen das Unternehmen auszuüben und um durch die Inhalte der Datenauskunft womöglich weitere Verstöße festzustellen. In einem früheren Fall verweigerte ein Unternehmen einer Kundin die Auskunft, weil die Kundin gleichzeitig Rechtsanwältin der Gegenseite in einem laufenden Zivilrechtsstreit war.

Bereits letztes Jahr hat der EuGH entschieden, dass betroffene Personen auch einen Anspruch auf Auskunft nach Art. 15 DSGVO haben können, wenn sie einen Zweck verfolgen, der nicht datenschutzrechtlicher Natur[231] ist. Es sind vielmehr auch datenschutzfremde Auskunftszwecke zulässig, wie z. B. die Geltendmachung von Haftungsansprüchen.[232] Dabei geht der EuGH davon aus, dass die betroffenen Personen ihre Anträge auch nicht begründen müssen und die Verantwortlichen eine solche Begründung auch nicht verlangen können.[233]

Die DSGVO sieht in Fällen von Rechtsmissbrauch aber ausdrücklich vor, dass der Verantwortliche bei offenkundig unbegründeten oder – insbesondere im Fall häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person ein angemessenes Entgelt verlangen oder sich weigern kann, aufgrund des Antrags tätig zu werden.[234] In der Praxis ist dabei wichtig, dass die Verantwortlichen die Beweislast für den exzessiven Charakter des Antrags der betroffenen Person tragen.[235]

Aus der Rechtsprechung des EuGH zum Beschwerderecht betroffener Personen gegenüber Aufsichtsbehörden lässt sich folgern, dass Anträge von betroffenen Personen nur dann als exzessiv gelten, wenn Verantwortliche anhand aller relevanten Umstände des Ein-

[231]Siehe ErwGr. 63 Satz 1 DSGVO.
[232]EuGH, Urteil vom 26. Oktober 2023, C-307/22, Rn. 43 ff.
[233]Ebd., Rn. 38.
[234]Art. 12 Abs. 5 Satz 2 DSGVO.
[235]Art. 12 Abs. 5 Satz 3 DSGVO.

zelfalls feststellen können, es liegt eine Missbrauchsabsicht der betroffenen Person vor.[236] Die bloße Zahl der von dieser Person gestellten Anträge reicht dafür bspw. allein nicht aus.[237] Das Vorliegen einer Missbrauchsabsicht kann aber festgestellt werden, wenn eine Person Anträge stellt, ohne dass dies objektiv erforderlich ist, um ihre Rechte aus der DSGVO zu schützen, sondern für einen anderen Zweck, der in keinem Zusammenhang mit diesem Schutz steht.[238] Dies gilt insbesondere dann, wenn sich aus den Umständen ergibt, dass die Anträge darauf abzielen, das ordnungsgemäße Funktionieren des Verantwortlichen zu beeinträchtigen, indem seine Ressourcen missbräuchlich in Anspruch genommen werden.[239]

Nach der Rechtsprechung des EuGH ist Vorsicht geboten vor der voreiligen Ablehnung von Betroffenenanträgen aufgrund angeblichen Rechtsmissbrauchs. Die Anzahl der von einer betroffenen Person gestellten Anträge, so groß sie auch sein mag, ist für sich genommen regelmäßig kein ausreichendes Kriterium, um festzustellen, dass „exzessive“ Anträge vorliegen. Dem Verantwortlichen obliegt es vielmehr nachzuweisen, dass die Anträge in Missbrauchsabsicht gestellt wurden, wie z. B. zur Beeinträchtigung des ordnungsgemäßen Funktionierens eines Unternehmens.

4. Auskunftspflicht für Logdateien

Betroffene Personen haben ein Recht darauf, eine vollständige Auskunft über alle sie betreffenden Daten vom Verantwortlichen zu erhalten. Das Bundesdatenschutzgesetz (BDSG) sieht jedoch eine Ausnahmeregelung für Daten vor, die für Zwecke der Datensicherung oder der Datenschutzkontrolle gespeichert wurden. Im Rahmen eines Beschwerdeverfahrens haben wir die Reichweite dieser Ausnahmeregelung unter Berücksichtigung der jüngsten Rechtsprechung des EuGH geklärt.

In einem Beschwerdeverfahren hat ein ehemaliger Beschäftigter eines Softwareunternehmens eine Auskunft über die ihn betreffenden Daten verlangt.[240] Sein Interesse galt insbesondere den Logdaten, die im Zusammenhang mit dem angespannten Arbeitsverhältnis für ihn relevant waren. Solche Logdaten werden auch als Sekundärdaten bezeichnet, weil sie sich typischerweise nicht auf den Hauptzweck einer Verarbeitung, sondern auf die Aktivitäten von Personen bei der Nutzung von IT und auf Vorgänge in IT-Systemen beziehen. Das Unternehmen war anfangs der Ansicht, dass lediglich

[236] EuGH, Urteil vom 9. Januar 2025, C-416/23, Rn. 50.
[237] Ebd.
[238] Ebd., Rn. 50, 56.
[239] Ebd., Rn. 56.
[240] Siehe Art. 15 DSGVO.

Daten bezüglich der Personalakte und der internen Kommunikation per E-Mail oder per Chat zu beauskunften seien.

Auf unser Einwirken hin hat das Unternehmen auch solche Daten beauskunftet, die in verschiedenen IT-Anwendungen und IT-Infrastrukturkomponenten erzeugt und aufbewahrt wurden und einen Bezug zu der Person des ehemaligen Beschäftigten aufwiesen. Hierzu gehörten u. a. Logdaten des kollaborativen Entwicklungssystems, Server-Logdaten, Netzwerk-Logdaten und Daten aus dem Zeiterfassungssystem. Das Unternehmen war in der Lage, in relativ kurzer Zeit die erforderlichen Datensätze teilautomatisiert aus den betroffenen Systemen auszulesen, aufzubereiten und bereitzustellen.

Unserem Handeln legten wir zum einen die Annahme zugrunde, dass die allenfalls in Betracht zu ziehende Ausnahmeregelung im BDSG – wonach bestimmte Daten wie etwa Logdaten, die für „Zwecke der Datensicherung oder der Datenschutzkontrolle“ erhoben wurden, nicht zu beauskunften sind[241]– hier nicht einschlägig war: Nur wenige Daten wurden ausschließlich zu Zwecken der Datenschutzkontrolle gespeichert. Zudem greift die Einschränkung des Auskunftsrechts nur, wenn die Auskunft über solche Daten einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung von Protokollierungs- und Logdaten zu anderen als den genannten Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Zum anderen stellt sich die Frage, ob die Ausnahmeregelung im BDSG europarechtskonform ist. Eine Ausnahme für bestimmte Datenkategorien sieht Art. 15 DSGVO nicht vor, und es ist zweifelhaft, ob die BDSG-Regelung die Voraussetzungen erfüllt, die die DSGVO für eine Einschränkung des Auskunftsrechts[242] vorsieht.

Der EuGH hat in einem Urteil[243] zum Auskunftsrecht bekräftigt, dass sich die Bereitstellungspflicht auch auf Daten bezieht, die nicht das Handeln der betroffenen Person selbst, sondern den Zugriff von Beschäftigten des Verantwortlichen auf Daten über die betroffene Person dokumentieren. Er hat die Bereitstellungspflicht für diese Art von Daten damit begründet, dass dadurch eine faire und transparente Verarbeitung gewährleistet wird, die es den Betroffenen letztendlich ermöglicht, ihre Rechte nach der DSGVO geltend zu machen.

[241] § 34 Abs. 1 Nr. 2 lit. b BDSG.
[242] Nach Art. 23 DSGVO.
[243] EuGH, Urteil vom 22. Juni 2023, C-579/21, Rn 69.

Für den Umfang des Auskunftsanspruchs ist der Datenbestand zum Zeitpunkt des Auskunftsverlangens maßgeblich. Die betroffene Person hat dabei stets einen Anspruch auf vollständige und inhaltlich richtige Auskunft über die konkret verarbeiteten Daten nach Maßgabe und im von Art. 15 DSGVO geregelten Umfang.[244] Soweit für das Verständnis der beauskunfteten Daten erforderlich, muss der Verantwortliche die bereitgestellten Daten erläutern. Schließlich muss die Auskunft so gestaltet werden, dass sie die Rechte anderer Personen nicht beeinträchtigt. Auskünfte über die Identität von Arbeitnehmer:innen, die auf Daten zur betroffenen Person zugegriffen haben, sind nur dann zu erteilen, „wenn diese Informationen unerlässlich sind, um es der betroffenen Person zu ermöglichen, die ihr durch [die DSGVO] verliehenen Rechte wirksam wahrzunehmen, und vorausgesetzt, dass die Rechte und Freiheiten dieser Arbeitnehmer berücksichtigt werden“.[245]

Logdaten sind neben den Primärdaten vom Auskunftsanspruch umfasst. Verantwortliche sollten die Auskunftsrechte von betroffenen Personen im Protokollierungs- und Auswertungskonzept berücksichtigen und darauf vorbereitet sein, auch technische Protokolle umfassend zu beauskunften. Dabei sind ggf. die Rechte anderer Personen durch Unkenntlichmachung zu berücksichtigen. Gerade hochgradig digital arbeitende Unternehmen sind gut beraten, teil- oder vollautomatisierte Suchmittel einzurichten und den zugehörigen Auskunftsprozess zu testen, um eine effiziente und rechtskonforme Auskunft zu geben.

5. Technische und organisatorische Voraussetzungen für die Änderung von Vornamen und Geschlechtseinträgen schaffen!

Am 1. November dieses Jahres ist das Gesetz über die Selbstbestimmung in Bezug auf den Geschlechtseintrag (SBGG) in Kraft getreten. Das SBGG erleichtert trans-, intergeschlechtlichen und nichtbinären Personen, ihren Geschlechtseintrag und ihre Vornamen ändern zu lassen. Daraus ergeben sich auch datenschutzrechtliche Verpflichtungen, die Verantwortliche umsetzen müssen.

Noch vor Inkrafttreten des SBGG erreichten uns Beschwerden betroffener Personen, die im Zusammenhang mit der Änderung ihrer Vornamen Anträge auf Berichtigung ihrer personenbezogenen Daten[246] ge-

[244] Siehe Simitis/Hornung/Spiecker (Hrsg.), Datenschutzrecht. DS-GVO (beck-online), Art. 15, Rn. 13, 16; Kühling/Buchner (Hrsg.), DS-GVO (beck-online), Art. 15, Rn. 8.
[245] EuGH, Urteil vom 22. Juni 2023, C-579/21, Rn 83.
[246] Siehe Art. 16 DSGVO.

stellt hatten. Sie waren dabei von dem Verantwortlichen (einem Anbieter elektronischer Dienstleistungen) aufgefordert worden, zunächst ein Formular zur Vertragsübernahme durch Dritte auszufüllen, da anders eine Änderung des Vornamens nicht zu bewerkstelligen sei. Außerdem werde für die Berichtigung eine Servicegebühr erhoben, die anschließend erstattet werden solle.

Die Stellungnahme des Unternehmens hat ergeben, dass die technische Ausgestaltung der dortigen IT-Systeme zum Zeitpunkt des Antrags auf Berichtigung eine Änderung des Vornamens allein nicht vorsah. Das Unternehmen ist daher auf das dort praktizierte Verfahren zur Übernahme bestehender Verträge ausgewichen, in dessen Rahmen eine Änderung des Vornamens vorgesehen war. Dabei wurde zunächst versäumt, die damit befassten Servicemitarbeiter:innen wirksam anzuweisen, bei Änderungen von Vornamen die Verwendung des für die Vertragsübernahme vorgesehenen Formulars zu unterlassen. Durch das Fehlen funktionierender Namensänderungsprozesse hat das Unternehmen gegen die Vorgaben der DSGVO zum Datenschutz durch Technikgestaltung[247] verstoßen.

Ein Verfahren, das für eine Datenberichtigung das Ausfüllen eines hierfür nicht erforderlichen Formulars voraussetzt, verstößt darüber hinaus gegen die Bestimmungen der DSGVO, wonach der Verantwortliche der betroffenen Person die Ausübung ihrer Betroffenenrechte erleichtern muss.[248] Die Erhebung einer Servicegebühr für die Berichtigung des Vornamens verstößt gegen eine Bestimmung der DSGVO, wonach u. a. Berichtigungsmaßnahmen grundsätzlich unentgeltlich zur Verfügung gestellt werden müssen.[249] Dies gilt auch für den Fall, dass die Gebühr zuerst erhoben und dann wieder erstattet wird.

Im Ergebnis hat der Verantwortliche aufgrund unserer Intervention die Berichtigungen kostenfrei vorgenommen und ohne dass die betroffenen Personen dafür ein Formular zur Vertragsübernahme ausfüllen mussten. Das Verfahren wurde so umgestellt, dass dies auch zukünftig unterbleibt und auch keine temporäre Gebühr mehr erhoben wird.

Änderungen von Vornamen und Geschlechtseinträgen nach dem SBGG gehen mit Ansprüchen der betroffenen Personen auf Berichtigung ihrer personenbezogenen Daten nach der DSGVO einher. Verantwortliche

[247] Siehe Art. 25 Abs. 1 DSGVO.
[248] Siehe Art. 12 Abs. 2 Satz 1 DSGVO.
[249] Siehe Art. 12 Abs. 5 Satz 1 DSGVO.

sind verpflichtet, entsprechenden Anträgen der betroffenen Personen zu entsprechen und bereits vor deren Eingang die technischen und organisatorischen Voraussetzungen dafür zu schaffen. Besonders zu beachten ist dabei, dass solche Berichtigungen für die betroffene Person regelmäßig kostenfrei sind.

XV. Datenpannen und -technischer Datenschutz

1. Vereinheitlichung der Meldung von Datenpannen

Die Meldung von Datenpannen bei der jeweils zuständigen Aufsichtsbehörde entsprechend den Vorgaben von Art. 33 Datenschutz-Grundverordnung (DSGVO) und die Benachrichtigung der Betroffenen entsprechend Art. 34 DSGVO sind wichtige Transparenzmaßnahmen und für uns regelmäßig Anlass, die Umsetzung von wirksamen technisch-organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus bei Verantwortlichen zu prüfen.

Aufgrund der großen Zahl von eingehenden Datenpannenmeldungen ist es für Aufsichtsbehörden wichtig, ein effizientes Verfahren für deren Sichtung und Bearbeitung anzuwenden. Genauer zu prüfen sind regelmäßig Meldungen, die Anzeichen von systematischen Defiziten bei den meldenden Stellen aufweisen oder bei denen entgegen den gesetzlichen Vorgaben die betroffenen Personen nicht informiert wurden, trotz hoher Risiken, die für sie mit der Datenpanne verbunden sind.

Wir haben einen Austausch zwischen den deutschen Aufsichtsbehörden zu diesem Thema organisiert, um zur Optimierung der Bearbeitungsprozesse beizutragen. Besprochen wurden sowohl organisatorische Fragen – wie die Vor- und Nachteile einer zentralisierten Bearbeitung der Meldungen durch bestimmtes Personal oder die Behandlung gleichförmiger Meldungen verschiedener Verantwortlicher, die aus einer Datenpanne bei (großen) Auftragsverarbeiter:innen resultieren – als auch technische Fragestellungen – wie die Beurteilung der Auswirkungen eines digitalen Einbruchs in IT-Systeme durch unberechtigte Dritte. Einhellig wurde ein Anstieg der Cyberangriffe bestätigt.

Wichtiger Aspekt des Austauschs war auch die Abstimmung untereinander, die insbesondere dann erforderlich ist, wenn bei Auftragsverarbeiter:innen eine Datenpanne aufgetreten ist, die Verantwortliche in mehreren Bundesländern betrifft. Ebenso wurde diskutiert, ob ein bundesweit einheitliches Meldeportal zur Steigerung der Effizienz beitragen könnte. Zudem wäre

eine einheitliche statistische Auswertung der gemeldeten Datenpannen wünschenswert, um bei auffälligen Trends besser und schneller steuernd eingreifen zu können.

Der erste Workshop zur Vereinheitlichung der Meldung und Bearbeitung von Datenpannen diente dem Erfahrungsaustausch und der Identifizierung von Themen, bei denen eine verstärkte Zusammenarbeit Vorteile sowohl für die Meldenden und die Betroffenen von Datenpannen als auch für die Aufsichtsbehörden bringen wird. Die Zusammenarbeit soll fortgeführt werden, um die skizzierten Ziele zu erreichen.

2. Nicht gelöschte Daten als Datenpannenrisiko

Uns erreichen immer wieder Meldungen und Hinweise zu Datenpannen oder Sicherheitslücken, bei denen Dritten Daten zugänglich waren, die nicht rechtzeitig gelöscht oder mehrfach gespeichert und unzureichend geschützt wurden. Verantwortliche In-stitutionen müssen schon bei der Konzeptionierung von Datenverarbeitungssystemen sowohl Speicher- als auch Löschkonzepte berücksichtigen und bei der Umsetzung ein besonderes Augenmerk auf deren korrekte Implementierung richten.

Anfang Juni dieses Jahres erhielten wir einen anonymen Hinweis auf eine zum Bewerberportal einer politischen Partei gehörenden Datenbank, die über das Internet öffentlich zugänglich war. Eine Überprüfung zeigte Listen mit mehr als 4.860 Vor- und Nachnamen, die ohne Zugangsbeschränkung einsehbar waren. Weitere Details zu einzelnen Personen waren nicht ersichtlich. Wir informierten den Datenschutzbeauftragten der Partei, der für eine umgehende Abschaltung des ungeschützten Zugangs sorgte.

Die Partei nutzte das Portal für die Entgegennahme von Bewerbungen und den Versand von Zwischenbescheiden. Ein Abgleich mit internen Systemen belegte die Offenbarung aller Namen aus Bewerbungen, die seit November 2016 über das Portal bei der Bundesgeschäftsstelle eingingen. Ursächlich für die Zugriffsmöglichkeit war eine fehlende oder fehlerhafte Überprüfung von Zugangsberechtigungen. Wie eine Überprüfung der Entwicklungsumgebung des Portals zeigte, bestand diese Möglichkeit seit Beginn der Nutzung.

Fehlende oder fehlerhaft implementierte Berechtigungsprüfungen stellen einen Verstoß gegen Art. 32 Abs. 1 DSGVO dar. Verantwortliche Institutionen sowie deren Auftrags-verarbeiter:innen sind verpflichtet, geeignete technische und organisatorische Maßnahmen

zu treffen, die ein dem Risiko angemessenes Schutzniveau gewährleisten. Die von der Partei ergriffenen Maßnahmen begegneten dem Risiko der unbefugten Offenlegung von Namen der Bewerberinnen und Bewerber nicht in ausreichendem Maße.

Erschwerend kam hinzu, dass die meisten der Daten bereits hätten gelöscht sein müssen. Werden – wie im vorliegenden Fall – personenbezogene Daten zum Zweck der Durchführung eines Bewerbungsverfahrens erhoben, sind diese nach Beendigung des Verfahrens[250] zu löschen, da sie danach nicht mehr zur Erfüllung des angegebenen Zwecks erforderlich sind.[251] Hätte für das Portal ein Löschkonzept vorgelegen und wäre dieses korrekt umgesetzt worden, hätte die gefundene Sicherheitslücke weitaus weniger Personen betroffen.

Ein weitere Datenpanne, die auch unzulässig bzw. zu lange gespeicherte Daten betraf, ereignete sich bei einem Unternehmen, das für seine Kund:innen einen flexiblen Zugang zu verschiedenen Sport- und Fitnessangeboten ermöglicht. In einem Cloudspeicher wurden eine Kopie der internen Kundendatenbank sowie Buchungsdaten einzelner Sportstätten abgelegt. Diese Daten sollten nur temporär in dem Cloudspeicher abgelegt werden, um sie in andere Systeme zu überführen. Nach der Überführung wurde die Löschung der personenbezogenen Daten jedoch über Jahre „vergessen“. Erschwerend kam hinzu, dass der betreffende Cloudspeicher ohne Zugangsbeschränkung über das Internet zugänglich war, was offensichtlich niemals überprüft wurde.

Kenntnis von der Sicherheitslücke erhielten wir auch hier durch einen anonymen Hinweis. Wir konnten aufgrund der Angaben des Hinweisgebers im März Stammdaten von ca. 30.000 Kund:innen des Unternehmens aus den Jahren 2015–2018 sowie ca. 100.000 Besuchsdaten aus einer Reihe von Fitnesseinrichtungen um den Jahreswechsel 2019/2020 dokumentieren. Der Hinweisgeber legte außerdem dar, dass die Daten bereits im Darknet zum Kauf angeboten würden.

Auf unseren Hinweis hat das Unternehmen unverzüglich und grundsätzlich angemessen reagiert: Die Sicherheitslücke wurde sofort geschlossen und die betroffenen Kund:innen zeitnah informiert. Uns gegen-

[250] Zur Verteidigung gegen Beschwerden nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) können die Bewerbungsdaten für höchstens sechs Monate nach Abschluss gespeichert werden.
[251] Siehe Art. 6 Abs. 1 Satz 1 lit. b DSGVO.

über hat das Unternehmen fristgerecht eine Datenpannenmeldung[252] abgegeben und ergänzt, nachdem die eigenen Untersuchungen und die eines beauftragten IT-Forensik-Unternehmens abgeschlossen waren.

Nach derzeitiger Erkenntnis bewerten wir in beiden Fällen die technischen und organisatorischen Maßnahmen der verantwortlichen Institutionen über den gesamten Zeitraum von der Entscheidung zur Nutzung der technischen Infrastruktur für die (Zwischen-)Speicherung bis zur Schließung der Sicherheitslücken als unzureichend. Die Verfahren zum Umgang mit schützenswerten personenbezogenen Daten waren nicht angemessen: Es fehlte allem Anschein nach eine umfassende Planung und Überwachung von Speicherorten, sodass über mehrere Jahre umfangreiche personenbezogene Daten ohne jeden Zweck gespeichert wurden. Auch Konzepte zur Löschung nicht mehr benötigter Daten lagen demnach offensichtlich nicht vor. Damit wurden mutmaßlich grundlegende Vorgaben der DSGVO bei der Vorbereitung und im Zuge der Datenverarbeitung nicht eingehalten. Nach abschließender Prüfung der Vorfälle werden wir ggf. weitere Maßnahmen ergreifen. Dafür stehen uns verschiedene Abhilfebefugnisse zur Verfügung.[253]

Verantwortliche müssen Datenschutzmanagementsysteme einrichten und Löschkonzepte umsetzen, sodass regelmäßig überprüft wird, welche Daten tatsächlich weiterhin notwendig sind, und ob insbesondere die Vertraulichkeit der Daten nach aktuellem Stand der Technik geschützt ist. Basis ist die Härtung der Serversysteme und ein starker logischer Zugangsschutz, der i. d. R. auf einer schlüsselbasierten oder Mehrfaktor-Authentifizierung basieren muss. Unnötig oder mehrfach gespeicherte personenbezogene Daten erhöhen das Risiko, dass Daten in falsche Hände geraten.

3. Häufige Ursachen für Datenpannen

Verantwortliche sind verpflichtet, uns zu melden, wenn eine Verletzung der Sicherheit personenbezogener Daten zu deren unbefugter Offenlegung oder zu einem unbefugten Zugriff auf sie geführt hat.[254] Wir erhalten eine Vielzahl derartiger Meldungen. Darin sind Muster für häufige Ursachen solcher Datenpannen zu erkennen.

Schulen und Kindertagesstätten

[252] Siehe Art. 33 DSGVO.
[253] Siehe Art. 58 Abs. 2 DSGVO.
[254] Art. 33 DSGVO.

Kinder bedürfen eines besonderen Schutzes. Dies betrifft auch Daten, die sich auf sie beziehen. In pädagogischen Einrichtungen werden verschiedene Arten von Daten verarbeitet: Stammdaten, Verhaltensbeurteilungen, Unterlagen zur Kindeswohlgefährdung, Entwicklungsbeurteilungen und nicht zuletzt Fotos der Kinder. Leider erhalten wir regelmäßig Meldungen über unbefugten Zugang zu diesen Daten. Dieser kann seine Ursache in unzureichend gesicherter Informationstechnik haben. Häufig gehen jedoch elektronische Datenträger einfach verloren oder werden gestohlen. Das können Laptops, Foto- und Videokameras oder auch Speichersticks sein. Sind die Daten dort unverschlüsselt gespeichert, können sie eingesehen werden. Diebe mögen nicht primär an den Daten interessiert sein, die sich auf den gestohlenen Geräten befinden. Im Zuge eines Verkaufs des Diebesguts können sie dennoch in Hände von Personen gelangen, die die Daten missbrauchen. Daher ist in der Regel von einem hohen Risiko für die betroffenen Kinder auszugehen. Diese Risiken im Nachhinein zu mindern, ist schwierig. Zumindest müssen die Erziehungsberechtigten über den Vorfall benachrichtigt werden.

Es ist jedoch verhältnismäßig einfach, negativen Folgen eines Verlusts oder Diebstahls elektronischer Geräte entgegenzuwirken. Datenträger sollten in ausreichend gesicherten Behältnissen und Räumlichkeiten gelagert werden. Allein mit einer derartig sicheren Aufbewahrung ohne Verschlüsselung wird jedoch oft kein ausreichend zuverlässiger Schutz erreicht. Davon zeugen die bei uns eingegangenen Meldungen zu Datenträgern, die dann doch versehentlich entgegen den Vorgaben ungesichert abgelegt worden sind. Die Verschlüsselung aller mobilen Datenträger ist deshalb zusätzlich regelmäßig das Mittel der Wahl.

In Schulen, in denen ältere Kinder und Jugendliche unterrichtet werden, sollte auch die Findigkeit der Unterrichteten nicht unbeachtet bleiben. Eine zentrale Speicherung der personenbezogenen Daten vermindert die Gelegenheiten für einen unbefugten Einblick in Aufzeichnungen über Mitschüler:innen. Der Speicherort, wie z. B. ein Schulportal, muss jedoch darauf ausgelegt sein, unbefugte Zugriffe aus dem Internet zurückzuweisen. Vom Eigenbau oder der Nutzung von Produkten und Dienstleistungen von Anbieter:innen, die ihre Sicherheitskompetenz nicht nachweisen können, raten wir dringend ab.

Fehlversand

Ein hoher Anteil an Datenpannenmeldungen betrifft den Versand von Unterlagen an falsche Empfänger:in-

nen. Dies geschieht sowohl elektronisch als auch postalisch. Uns wurde u. a. der Fehlversand von Abrechnungen medizinischer Dienstleistungen, Konto-, Pfändungs-, Lohn- und Sozialdaten sowie Immobilieneinstufungen mitgeteilt. Durch den Fehlversand erhalten fremde Personen u. U. sehr private Daten des persönlichen Lebens der richtigen Adressat:innen. Ehrliche Empfänger:innen senden postalische Sendungen zurück und löschen fehlgeleitete elektronische Nachrichten. Doch auch ein Missbrauch durch die Empfänger:innen oder Personen mit Zugriff auf deren Post ist möglich. So können die betroffenen Menschen bloßgestellt, einer Gefahr ausgesetzt oder in der Zukunft benachteiligt werden.

Derartigen Vorfällen kann auf vielfältige Weise vorgebeugt werden. Am Anfang steht die Qualität der Adressdaten. Sie sollte regelmäßig überprüft werden. Ein automatisierter Versand kann zur Vermeidung falscher Adressierung aufgrund menschlicher Fehler beitragen. Wird die Adressierung durch Mitarbeitende durchgeführt, helfen klare Handlungsanweisungen, die z. B. auf eine Überprüfung der Übereinstimmung von Anrede und Adressat:in eines Briefs zielen, eine Sensibilisierung der Beschäftigten für die Konsequenzen von Fehlern und ihre Auswirkungen beinhalten sowie ein konzentrationsförderndes Arbeitsumfeld schaffen. Für besonders sensible Unterlagen kann schließlich das Vier-Augen-Prinzip hilfreich sein.

Eine weitere Ursache für den Fehlversand kann in der technischen Umsetzung von Druck und Kuvertierung liegen. Ein Testbetrieb im Vorfeld vermeidet einige der möglichen Fehler.

Phishing, Ransomware und kompromittierte E-Mail-Accounts

Im letzten Jahr berichteten wir ausführlich über Phishing und Ransomware.[255] Auch in diesem Jahr verzeichneten wir eine Reihe von Meldungen aufgrund von Ransomwareangriffen. Die Täter:innen verfolgen verschiedene Wege, um Zugriff auf die IT-Infrastruktur von Unternehmen zu erhalten. Ein wichtiger Angriffsvektor ist Phishing, dessen Einsatz durch Angreifer:innen auch in diesem Jahr häufig war. Die Beschäftigten des Unternehmens geben dabei Kennwörter, die Zugang zu IT-Ressourcen ermöglichen, auf einer durch Angreifer:innen bereitgestellten gefälschten Plattform preis.

[255] Siehe JB 2023, A.IX.4.

Schon ein einzelner kompromittierter Account kann zur Ausspähung des Opferunternehmens und zur Ausweitung des Angriffs auf weitere Konten und die IT-Infrastruktur genutzt werden. Diese Zugangsmöglichkeiten werden dann für verschiedene Ziele verwendet, wobei die Erpressung der Opfer die häufigste und für die Täter:innen ertragreichste Methode ist. Die personenbezogenen Daten in einem gekaperten Konto können abgezogen werden, um zusätzlich mit der Veröffentlichung der Daten zu drohen. Schließlich werden übernommene E-Mail-Accounts auch für weitere, zielgerichtete Phishing-Angriffe und für den Spam-Versand genutzt.

Um solche Angriffe zu vermeiden, ist eine effektive Aufklärung über Vorgehensweisen notwendig, mit denen Beschäftigte vermeiden können, Kennwörter an Angreifer:innen preiszugeben. Ein Zugriff auf ein Konto sollte, wo immer möglich, nur über ein sicheres Log-in-Verfahren, z. B. mittels schlüsselbasierter oder Zwei-Faktor-Authentisierung, ermöglicht werden. Ausführliche Hinweise zur Angriffsvermeidung sind beim Bundesamt für Sicherheit in der Informationstechnik (BSI) erhältlich.

Dem Risiko von Datenpannen kann und muss mit technischen und organisatorischen Schutzmaßnahmen begegnet werden: Mobile Datenträger sollten verschlüsselt, Beschäftigte und Mitarbeitende über Phishing-Attacken aufgeklärt und sensibilisiert sowie sichere Log-in-Verfahren und schlüsselbasierte oder Zwei-Faktor-Authentisierung eingeführt werden. Dies sind geeignete Maßnahmen, um das Risiko von häufig vorkommenden Datenpannen zu verringern bzw. negative Folgen bei Verlust oder Diebstahl abzumildern. Sie sind nach dem Stand der Technik umzusetzen.

Die Senatsverwaltung für Bildung, Jugend und Familie hat im edukativen Bereich bereits umfangreiche technische und organisatorische Maßnahmen umgesetzt, um das Risiko von Datenpannen zu minimieren. Datenträger der mobilen Endgeräte für pädagogische Beschäftigte (MEG) sind grundsätzlich verschlüsselt, Zugriff auf die MEGs ist nur nach Anmeldung möglich.
Durch die Einführung des § 64 c im Berliner Schulgesetz wurden gesetzliche Grundlagen für ein effektives Identitätsmanagement geschaffen. Der Zugriff auf das Berliner Schulportal ist ausschließlich authentifizierten und autorisierten Personen gestattet. Die Zwei-Faktor-Authentisierung erfolgt über die „Bildung im Dialog“-App.
Durch das Identitätsmanagement erhalten die pädagogischen Beschäftigten Zugriff auf ein dienstliches E-Mail-Konto, welches eine Ende-zu-Ende Verschlüsselung mit S/MIME und einen Spam-Filter beinhaltet.
Ein Mobile-Device-Management sorgt dafür, dass die neuesten Sicherheitsupdates automatisch installiert werden. Im Falle von Diebstahl oder Verlust kann das mobile Endgerät aus der Ferne gesperrt und die Daten gelöscht werden.

XVI. Medienkompetenz

In diesem Jahr haben wir unser Engagement für die Förderung der Medienkompetenz von Kindern und Jugendlichen intensiviert. Wir haben unser Workshopprogramm erweitert und die kontinuierliche Arbeit an unserem Internetauftritt fortgesetzt, um viele junge Menschen für das Thema Datenschutz zu sensibilisieren. Die enge Zusammenarbeit mit medienpädagogischen Fachkräften und unsere Präsenz auf wichtigen Bildungs- und Digitalveranstaltungen haben dazu beigetragen, einen bewussteren und sichereren Umgang mit digitalen Medien zu fördern. Wir wollen nicht nur die Medienkompetenz der Schülerinnen und Schüler stärken, sondern auch Lehr- und Fachkräfte in ihrer pädagogischen Arbeit unterstützen.

Pädagog:innen stehen noch immer vor der Herausforderung, digitale Medien sinnvoll in den Schulalltag zu integrieren. Damit Schüler:innen in ihrer Lebenswelt abgeholt und ihr Umgang mit Medien geschult wird, bedarf es eines reflektierten Einsatzes digitaler Medien im Unterricht. Um Schulen in ihrer Arbeit zu unterstützen, haben wir unser Workshopprogramm erweitert. Wir haben in diesem Jahr 39 Workshops in Grundschulklassen der Jahrgangsstufen 4 bis 6 an verschiedenen Schulen durchgeführt. Durch vielfältige Formate sensibilisieren wir dabei die Schüler:innen für die Bedeutung des Datenschutzes und klären sie über ihre Rechte in Bezug auf Privatsphäre, informationelle Selbstbestimmung und den Schutz persönlicher Daten auf. Besonderen Wert legen wir auf den verantwortungsvollen Umgang mit sozialen Medien, das Bewusstsein für bestehende Risiken und die Auswirkungen der Nutzung Künstlicher Intelligenz.

Die Arbeit an unserer Website data-kids.de wurde auch in diesem Jahr fortgesetzt. Auf data-kids.de haben wir überarbeitete Lehrmaterialien mit didaktischen Anleitungen für Lehrkräfte bereitgestellt, damit diese die Inhalte unserer Workshops auch eigenständig an Schulen nutzen können. Unter dem Motto „Datenschutz spielerisch erleben“ präsentieren wir zudem vier neue interaktive Spiele, die sich an Kinder zwischen 6 und 13 Jahren richten. Die Spiele können auf dem Smartphone, Computer oder Tablet genutzt werden und umfassen ein Richtig-oder-Falsch-Quiz, ein Memory, ein Fehlersuchbild und ein Kreuzworträtsel zu wichtigen Datenschutzbegriffen. Kinder können damit spielerisch ihr Wissen über Datenschutz prüfen und lernen, was zum Schutz ihrer Daten und ihrer Privatsphäre zu beachten ist.

Im Zuge unserer Zusammenarbeit mit der Senatsverwaltung für Bildung, Jugend und Familie (SenBJF) haben wir zudem den digitalen „Berliner Datenschutzwegweiser für Kitas“ entwickelt.[256] Dieses Angebot im Rahmen der Initiative „DigitalPakt Kita“ setzt ein deutliches Zeichen für den Datenschutz in Kindertagesstätten. Die Website richtet sich an Kitafachkräfte und Träger, bietet praxisnahe Unterstützung und schafft mehr Transparenz bei Datenschutzfragen im Kitaalltag.[257]

Außerdem waren wir in diesem Jahr auf zwei wichtigen Messen aktiv: der didacta 2024 und der re:publica 2024. Auf der didacta, Europas größter Bildungsmesse, präsentierten wir unsere Arbeit zusammen mit anderen deutschen Landesdatenschutzbehörden erstmals an einem gemeinsamen Stand. Dabei standen die Vermittlung von Datenschutz im Unterricht und die Förderung der digitalen Bildung durch unsere Websites youngdata.de und data-kids.de im Fokus. Lehrkräfte zeigten großes Interesse an praktischen Ansätzen zur Integration von Datenschutzthemen in den Schulalltag. Auch auf der re:publica 2024 stellten wir unser medienpädagogisches Programm vor und boten verschiedene Aktionen für die Öffentlichkeit an.

Durch die Erweiterung unseres Workshopangebots und die Entwicklung neuer didaktischer Materialien konnten wir das Bewusstsein für Datenschutz bei Kindern und Jugendlichen nachhaltig fördern. Dies zeigt die positive Resonanz von Schüler:innen und Lehrkräften sowie die erfolgreiche Zusammenarbeit mit medienpädagogischen Fachkräften. Angespornt durch diese Ergebnisse werden wir unser Engagement fortsetzen und weiter intensivieren, um jungen Menschen auch in Zukunft die notwendigen Kompetenzen für einen verantwortungsvollen und sicheren Umgang mit digitalen Medien zu vermitteln.

B. Wir in Deutschland

I. Gesetzesvorhaben des -Bundes

1. Wir setzen uns für eine einheitliche Auslegung des Datenschutzrechts ein – auch ohne BDSG-Reform

Ein für den Datenschutz wichtiges Gesetzgebungsvorhaben wurde in der abgelaufenen Legislaturperiode nicht mehr finalisiert: Die Reform des Bundesdatenschutzgesetzes (BDSG). Dabei war u. a. vorgesehen,

[256] Siehe A.VIII.1.
[257] Weitere Informationen sind unter www.datenschutzwegweiser-kita.de verfügbar.

die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) als Institution im Gesetz zu verankern. Im Gespräch war es auch, dieser eine Geschäftsstelle einzurichten.

Den Datenschutzaufsichtsbehörden in Deutschland wird immer wieder vorgeworfen, dass sie bei der Auslegung des Datenschutzrechts zu unterschiedlichen Ergebnissen kommen. Tatsächlich enthalten die Datenschutzgesetze, allen voran die Datenschutz-Grundverordnung (DSGVO), viele unbestimmte und damit auslegungsbedürftige Rechtsbegriffe. Die deutschen Datenschutzaufsichtsbehörden arbeiten daher schon seit etlichen Jahren in der DSK und ihren Arbeitskreisen eng zusammen, um dort Klarheit zu schaffen, wo gesetzliche Festlegungen fehlen bzw. Regelungen interpretationsoffen sind. Dazu veröffentlicht die DSK regelmäßig Beschlüsse, Orientierungshilfen und Anwendungshinweise für die Praxis. Die geplante Institutionalisierung der DSK, und insbesondere die Einrichtung einer Geschäftsstelle, hätte diese Arbeit deutlich fortentwickelt und erleichtert.

Gemeinsam mit anderen deutschen Datenschutzaufsichtsbehörden haben wir das Vorhaben daher begrüßt und uns für die Einrichtung einer Geschäftsstelle eingesetzt. Darüber hinaus haben wir uns auch zu den weiteren Bestandteilen des bereits erstellten Gesetzentwurfs[258] geäußert, um den Bundesgesetzgeber zu beraten. Dies betraf u. a. geplante Regelungen zum Scoring, zum Schutz von Betriebs- und Geschäftsgeheimnissen bei Auskunftsansprüchen und zu länderübergreifenden Datenverarbeitungsvorhaben. Außerdem haben wir auf weiteren wichtigen Reformbedarf hingewiesen, wie z. B. die Anpassung von Bußgeldvorschriften, die in dem Gesetzentwurf fehlte.[259]

Wir hoffen, dass die neue Bundesregierung die BDSG-Reformpläne bald wieder aufgreift. Dessen ungeachtet werden wir uns weiter intensiv mit anderen Datenschutzaufsichtsbehörden in der DSK und ihren Arbeitskreisen abstimmen. Das ist nicht nur wichtig, um eine konsistente Datenschutzaufsicht innerhalb Deutschlands zu etablieren, sondern auch, um sicherzustellen, dass diese sich auf internationaler und europäischer Ebene – insbesondere im Europäischen Datenschutzausschuss (EDSA) – effektiv einbringen kann. Unserer Behörde kommt in diesem Zusammenhang im nächsten Jahr eine besondere Verantwortung zu, da wir 2025 den Vorsitz in der DSK innehaben und die Aktivitäten der DSK koordinieren werden.

[258] BT-Drs. 20/10859.
[259] Siehe unter https://www.datenschutzkonferenz-online.de/media/st/240412_BDSG-E_Stellungnahme_DSK.pdf.

Wir hoffen, dass das Reformvorhaben zum BDSG von der neuen Bundesregierung schnell wieder aufgegriffen und die Institutionalisierung der DSK vorangetrieben wird. Auch ohne BDSG-Reform arbeiten wir intensiv mit anderen deutschen Datenschutzaufsichtsbehörden zusammen, um eine konsistente Aufsicht zu fördern und uns effektiv in die europäischen Entscheidungsprozesse einbringen zu können.

2. Umsetzung der KI-Verordnung in nationales Recht: Wer ist für die KI-Aufsicht zuständig?

Am 1. August dieses Jahres ist die europäische KI-Verordnung (KI-VO)[260] in Kraft getreten. Sie sieht eine Aufsichtsstruktur u. a. durch Marktüberwachungsbehörden vor, die in den Mitgliedstaaten gesetzlich bestimmt werden müssen. Die DSK hatte sich bereits am 3. Mai positioniert[261]: Sie empfiehlt, die Datenschutzaufsichtsbehörden in den nicht spezifisch anderen Behörden zugewiesenen Bereichen als Marktüberwachungsbehörden für die Nutzung oder Entwicklung von KI-Systemen für den internen Gebrauch durch Unternehmen und Behörden einzusetzen.

In vielen Fällen werden mit KI-Modellen bzw. -Systemen personenbezogene Daten verarbeitet bzw. Modelle und Systeme werden mit solchen trainiert oder justiert. Zu diesen Datenverarbeitungen trifft die KI-VO im Wesentlichen keine Regelungen, sondern überlässt die datenschutzrechtliche Bewertung dieser Verarbeitungen der DSGVO.[262] Das heißt, die Datenschutzaufsichtsbehörden sind nach der DSGVO ohnehin dafür zuständig, diese Verarbeitungen zu beaufsichtigen. Vor diesem Hintergrund setzen wir uns dafür ein, dass auch die Marktüberwachung nach der KI-VO – dort, wo nicht anderweitig zugewiesen – auf die Datenschutzaufsichtsbehörden übertragen wird. Mit der Aufsicht aus einer Hand können eine einheitliche Ausübung der mit den Datenschutzanforderungen eng verknüpften Verpflichtungen der KI-VO ermöglicht und Koordinierungsaufwand zwischen parallelen Aufsichtsstrukturen vermieden werden.

Im Mai dieses Jahres haben wir unsere Empfehlung sowie das Positionspapier der DSK dem Regierenden

[260] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

[261] Positionspapier der DSK vom 3. Mai 2024: „Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO)“, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf.

[262] Die KI-VO lässt die DSGVO im Wesentlichen unberührt, siehe Art. 2 Abs. 7 KI-VO.

Bürgermeister übermittelt und dabei betont, dass mit der Aufsicht aus einer Hand Berliner Unternehmen und Behörden eine einheitliche Ansprechpartnerin in Sachen KI-VO und DSGVO hätten.

Allerdings zeigten die Verlautbarungen zur Mitte und zum Ende des Jahres, dass beim Bund und offenbar auch in vielen Landesregierungen eine zentralisierte Bundesaufsicht für die Aufsichtsstruktur der KI-VO favorisiert wird: In einem Beschluss[263] begrüßt die Digitalministerkonferenz der Länder (DMK) den Vorschlag des Bundesministeriums für Wirtschaft und Klimaschutz und des Bundesministeriums der Justiz, dass der Bundesnetzagentur im Hinblick auf die Marktüberwachung eine zentrale Rolle zukommen soll. Beim Einsatz von KI in den Landesverwaltungen strebt die DMK eine Lösung an, „die eine möglichst einheitliche Rechtsanwendung sicherstellt".[264] Wie dies geschehen soll, bleibt unklar. Eine Marktüberwachung des Bundes über die Länder bedürfte voraussichtlich einer Verfassungsänderung. So haben wir uns auch gegenüber dem Regierenden Bürgermeister positioniert.

Unbeachtet bleibt zudem, dass die KI-VO für Kernelemente der demokratischen Ordnung den Datenschutzaufsichtsbehörden die Aufgabe der Marktüberwachung bereits zuweist: Insofern heißt es in der KI-VO, dass die Mitgliedstaaten als Marktüberwachungsbehörden für Hochrisiko-KI-Systeme in den Bereichen Biometrie (für Strafverfolgungszwecke, Grenzmanagement, Justiz und Demokratie), Strafverfolgung, Migration, Asyl, Grenzkontrolle sowie Rechtspflege und demokratische Prozesse die Datenschutzaufsichtsbehörden benennen (bzw. jene Behörden, die die Aufsicht im Bereich der Strafvollstreckung und -verfolgung innehaben, was in Deutschland ebenfalls die Datenschutzaufsichtsbehörden sind).[265] Ein eindeutiges Signal, wie diese Vorgaben im deutschen Durchführungsgesetz Beachtung finden werden, ist bisher ausgeblieben.

In den Diskussionen um die Aufsichtsstruktur der KI-VO spielt die Frage der Innovationsförderung eine entscheidende Rolle. Fast scheint es, als ob die Regulierung von KI, die immer wieder auch als innovationsfeindlich oder Hemmnis kritisiert wurde, durch eine maximal innovationsfreundliche Aufsichtsstruktur wieder „eingefangen" werden soll. In dem zitierten Beschluss der DMK wird einer zukünftigen Marktüberwachung bereits ins Stammbuch geschrieben, „die KI-

[263]DMK, Beschluss vom 18. Oktober 2024: „Zusammenwirkungen von Bund und Ländern bei der Durchführung der EU-Verordnung über künstliche Intelligenz".
[264]Ebd.
[265]Siehe Art. 74 Abs. 8 Satz 1 KI-VO u. a. mit Verweis auf die Behörden nach Art. 41–44 der Richtlinie (EU) 2016/680.

Verordnung innovations- und mittelstandsfreundlich“ anzuwenden.[266] Innovationsförderung ist aber nicht das einzige Zielbild der KI-VO, vielmehr geht es um die Förderung von menschenzentrierter und vertrauenswürdiger KI: Neben der Innovationsförderung steht die Forderung nach einem hohen Schutzniveau der in der EU-Grundrechtecharta verankerten Grundrechte. Innovation wird in Europa also als Innovation im Rahmen der europäischen Werte verstanden. Dies sollte auch bei den Überlegungen der nationalen Aufsichtsstruktur eine Rolle spielen.

Bei den bisherigen Überlegungen auf Bundes- und Landesebene zur Umsetzung der Aufsichtsstruktur der KI-VO ist vieles noch unklar. Insbesondere scheinen die Zuweisung der Marktüberwachung in den Bereichen Biometrie (für Strafverfolgungszwecke, Grenzmanagement, Justiz und Demokratie), Strafverfolgung, Migration, Asyl, Grenzkontrolle sowie Rechtspflege und demokratische Prozesse an die Datenschutzaufsichtsbehörden sowie die Frage der Marktüberwachung bei der öffentlichen Verwaltung noch nicht zu Ende gedacht. Die Datenschutzaufsichtsbehörden blicken auf eine langjährige Expertise im digitalen Grundrechtsschutz zurück. Die Abwägung verschiedener Interessen bildet das tägliche Kerngeschäft in der Aufsichtspraxis. Wir bleiben also dabei, dass wir uns als Marktüberwachungsbehörden empfehlen!

3. Entwurf eines Gesetzes zur Einführung eines Registerzensus

Ein Gesetzesvorhaben auf Bundesebene sah die Weiterentwicklung der Methode des Zensus zu einem registerbasierten Verfahren vor, indem die Daten, so weit wie möglich, aus vorhandenen Quellen der Verwaltung und Statistik gewonnen, automatisiert zusammengeführt sowie aufbereitet werden. Dafür sollte u. a. ein Bevölkerungsstatistischer Datenbestand (BESD) beim Statistischen Bundesamt (StBA) aufgebaut und dauerhaft betrieben werden. Dieser sollte die Daten aller melde- und ausländerrechtlich in Deutschland erfassten Personen beinhalten. Dagegen bestehen grundlegende Bedenken.

Aufgrund einer europäischen Verordnung muss in jedem Mitgliedstaat der Europäischen Union (EU) alle zehn Jahre eine Zählung der Bevölkerung durchgeführt werden.[267] Dadurch wird ermittelt, wie viele Menschen in Deutschland leben, wie sie wohnen und arbeiten.

[266] DMK, Beschluss vom 18. Oktober 2024.

[267] Art. 1 der Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen.

Diese Volkszählung wird auch als Zensus bezeichnet. Derzeit werden im Rahmen des Zensus bereits in erster Linie Daten aus den Melderegistern genutzt.[268] Die Meldebehörden übermitteln hierfür die Daten aller gemeldeten Personen an die jeweiligen Statistischen Landesämter. Zusätzlich wird eine stichprobenhafte Haushaltserhebung bzw. Befragung der Haushalte durchgeführt.

Für die Zukunft hatte das Bundesministerium des Innern und für Heimat (BMI) in dem dieses Jahr vorgelegten Entwurf eines Gesetzes zur Einführung eines Registerzensus (Registerzensusgesetz – RegZensG-E) eine „Weiterentwicklung der Zensusmethodik hin zu einem registerbasierten Verfahren“ vorgesehen, „bei dem die Zensusdaten aus bereits in der Verwaltung und Statistik vorhandenen Daten und weitestgehend ohne primärstatistische Befragungen gewonnen werden“.[269]

Die Senatsverwaltung für Inneres und Sport (SenInnSport) hatte uns im Rahmen der Länder- und Verbändebeteiligung Gelegenheit zur Stellungnahme zum RegZensG-E gegeben. Wir haben daraufhin unsere generellen Bedenken mitgeteilt, die sich im Wesentlichen auf den Aufbau und die Führung eines BESD beziehen.[270] Nach dem Gesetzentwurf sollte der BESD zentral beim StBA geführt werden. Dazu wäre der nahezu vollständige Datenbestand des Berliner Melderegisters und damit aller in Berlin melde- und ausländerrechtlich erfassten Bürger:innen sowie die entsprechenden Datenbestände aller anderen deutschen Meldebehörden zentral gespiegelt worden. Angesichts der Größe des so geschaffenen Datenbestands beim StBA sowie des Umfangs der fortlaufenden Datenverarbeitungen und der daraus resultierenden hohen Eingriffsintensität in das Recht auf informationelle Selbstbestimmung der betroffenen Personen wären bereits strenge verfassungsrechtliche Anforderungen zugrunde zu legen.

Hinzu kommt, dass nicht erkennbar war, inwiefern die Einrichtung eines solchen Datenbestands überhaupt erforderlich ist, jedenfalls bedarf die Durchführung eines Registerzensus keines zentralisierten Datenbestands. Die Erforderlichkeit wurde in den Ausführungen zum RegZensG-E insbesondere mit künftigen Vorgaben nach EU-Recht begründet, obwohl derzeit noch völlig offen ist, ob und mit welchem Inhalt die entsprechenden Regelungen in Kraft treten werden. Zudem war nicht nachvollziehbar, aus welchen Gründen allein das BESD diese (noch nicht bekannten) Anforderungen der

[268] Sog. registergestützter Zensus.
[269] Siehe BMI, Referentenentwurf vom 28. Mai 2024, abrufbar unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/RegZensErpG.html.
[270] Siehe § 8 RegZensG-E.

EU-Vorgaben erfüllen sollte. Eine Auseinandersetzung mit anderen Modellen war ebenfalls nicht ersichtlich.

Darüber hinaus wurde der Aufbau und Betrieb eines BESD ausweislich des Begründungsentwurfs insbesondere auch mit der Herstellung bzw. Sicherstellung eines Qualitätsniveaus der zu Zensuszwecken benötigten Daten gerechtfertigt. Dabei wurde außer Betracht gelassen, dass u. a. im Rahmen der Registermodernisierung bereits Regelungen zur Verbesserung der Qualität von den zu Statistikzwecken genutzten Registerdaten, insbesondere der Melderegisterdaten, eingeführt wurden.[271] Die Ergreifung weiterer Maßnahmen zur Verbesserung der Qualität der Melderegisterdaten aus Statistikgründen ist auch im Hinblick auf den Grundsatz der Datenminimierung[272] problematisch, da die Meldebehörden Daten sowohl an das Bundesverwaltungsamt (BVA) als Registermodernisierungsbehörde als auch an das StBA als Verantwortlicher für das BESD übermitteln und so zusätzliche Datenverarbeitungen erfolgen würden.

Die Einrichtung eines BESD wäre als Eingriff in die Datenschutzrechte der betroffenen Personen rechtfertigungsbedürftig. Hier muss eine Abwägung mit milderen, gleich geeigneten Mitteln zur Erreichung eines qualitativ hochwertigen Registerzensus inklusive einer Betrachtung der jeweiligen Auswirkungen auf das Recht auf informationelle Selbstbestimmung erfolgen. Das Bundesverfassungsgericht (BVerfG) hat ausdrücklich festgestellt, dass die zukünftige Methodenentwicklung daraufhin beobachtet werden muss, ob sie grundrechtsschonendere Verfahren ermöglicht.[273] Der Gesetzentwurf ließ dies vermissen.

4. Digitaler Check-in und gesetzliche Neuerungen bei Beherbergungsbetrieben

Beherbergungsbetriebe stellen zunehmend auf digitale Check-in-Verfahren um. Reisen-den soll damit die Möglichkeit eingeräumt werden, bereits vor ihrem Aufenthalt über ihr Smartphone, Tablet oder ihren Computer digital einzuchecken. Das jüngst verabschiedete Vierte Bürokratieentlastungsgesetz (BEG IV) bringt gesetzliche Neuerungen mit sich, die sich auf die Erhebung und Verarbeitung personenbezogener Daten im Rahmen des digitalen Check-in bei Beherbergungsbetrieben beziehen.

[271] Siehe Registermodernisierungsgesetz (RegMoG).
[272] Art. 5 Abs. 1 lit. c DSGVO.
[273] BVerfG, Urteil vom 19. September 2018, 2 BvF 1/15 und 2BvF 2/15, Rn. 284.

Wir haben in diesem Jahr eine Reihe von Beschwerden zu digitalen Check-in-Verfahren in Beherbergungsbetrieben wie Hotels und Anbieter:innen von Ferienwohnungen erhalten. Dabei kritisierten einige Beschwerdeführer:innen, dass ihnen die Beherbergungsbetriebe keine analoge Alternative zum Online-Check-in zur Verfügung stellen. Andere beschwerten sich, dass sie im Rahmen dieses Verfahrens eine Vielzahl von personenbezogenen Daten zur Verfügung stellen müssen, deren Verarbeitung nicht erforderlich sei, etwa die Angabe des Geschlechts, die Telefonnummer oder gar ein ungeschwärztes Ausweisdokument.

Beherbergungsbetriebe unterliegen den Vorschriften aus dem Bundesmeldegesetz (BMG). Leiter:innen von Beherbergungsstätten haben danach für alle Beherbergten besondere Meldescheine bereitzuhalten[274], die folgende Daten enthalten müssen:

Die Datenverarbeitung im Rahmen eines digitalen Check-in bei touristischen Übernachtungen muss auf eine Rechtsgrundlage gestützt werden.[275]

- Datum der Ankunft und der voraussichtlichen Abreise
- Familiennamen und Vornamen
- Geburtsdatum
- Staatsangehörigkeit
- Anschrift
- Zahl der Mitreisenden und deren Staatsangehörigkeit
- Seriennummer des anerkannten und gültigen Passes oder Passersatzpapieres[276]

Für elektronische Meldeverfahren legt das BMG fest, welche Anforderungen Beherbergungsbetriebe zu erfüllen haben;[277] so haben sie durch geeignete technische und organisatorische Maßnahmen[278] sicherzustellen, dass die zu erhebenden Daten in den dafür festgelegten Verfahren verarbeitet werden. Die Meldepflicht kann mit Zustimmung der beherbergten Person auch dadurch erfüllt werden, dass die im Gesetz genannten Daten elektronisch erhoben werden und die beherbergte Person deren Richtigkeit und Vollständigkeit am Tag der Ankunft bestätigt.[279] Das BMG sieht dabei drei digitale Verfahren vor, welche die händische Unterschrift ersetzen sollen:

[274] § 30 Abs. 1 Satz 1 BMG.
[275] Siehe Art. 6 Abs. 1 Satz 1 DSGVO.
[276] § 30 Abs. 2 Satz 1 BMG; siehe zu den Vorgaben für die elektronische Speicherung des Daten-satzes § 2 i. V. m. der Anlage (zu § 2 Abs. 5) der Beherbergungsmeldedatenverordnung (BeherbMeldV).
[277] § 30 Abs. 5 BMG.
[278] Nach Art. 24, 25 und 32 DSGVO.
[279] § 29 Abs. 5 BMG.

- ein kartengebundener Zahlungsvorgang mit einer starken Kundenauthentifizierung
- die Erbringung des elektronischen Identitätsnachweises[280]
- die Verwendung der eID-Karte[281]

Durch das BEG IV wird ab dem 1. Januar 2025 die Meldepflicht bei touristischen Übernachtungen so weit wie möglich abgeschafft. Für deutsche Staatsangehörige besteht zukünftig keine Meldepflicht mehr in Beherbergungsbetrieben, sodass aus datenschutzrechtlicher Sicht dort damit auch die Rechtsgrundlage zur Erfassung der Daten der Meldebescheinigung für diese Personengruppe entfällt.[282] Für Beherbergungsbetriebe ergibt sich damit sowohl im analogen als auch im digitalen Kontext, dass sie beim Check-in-Verfahren für deutsche Staatsangehörige nur noch diejenigen personenbezogenen Daten erheben dürfen, die zur Durchführung des Beherbergungsvertrags erforderlich sind.[283]

Im Hinblick auf Personen ohne deutsche Staatsangehörigkeit sieht das Unionsrecht[284] allerdings vor, dass beherbergte Ausländer:innen, einschließlich der Angehörigen anderer Schengen-Staaten sowie anderer Mitgliedstaaten der Europäischen Gemeinschaften, grundsätzlich einer Hotelmeldepflicht unterliegen, sodass die Hotelmeldepflicht hinsichtlich dieses Personenkreises erhalten werden musste.[285]

Sofern Beherbergungsbetriebe ausschließlich elektronische Check-in-Verfahren anbieten wollen, sollten sie bereits in der Bewerbung ihrer Angebote transparent auf diesen Umstand hinweisen. Auf diese Weise haben interessierte Kund:innen die Möglichkeit, freiwillig darüber zu entscheiden, ob sie personenbezogene Daten im Rahmen eines Online-Check-in zur Verfügung stellen wollen. Mit Inkrafttreten des BEG IV müssen Beherbergungsbetriebe für ausländische Personen im Hinblick auf die Modalitäten des digitalen Check-in weiterhin die einschlägigen Vorschriften des BMG beachten. Bei deutschen Staatsangehörigen dürfen mit dem Wegfall der Meldepflicht hingegen nur noch solche personenbezogenen Daten erhoben werden, die zur Durchführung des Beherbergungsvertrags erforderlich sind.

[280] Nach neuer Rechtslage nach § 1 eID-Karte-Gesetz (eIDKG) oder nach § 78 Abs. 5 Aufenthaltsgesetz (AufenthG).
[281] Nach neuer Rechtslage nach § 13 eIDKG oder nach § 78 Ab. 5 AufenthG.
[282] Bisher Art. 6 Abs. 1 Satz 1 lit. c DSGVO i. V. m. § 29 Abs. 2 Satz 1, § 30 Abs. 2 Satz 1 BMG.
[283] Siehe Art. 6 Abs. 1 Satz 1 lit. b DSGVO.
[284] Art. 45 Abs. 1 lit. a Schengener Durchführungsübereinkommen (SDÜ).
[285] Siehe BT-Drs. 20/11306, S. 50.

II. Zusammenarbeit mit deutschen Datenschutzaufsichtsbehörden

1. Kostenfreie Auskunftsersuchen bei Ärzt:innen

Immer wieder sind wir mit Fällen befasst, in denen Patient:innen ihre Ärzt:innen bitten, ihnen Auskunft über ihre personenbezogenen Daten aus der Patientenakte zu erteilen. Rechtsunsicherheiten entstehen in diesem Bereich dadurch, dass es in Deutschland gesetzliche Regelungen gibt, die für die Erstellung einer Kopie der Patientenakte eine Kostenerstattungspflicht der Patient:innen vorsehen, während der datenschutzrechtliche Auskunftsanspruch eine kostenlose Erstkopie gewährt. Vor diesem Hintergrund hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Entschließung gefasst, damit hier Rechtsklarheit und Rechtssicherheit geschaffen werden.[286]

Während die Datenschutz-Grundverordnung (DSGVO) einen Anspruch auf eine kostenlose Erstkopie der verarbeiteten personenbezogenen Daten vorsieht,[287] sehen das Bürgerliche Gesetzbuch (BGB)[288] und eine Reihe von Berufsordnungen der Heilberufskammern[289] vor, dass eine Kopie der Patientenunterlagen nur gegen eine Kostenerstattung an die Patient:innen ausgehändigt wird. Der Europäische Gerichtshof (EuGH) stellte allerdings im Jahr 2023 fest, dass durch die Regelung im BGB den Patient:innen keine Kostenlast für die erste Kopie auferlegt werden darf.[290]

Als Vorsitz des Arbeitskreises Gesundheit und Soziales der DSK haben wir gemeinsam mit anderen deutschen Aufsichtsbehörden eine Entschließung erarbeitet, die von der DSK verabschiedet wurde. Mit der Entschließung weisen die deutschen Aufsichtsbehörden darauf hin, dass nach dem Urteil des EuGH dringender Handlungsbedarf für den Bundesgesetzgeber besteht, § 630g Abs. 2 Satz 2 BGB an die Vorgaben der DSGVO anzupassen und das Recht der Patient:innen auf eine kostenlose Kopie ihrer Patientenakte umzusetzen. Darüber hinaus fordert die DSK auch die Heilberufskammern auf, im Sinne eines möglichst einheitlichen Rechtsrahmens und aus Gründen der Rechtsklarheit die berufsrechtlichen Regelungen an die Vorgaben der DSGVO

[286] DSK, Entschließung vom 11. September 2024: „Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden! Datenschutzaufsichtsbehörden sehen konkreten Handlungsbedarf auf Seiten der Heilberufskammern“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2024/20240911_DSK_Patientenakte.pdf.
[287] Art. 12 Abs. 5 Satz 1 und Art. 15 Abs. 3 Satz 1 DSGVO.
[288] § 630g Abs. 2 BGB.
[289] In Berlin z. B. in § 10 Abs. 2 Satz 2 Berufsordnung der Ärztekammer Berlin.
[290] EuGH, Urteil vom 26. Oktober 2023, C-307/22.

anzupassen und – bis zu einer solchen Änderung der Berufsordnungen – ihre Kammermitglieder zu einem rechtskonformen Vorgehen anzuhalten.

Machen Patient:innen einen Auskunftsanspruch gegenüber Ärzt:innen geltend, sind diese verpflichtet, den Patient:innen eine erste Kopie der Patientenakte unentgeltlich zur Verfügung zu stellen. Die noch bestehenden zivil- und berufsrechtlichen Regelungen, die für die Bereitstellung einer Erstkopie eine Kostenpflicht für die Patient:innen vorsehen, sind nicht anwendbar und müssen angepasst werden.

2. Einsatz von Gesichtserkennung durch Sicherheitsbehörden

Die DSK hat sich einstimmig gegen einen voreiligen Einsatz biometrischer Gesichtserkennung ausgesprochen. Sie erwartet im Falle einer Entscheidung durch den Gesetzgeber, dass dieser die unbedingte Notwendigkeit der Vorhaben sorgfältig abwägt und eine Verwendung nur unter strenger Beachtung der relevanten Vorgaben erlaubt.

Der Senat teilt die Auffassung, dass es sich bei der biometrischen Gesichtserkennung um Grundrechtseingriffe handelt, die einer Rechtsgrundlage bedürfen. Der Senat begrüßt es, dass mit dem Antrag der Koalitionsfraktionen über ein Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin (Drucksache 19/2553) eine Rechtsgrundlage für den nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet geschaffen werden soll.

Die DSK hat in einer gemeinsamen Entschließung grundlegende Bedenken zur automatisierten Gesichtserkennung durch Sicherheitsbehörden geäußert.[291] Die Positionierung der Aufsichtsbehörden erfolgte auch vor dem Hintergrund, dass einige Sicherheitsbehörden bereits biometrische Gesichtserkennungssysteme im öffentlichen Raum einsetzen und sich dabei auf strafprozessuale Normen stützen, die dafür keine ausreichende Rechtsgrundlage bieten.[292] Durch einen Einsatz dieser Technologien ohne klaren gesetzlichen Rahmen werden das Recht auf informationelle Selbstbestimmung und die allgemeine Handlungsfreiheit der Bürgerinnen und Bürger nicht angemessen geschützt.

Die Intensität des grundrechtlichen Eingriffs hängt von verschiedenen Faktoren ab: der Art der ausgewerteten Daten, den spezifischen Auswirkungen der automatisierten Verarbeitung sowie der Menge der erfassten Personen. Bei der automatisierten Verarbeitung sind insbesondere eine fehlende unmittelbare menschliche Bewertung der Einzelfälle und die gesteigerte Verar-

[291] DSK, Entschließung vom 20. September 2024: „Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2024/20240920-DSK-Entschliessung-Gesichtserkennung.pdf.

[292] In Berlin etwa §§ 100h, 163f und 98a der Strafprozessordnung (StPO), siehe A.V.1.

beitungskapazität für die Eingriffsintensität maßgeblich; ggf. kommt noch ein technisch bedingtes Eigengewicht durch die eigenständige Bewertungslogik der algorithmischen Analyse hinzu. Die spezifische Funktionsweise der Systeme ist besonders grundrechtsrelevant, da sie zu einer stark schematisierten Bewertung führen kann, die der Komplexität menschlichen Verhaltens nicht immer gerecht wird. Zudem können die getroffenen Entscheidungen aufgrund der komplexen technischen Prozesse für die Betroffenen intransparent und schwer anfechtbar sein.

Besonders problematisch ist die Überwachung im öffentlichen Raum, bei der viele Menschen ohne konkreten Anlass und – bei heimlichem Einsatz – auch ohne ihre Kenntnis erfasst werden. Die neue europäische KI-Verordnung (KI-VO)[293] zieht daher enge rechtliche Grenzen für solche grundrechtsintensiven Anwendungen. Der Europäische Datenschutzausschuss (EDSA) betont hierzu, dass Gesichtserkennungstechnologien nur bei strikter Einhaltung der rechtlichen Rahmenbedingungen eingesetzt werden dürfen.[294] Der Einsatz solcher Technologien durch den Gesetzgeber setzt voraus, dass spezifische Rechtsgrundlagen geschaffen werden, die die Verhältnismäßigkeit und Notwendigkeit der Verarbeitung im Einzelfall nachweisen können.

Die DSK fordert daher, dass die Planung von Gesichtserkennungssystemen, wie sie im „Sicherheitspaket“ der Bundesregierung[295] vorgesehen war, nur erfolgen soll, wenn eine sorgfältige rechtliche Prüfung und Beachtung der Verfassungsmäßigkeit gewährleistet ist. Die Zahl der betroffenen Personen, die Heimlichkeit der Maßnahme, der Grad und die Qualität der Automatisierung und die Art der gesammelten Daten müssen dabei in Betracht gezogen werden. Zusätzlich sollte der Gesetzgeber Schutzmechanismen und Eingriffsschwellen festlegen, um die Rechte der betroffenen Personen zu schützen.

Der technologische Fortschritt darf nicht zu einer schleichenden Aushöhlung von Bürgerrechten führen. Die DSK hat mit ihrer Positionierung ein wichtiges

[293]Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz.
[294]EDSA, Leitlinien 05/2022 vom 26. April 2023 über den Einsatz von Gesichts-erkennungs-technologie im Bereich der Strafverfolgung, abrufbar unter https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_de.pdf.
[295]Die Gesetzesvorhaben aus dem „Sicherheitspaket“ der Bundesregierung wurden in der abgelaufenen Legislaturperiode nur teilweise verabschiedet. Das zustimmungsbedürftige Gesetz zur Verbesserung der Terrorismusbekämpfung wurde durch den Bundesrat abgelehnt (BR-Drs. 512/24 und BT-Drs. 20/13476). Das Gesetz zur Verbesserung der inneren Sicherheit und des Asylsystems wurde durch den Bundestag verabschiedet (BT-Drs. 20/12805 und BT-Drs. 20/13413).

Signal gesetzt: Bevor neue Überwachungstechnologien wie die biometrische Gesichtserkennung eingeführt werden, müssen deren Notwendigkeit und Verhältnismäßigkeit sorgfältig geprüft und klare rechtliche Grenzen gezogen werden.

3. Ein „Einer für alle"-Modell beim Datenschutz?

Im Juli ist das Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZGÄndG)[296] in Kraft getreten. Damit wird das „Einer für alle (EfA)"-Modell[297] als zentrales Nachnutzungsmodell für die Umsetzung des Onlinezugangsgesetzes (OZG) festgelegt. Wir setzen uns dafür ein, dass für die Umsetzung der Datenschutzanforderungen in den OZG-Projekten einheitliche Standards entwickelt werden. Die DSK hat für die mit der Umsetzung des OZG in der Praxis betrauten Stellen eine Anwendungshilfe veröffentlicht, in der die Änderungen des OZG aufgegriffen und praxisnah erläutert werden.[298]

Mit den länderübergreifenden Onlinediensten verankert das OZG das EfA-Modell als zentrales Nachnutzungsmodell bei der Umsetzung der Digitalisierungsprojekte. Bei den Onlinediensten handelt es sich nach der Legaldefinition des OZG um IT-Komponenten zur Abwicklung elektronischer Verwaltungsleistungen von Bund oder Ländern, die insbesondere dem elektronischen Ausfüllen der hierfür erforderlichen Onlineformulare dienen.[299] Kern der „länderübergreifenden Onlinedienste" ist, dass ein Bundesland die für eine oder mehrere Verwaltungsleistungen erforderlichen Antragsdaten zentral sammelt und dann an die für die Gewährung der Verwaltungsleistung jeweils zuständigen Fachbehörden der anderen Bundesländer übermittelt. Insbesondere mit Blick auf die gesetzliche Festlegung der datenschutzrechtlichen Verantwortlichkeit bei EfA-Projekten in § 8a OZG[300] wird von den Umsetzungsverantwortlichen die Erwartung formuliert, dass auch die Kontrolle der Umsetzung der Datenschutzanforderungen bei EfA-Projekten durch die Aufsichtsbehörden effektiv und arbeitsteilig erledigt werden kann.[301]

[296]BGBl. I 2024 I Nr. 245.
[297]Das „Einer für alle"-Modell bedeutet, dass ein Land eine Verwaltungsdienstleistung in der Weise digitalisiert, dass andere Länder diese übernehmen und nachnutzen können. Siehe auch JB 2021, 2.3.
[298]Siehe DSK, Ausgewählte Fragestellungen des neuen Onlinezugangsgesetzes, Anwendungshilfe für Stellen, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen, Version 1.0, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_OZG.pdf.
[299]§ 2 Abs. 8 OZG.
[300]Siehe auch JB 2023, B.I.2.
[301]Der IT-Planungsrat sieht in § 8a OZG den Grundsatz „Einer prüft für alle" definiert, siehe IT-Planungsrat, Beschluss 2024/21 vom 19. Juni 2024, Punkt 5.

Die Voraussetzungen für ein solches „Einer prüft für alle“-Modell bei der Umsetzung der Datenschutzanforderungen lassen sich aber § 8a OZG nicht ohne Weiteres entnehmen. Die Vorschrift weist zwar die datenschutzrechtliche Verantwortung ausdrücklich den Behörden zu, die den länderübergreifenden Onlinedienst betreiben.[302] Daraus folgt aber zunächst nur die Zuständigkeit derjenigen Aufsichtsbehörde, die auch für die den Onlinedienst betreibende Behörde zuständig ist. Das OZG enthält dagegen keine Vorgaben, welche konkreten Datenschutzanforderungen zu prüfen sind.

Wir setzen uns innerhalb der von der DSK eingesetzten Kontaktgruppe OZG 2.0, deren Vorsitz von uns wahrgenommen wird, dafür ein, Kriterien für eine Standardisierung der Prüfung der Datenschutzanforderungen zu entwickeln und die Vorgaben des Datenschutzes in ein standardisiertes Prüfprogramm für länderübergreifende Onlinedienste zu übersetzen. Auf dieser Grundlage können dann standardisierte Prozessschritte entwickelt werden, die die verantwortlichen Behörden bereits während der Entwicklung von länderübergreifenden Onlinediensten selbstständig umsetzen können. Diesen Ansatz einer „Hilfe zur Selbsthilfe“ für die Behörden halten wir für notwendig, weil die Aufsichtsbehörden angesichts begrenzter Kapazitäten und der großen Anzahl künftig zu erwartender OZG-Onlinedienste auf einheitliche Prüfstandards angewiesen sein werden. Wir bringen insoweit unsere Erfahrungen aus der Entwicklung und Anwendung des Standardprozesses Datenschutz bei öffentlichen Digitalisierungsvorhaben für die Berliner Verwaltung[303] ein.

Im Rahmen von EfA-Projekten müssen die Anforderungen des Datenschutzes effektiv und arbeitsteilig umgesetzt werden. Dafür sollten einheitliche Standards der Aufsichtsbehörden entwickelt werden. Wir setzen uns für die Entwicklung dieser Standards innerhalb der DSK ein.

4. Neue Entwicklungen im Forschungsbereich

Der Bundesgesetzgeber hat in diesem Jahr wesentliche Gesetze verabschiedet, die mehr Rechtssicherheit für Forschende hinsichtlich der Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken schaffen und eine Verbesserung der Nutzbarkeit von Gesundheitsdaten zu diesem Zweck ermöglichen sollen. Auch die DSK hat sich in diesem Jahr mit Forschungsthemen befasst.

[302] Siehe hierzu die in § 8a Abs. 4 Satz 1 OZG geregelte Verantwortungszuweisung i. S. d. Art. 4 Nr. 7 Hs. 2 DSGVO.

[303] Siehe https://www.datenschutz-berlin.de/themen/behoerden/standardprozess/.

Mit dem Digital-Gesetz (DigiG) und dem Gesundheitsdatennutzungsgesetz (GDNG) sind zwei Gesetze in Kraft getreten, die die Nutzungsmöglichkeiten von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken wesentlich verbessern sollen. Mit dem DigiG wurde die flächendeckende Einführung der elektronischen Patientenakte für die gesetzlich Versicherten geregelt. Das GDNG regelt die automatisierte Übermittlung der Gesundheitsdaten aus der elektronischen Patientenakte an das Forschungsdatenzentrum Gesundheit (angesiedelt beim Bundesinstitut für Arzneimittel und Medizinprodukte) und die Nutzung der Daten zu wissenschaftlichen Forschungszwecken. Zugleich wurde die Zulässigkeit einer Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, Patientensicherheit und zu Forschungszwecken durch Gesundheitseinrichtungen geregelt.

Die beiden Gesetze dienen auch der Vorbereitung auf den zukünftigen Europäischen Gesundheitsdatenraum (EHDS). Mit der Verordnung zum EHDS[304] soll ein EU-weiter Rechtsanspruch auf einen schnellen und einfachen Zugang zu den eigenen elektronischen Gesundheitsdaten für Patientinnen und Patienten geschaffen werden. Auch Angehörige der Gesundheitsberufe sollen einen umfassenden Zugang zu Daten (z. B. Röntgenbilder, Impfungen etc.) erhalten. Zudem wurden Regelungen für die weitere Nutzung von Gesundheitsdaten zur Patienten- und Produktsicherheit, Forschung, Innovation und Politikgestaltung festgelegt. Der EHDS sieht außerdem für die Primär- und Sekundärnutzung von Gesundheitsdaten standardmäßig Opt-out-Regelungen vor.

Auch die DSK hat sich mit Forschungsfragen beschäftigt. So sieht die DSGVO zahlreiche Regelungen vor, die Datenverarbeitungen zu wissenschaftlichen Forschungszwecken privilegieren und bestimmte Ausnahmen und Einschränkungen von datenschutzrechtlichen Anforderungen vorsehen. Um festzustellen, ob diese privilegierenden Regelungen anwendbar sind, muss geprüft werden, ob eine Verarbeitung tatsächlich zu wissenschaftlichen Forschungszwecken erfolgt. Dies kann regelmäßig nur in einer Einzelfallbeurteilung erfolgen. Wir haben zusammen mit anderen deutschen Datenschutzbehörden in der DSK Kriterien formuliert, die eine Hilfestellung bei dieser Beurteilung geben sollen.[305]

[304]Verordnung über den Europäischen Raum für Gesundheitsdaten (EHDS), abrufbar unter https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_de.
[305]DSK, Beschluss vom 11. September 2024: Positionspapier zum Begriff „wissenschaftliche Forschungszwecke“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2024/20240911_DSK_Wissenschaftliche-Forschungszwecke.pdf.

Die Verarbeitung genetischer Daten zu wissenschaftlichen Forschungszwecken ist die Grundlage für eine personalisierte, auf die individuelle Patientin oder den individuellen Patienten angepasste Präzisionsmedizin. Da es sich um einen hochsensiblen Bereich handelt, fordert die DSK in einem weiteren Positionspapier eine datenschutzkonforme wissenschaftliche biomedizinische Forschung mit genetischen Daten zum Wohle der Patientinnen und Patienten, indem dazu ein gesetzlicher Rahmen geschaffen wird, der sanktionsbewehrte hohe Schutz- und Vertrauensanforderungen und wirksame Mitwirkungs- und Kontrollmöglichkeiten der betroffenen Personen vorsieht.[306]

Die Verarbeitung personenbezogener Daten, insbesondere Gesundheitsdaten, zu wissenschaftlichen Forschungszwecken ist von erheblicher Bedeutung und wurde durch neue Gesetze ausgeformt. Gleichzeitig wurde in Deutschland gesetzlich bereits der Weg zum Europäischen Gesundheitsdatenraum geebnet. Trotz der neuen Regelungen bestehen noch zahlreiche datenschutzrechtliche Fragen. Die Aufsichtsbehörden stehen hierzu miteinander im engen Austausch, um den Forschenden Hilfestellungen zu geben.

5. Eine neue Form der Datenverarbeitung durch die Bezahlkarte

Im Januar hat der Senat beschlossen, dass sich das Land Berlin dem länderübergreifenden Vergabeverfahren zur Einführung einer Bezahlkarte für geflüchtete Menschen anschließt.[307] Die Bezahlkarte ist eine guthabenbasierte Karte mit Debitfunktion, die jedoch nicht mit einem herkömmlichen Girokonto verbunden ist. Sie stellt eine vollständig neue Art der Leistungsgewährung dar. Die Einführung und der Einsatz der Bezahlkarte sind mit der Verarbeitung personenbezogener Daten der Leistungsberechtigten verbunden, die datenschutzrechtliche Grundsatzfragen berühren. Die DSK hat diese Datenverarbeitungsvorgänge in einem Positionspapier[308] rechtlich eingeordnet und die Grenzen eines möglichen Einsatzes von Bezahlkarten aufgezeigt. Das Positionspapier dient als eine Handreichung für die Praxis der Leistungsgewährung. Wir haben an

[306]DSK, Beschluss vom 15. Mai 2024: Positionspapier „Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2024/20240515-DSK-Beschluss-Genetische-Daten.pdf.

[307]Senatskanzlei Berlin, Pressemitteilung vom 31. Januar 2024, abrufbar unter https://www.berlin.de/aktuelles/8692239-958090-berlin-kooperiert-bei-bezahlkarte-fuer-a.html.

[308]DSK, Beschluss vom 19. August 2024: Positionspapier „Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG)“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2024/20240819-DSK-Beschluss-Bezahlkarte.pdf.

dem Positionspapier mitgewirkt und unsere Positionierung der Senatsverwaltung übermittelt.

Bund und Länder haben sich im Herbst 2023 auf die Einführung einer Bezahlkarte verständigt, mit der die Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG) zu gewähren sind. Zunächst wurde eine gesetzliche Grundlage geschaffen, um die Bezahlkarte als Methode der Leistungserbringung zu ermöglichen.[309] Eine spezifische Rechtsgrundlage für die mit dem Einsatz der Bezahlkarte bei den Leistungsbehörden anfallenden Datenverarbeitungsvorgänge hat der Gesetzgeber dabei jedoch nicht vorgesehen.

Für die Verarbeitung personenbezogener Daten durch öffentliche Stellen bedarf es immer einer gesetzlichen Aufgabe sowie einer Datenverarbeitungsbefugnis[310]. Gleichzeitig muss die Datenverarbeitung auch erforderlich sein, um die gesetzliche Aufgabe zu erfüllen. Die gesetzliche Aufgabe der Leistungsgewährung in Form der Bezahlkarte ergibt sich aus den Vorschriften des AsylbLG[311]. Da dort jedoch keine spezifische Rechtsgrundlage für die damit verbundene Datenverarbeitung besteht, muss ein Rückgriff auf die landesdatenschutzrechtlichen Generalklauseln[312] erfolgen. Dies ist jedoch nur soweit möglich, wie ausschließlich die zur Leistungserbringung erforderlichen personenbezogenen Daten verarbeitet werden.

In dem Positionspapier hat die DSK die bei der Umsetzung der Bezahlkarte geltenden datenschutzrechtlichen Grenzen dargestellt. So ist die Einsicht des Kontostands einer Bezahlkarte durch die Leistungsbehörde ohne Mitwirkung der betroffenen Person nicht zulässig. Auch eine pauschale Einschränkung der Nutzungsfunktion der Bezahlkarte auf ein bestimmtes Postleitzahlengebiet ist nicht notwendig, weil damit keine gesetzliche Aufgabe der Leistungsbehörde verfolgt wird. Den für das AsylbLG zuständigen Behörden obliegt lediglich die Aufgabe der Leistungsgewährung, nicht die Durchsetzung von aufenthalts- oder asylrechtlichen Beschränkungen. Auch weist das Positionspapier darauf hin, dass ein Zugriff auf Buchungsdaten der Bezahlkarte durch etwaige Sicherheitsbehörden immer nur aufgrund der spezialrechtlichen Sicherheitsgesetze zulässig ist.

Die Verwaltung muss für den Einsatz der Bezahlkarte auf einen Zahlungsdienstleister als Auftragsverarbeiter

[309]Gesetz zur Anpassung von Datenübermittlungsvorschriften im Ausländer- und Sozialrecht (DÜV-AnpassG) vom 8. Mai 2025, BGBl. I 2024 Nr. 152.
[310]Art. 6 Abs. 1 Satz 1 lit. e, Abs. 2, 3 Satz 1 lit. b DSGVO.
[311]§§ 2, 3 und 11 AsylbLG.
[312]In Berlin: § 3 Berliner Datenschutzgesetz (BlnDSG).

zurückgreifen, der die Durchführung der Transaktionen übernimmt. Da der jeweilige Zahlungsdienstleister behördenübergreifend tätig werden soll, ist insbesondere auf eine Mandantentrennung zu achten, die die Integrität und Vertraulichkeit bei der Verarbeitung der personenbezogenen Daten gewährleistet. Weiterhin muss ein behördenübergreifender Abgleich der Datenbestände beim Zahlungsdienstleister ausgeschlossen werden, da hierfür keine gesetzliche Grundlage besteht. Aufgrund der spezialgesetzlichen Regelungen zum Ausländerzentralregister (AZR) ist insoweit auch ein Zugriff über die landesrechtlichen Generalklauseln gesperrt. Schließlich darf auch eine Weitergabe der Ausländerzentralregister-Nummer (AZR-Nr.) an den Dienstleister nicht erfolgen, da diese nur zur Leistungsprüfung zur Verfügung steht. Im Moment der Einbindung des Dienstleisters zur Ausgabe der Bezahlkarte ist die Leistungsprüfung jedoch schon positiv abgeschlossen, weshalb eine Weiterleitung dieses personenbezogenen Datums nicht erforderlich ist.

Wir haben der in Berlin federführenden Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung (SenASGIVA) im Sommer unsere Beratung bei der Umsetzung der Bezahlkarte im Land Berlin angeboten. Im November hat sich der Senat auf Details der Einführung der Bezahlkarte im Land Berlin verständigt. Wir haben der Senatsverwaltung das Positionspapier der DSK zur Verfügung gestellt. Gleichzeitig haben wir unser Beratungsangebot erneuert.

6. Modelle und Systeme Künstlicher Intelligenz: Hinweise für Hersteller:innen

Dienste und Anwendungen Künstlicher Intelligenz (KI) entwickeln sich derzeit hochdynamisch. Für Verantwortliche entsteht dadurch ein erhöhter Bedarf an datenschutzrechtlicher Beratung. Die DSK hat in diesem Jahr neben einer Orientierungshilfe KI, die sich explizit an Anwender:innen richtet,[313] auch für Hersteller:innen und Betreiber:innen von KI-Systemen ein Positionspapier zu empfohlenen technischen und organisatorischen Maßnahmen erarbeitet. Wir haben uns aktiv daran beteiligt.

Im Mai dieses Jahres veröffentlichte die DSK eine Orientierungshilfe mit datenschutz-rechtlichen Kriterien für die Auswahl und den datenschutzkonformen Einsatz von KI-Anwendungen. Die Orientierungshilfe, zu

[313] DSK, Beschluss vom 6. Mai 2024: Orientierungshilfe „Künstliche Intelligenz und Datenschutz“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/orientierungshilfen/2024-DSK-OH_KI-und-Datenschutz.pdf.

der auch wir beigetragen haben, richtet sich an Unternehmen, Behörden und andere Organisationen und dient als Leitfaden, um KI-Anwendungen auszuwählen und diese datenschutzkonform zu implementieren und zu nutzen. Um auch den Hersteller:innen und Betreiber:innen der diesen Anwendungen zugrunde liegenden Modelle und Systeme datenschutzrechtliche Orientierung zu bieten, erarbeitete eine Unterarbeitsgruppe des DSK-Arbeitskreises Technik unter unserer Beteiligung einen Katalog von empfohlenen technischen und organisatorischen Maßnahmen für die datenschutzfreundliche Entwicklung von KI-Modellen sowie den DSGVO-konformen Betrieb von KI-Systemen, die diese Modelle integrieren. Eine Veröffentlichung dieses Maßnahmenkatalogs ist in Form einer Publikation der DSK geplant.

Der Maßnahmenkatalog orientiert sich an den Gewährleistungszielen des Standard-Datenschutzmodells (SDM). Ziel ist es, für jede Phase des Lebenszyklus eines KI-Systems geeignete technische und organisatorische Maßnahmen zu identifizieren, welche die mit der jeweiligen Verarbeitung personenbezogener Daten verbundenen Risiken ausreichend mindern. Hierdurch soll ein Rahmen geschaffen werden, der den Hersteller:innen und Betreiber:innen von KI-Systemen erlaubt, durch den Einsatz spezifischer Maßnahmen den Anforderungen des Datenschutzrechts zu entsprechen und die Rechte und Freiheiten von natürlichen Personen bei der Entwicklung und dem Betrieb von KI-Systemen zu schützen.

Beispielhaft sei hier das Gewährleistungsziel Transparenz herausgegriffen. Um Transparenz im Zusammenhang mit der Entwicklung und dem Betrieb von KI-Modellen und -Systemen zu gewährleisten, bedarf es in jeder Phase des Systemlebenszyklus einer ausführlichen Dokumentation. So ist bspw. in der Designphase festzulegen, welcher Zweck mit dem KI-System verfolgt werden soll und welche Daten für das Erreichen dieses Zwecks notwendig sind. Der Umfang dieser Daten sollte für ein späteres Training theoriegestützt abgeschätzt werden. All diese Überlegungen sind zur Gewährleistung der Transparenz zu dokumentieren.

In der anschließenden Entwicklungsphase des Modells bzw. des Systems müssen zur Wahrung der Transparenz wiederum andere Faktoren dokumentiert werden. So ist die Herkunft der Rohdaten, die für das Training verwendet werden sollen, von besonderer Wichtigkeit: Welche Institutionen haben sie erhoben und wer hat die Rohdaten anschließend zu Trainingsdaten verarbeitet. Auch ist es sinnvoll, Transparenz im Sinne der Güte und Erklärbarkeit des KI-Systems herzustellen, wobei

Angaben zu gewählten Validierungsmethoden das nötige Niveau an Transparenz schaffen können.

Wie hier für zwei Lebenszyklusphasen bezüglich des Gewährleistungsziels Transparenz angedeutet, werden im Positionspapier Maßnahmen zu allen sieben Gewährleistungszielen für jede Phase des Lebenszyklus eines KI-Systems – vom Design über die Entwicklung und Einführung bis zu Betrieb und Monitoring – technische und organisatorische Maßnahmen beschrieben, die geeignet sind, identifizierten Risiken zu begegnen und ein angemessenes Schutzniveau zu gewährleisten.

Um eine einheitliche Rechtsauslegung aller deutschen Aufsichtsbehörden zu fördern, arbeiten wir mit anderen Aufsichtsbehörden in Deutschland zusammen, erstellen und veröffentlichen gemeinsam mit ihnen praxisrelevante Dokumente. Damit soll sowohl die Prüf- als auch die Beratungspraxis harmonisiert und darüber hinaus Hersteller:innen und Entwickler:innen von KI-Modellen und -Systemen Orientierung bezüglich datenschutzrechtlicher Anforderungen geboten werden.

7. Die neue Orientierungshilfe Digitale Dienste

Seit der Veröffentlichung der Orientierungshilfe Telemedien hat sich einiger Änderungsbedarf ergeben, weshalb in diesem Jahr – als Neufassung – die Orientierungshilfe für Anbieter:innen von digitalen Diensten (OH Digitale Dienste)[314] von der DSK verabschiedet wurde.

Die bisherige Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien (OH Telemedien) befand sich auf dem Stand vom Dezember 2022. Seither haben sich diverse Änderungen ergeben, die eine Überarbeitung der Orientierungshilfe notwendig gemacht haben. Die OH Digitale Dienste ersetzt daher seit November dieses Jahres die bisherige OH Telemedien und befasst sich mit digitalen Diensten wie Websites und Apps, die personenbezogene Daten von Nutzenden verarbeiten und zu Profilen zusammenführen, um das individuelle Verhalten der Nutzenden nachzuverfolgen und die Daten für unterschiedliche Zwecke, meist Werbezwecke, zu verwenden.

Besonders hervorzuheben bei der neuen OH Digitale Dienste ist Folgendes: Die Bezugnahmen auf das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) sind durch solche auf das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) ersetzt und die Ausführungen zu Drittstaatenübermitt-

[314] Abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf.

lungen im Hinblick auf den neuen Angemessenheitsbeschluss zu den Vereinigten Staaten von Amerika[315] geändert worden. Zugleich wurden die Erkenntnisse aus den neuen Leitlinien des Europäischen Datenschutzausschusses (EDSA)[316] zu Art. 5 Abs. 3 ePrivacy-Richtlinie[317] berücksichtigt.

Die OH Digitale Dienste ist durch die vorgenommenen Änderungen auf dem neuesten Stand und bietet dabei für die Anbieter:innen von digitalen Diensten eine hilfreiche Grundlage für die datenschutzkonforme Gestaltung ihrer Websites und Apps. Gleichzeitig bietet die überarbeitete Fassung für die Rechtsanwender:innen die Gelegenheit, entsprechende Arbeitsmittel auf Aktualität zu überprüfen und aktuelle Entwicklungen im Blick zu behalten.

C. Wir in Europa und der Welt

I. Mitarbeit im Europäischen Datenschutzausschuss

1. Pseudonymisierung und Anonymisierung

a) Durch Pseudonymisierung schließt der Verantwortliche aus, dass personenbezogene Daten während ihrer Verarbeitung und ggf. auch unbefugt den Personen zugeordnet werden, auf die sie sich beziehen, und mindert damit die Risiken für die betroffenen Personen. Sie kann aufgrund gesetzlicher Anordnung oder auf Grundlage der Entscheidung des Verantwortlichen angewendet werden, um diesen zu unterstützen, seine datenschutzrechtlichen Verpflichtungen zu erfüllen. Damit stellen sich folgende Fragen: Welchen Nutzen können die Verantwortlichen aus der Anwendung der Pseudonymisierung konkret ziehen und wie setzen sie Pseudonymisierung so um, dass mit ihr die Risiken für die betroffenen Personen wirksam gemindert werden.

Unter der Federführung unserer Behörde hat die Technology Expert Subgroup Datenschutz des Europäischen Datenschutzausschusses (EDSA) Leitlinien zur Pseudonymisierung personenbezogener Daten erarbeitet, die diese Fragen beantworten.[318]

[315] EU-U.S. Data Privacy Framework (DPF).
[316] EDSA, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, abrufbar unter https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf.
[317] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).
[318] EDSA, Guidelines 1/2025 on Pseudonymisation, abrufbar unter https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation.

Die Datenschutz-Grundverordnung (DSGVO) definiert Pseudonymisierung als „Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können“; sie verlangt dabei, dass „diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.[319]

Pseudonymisierung hat den Vorzug, die Risiken für die betroffenen Personen zu mindern, eine Analyse der personenbezogenen Daten jedoch weiterhin weitgehend ohne Beeinträchtigung zu ermöglichen. Sie kann so durchgeführt werden, dass verschiedene Datensätze, die sich auf die gleiche Person beziehen, im Laufe der Verarbeitung zusammengeführt und die Ausgangsdaten nach Abschluss der pseudonymisierten Verarbeitung wiederhergestellt werden können. Dabei lässt sich Pseudonymisierung flexibel einsetzen, denn abseits einer gesetzlichen Verpflichtung kann der Verantwortliche für sich entscheiden, welchen Personen er die Möglichkeit nehmen möchte, die pseudonymisierten Daten den betroffenen Personen zuzuordnen. So kann er einer Arbeitsgruppe innerhalb der eigenen Organisation die Daten pseudonymisiert zur Analyse übergeben, aber auch einem anderen Verantwortlichen als dem Empfänger, der die Daten für eigene Zwecke verarbeitet – ohne dazu jedoch die Daten den betroffenen Personen zuordnen zu müssen. Der Verantwortliche kann Pseudonymisierung auch dazu einsetzen, zu einem angemessenen Schutzniveau für die personenbezogenen Daten beizutragen. Dazu führt er die Pseudonymisierung so durch, dass auch Dritte nach einem unbefugten Zugriff die Daten nicht den betroffenen Personen zuordnen können.

Dem Verantwortlichen dient Pseudonymisierung zur Erfüllung der Verpflichtungen zum Datenschutz durch Technikgestaltung und zur Sicherheit der Verarbeitung.[320] Wirksame Pseudonymisierung kann zur Umsetzung der Datenschutzgrundsätze zur Datenminimierung, zum Schutz der Vertraulichkeit der Daten und zur Zweckbindung beitragen.[321] Der Verantwortliche kann die mit einer Pseudonymisierung erreichte Risikoreduktion bei der Abwägung seiner berechtigten Interes-

[319] Art. 4 Nr. 5 DSGVO.
[320] Siehe Art. 25 und Art. 32 DSGVO.
[321] Siehe Art. 5 Abs. 1 lit. b, c, f DSGVO.

sen mit den Interessen der betroffenen Personen berücksichtigen; auch bei der Entscheidung über die Vereinbarkeit des Zweckes einer Weiterverarbeitung mit den ursprünglichen Zwecken, zu denen die Daten erhoben wurden. Schließlich kann eine wirksame Pseudonymisierung dazu beitragen, ein im Wesentlichen äquivalentes Schutzniveau für Daten zu garantieren, die er zu exportieren beabsichtigt.

Pseudonymisierung wird grundsätzlich dadurch durchgeführt, dass direkt identifizierende Angaben wie der Name einer Person aus personenbezogenen Daten entfernt und durch ein Pseudonym ersetzt werden. Dieser Prozess wird so gestaltet, dass er die Kenntnis von Zusatzinformationen voraussetzt, die der Verantwortliche besonders gegen unbefugte Kenntnisnahme und Nutzung schützt. Das werden i. d. R. Tabellen aus Namen und zugeordneten Pseudonymen sein oder kryptografische Schlüssel. Es kann notwendig sein – in Abhängigkeit davon, wer an der Zuordnung der pseudonymisierten Daten zu Betroffenen gehindert werden soll und über welche Informationen diese Personen voraussichtlich verfügen – über die direkt identifizierenden hinaus auch weitere (z. B. demografische) Angaben zu modifizieren. Dies muss geschehen, wenn deren gemeinsame Betrachtung eine Zuordnung zu den Betroffenen – möglicherweise im Wege einer Zusammenführung mit anderen personenbezogenen Daten – erlaubt. Im Verlauf der Verarbeitung pseudonymisierter Daten muss der Verantwortliche dann durch technische und organisatorische Maßnahmen dafür Sorge tragen, dass Zusatzinformationen – die eine Zuordnung der pseudonymisierten Daten zu den Betroffenen erlauben – nicht denjenigen zur Kenntnis gelangen bzw. von ihnen genutzt werden können, die an der Zuordnung gehindert werden sollen. Unter den dabei zu berücksichtigenden Zusatzinformationen sind zuvorderst diejenigen, die der Verantwortliche selbst im Zuge der Änderung der Daten angelegt hat. Es gehören aber auch alle weiteren Informationen dazu, deren Zusammenführung mit den pseudonymisierten Daten eine Zuordnung zur betroffenen Person ermöglicht.

Die Leitlinien enthalten ferner Hinweise zur Zusammenführung verschiedener pseudonymisierter Datenbestände und zur Gewährung der Betroffenenrechte in Bezug auf pseudonymisierte Daten.

Pseudonymisierung ist eine flexible technische und organisatorische Maßnahme, mit der Risiken für die betroffenen Personen effektiv gemindert werden können. Abseits eines spezifischen gesetzlichen Mandats kann der Verantwortliche die Wirkung der Pseudonymisierung gezielt steuern. Sie kann zum Datenschutz durch

Technikgestaltung und datenschutzfreundliche Voreinstellungen sowie zur Sicherheit der Verarbeitung beitragen und dem Verantwortlichen u. U. eine Verarbeitung nach einer Rechtsgrundlage eröffnen, die bei direkt identifizierenden Daten nicht möglich wäre. Eine Effektivität der Pseudonymisierung setzt ihre sorgfältige Umsetzung voraus. Dies betrifft insbesondere die Umgestaltung der personenbezogenen Daten und den Schutz von solchen Zusatzinformationen vor unbefugter Nutzung oder Kenntnisnahme, die eine Zuordnung der pseudonymisierten Daten zu den betroffenen Daten ermöglichen. Pseudonymisierte Daten, die unter Nutzung derartiger Zusatzinformationen Betroffenen zugeordnet werden können, bleiben personenbezogene Daten, sodass bei ihrer Verarbeitung die Vorgaben des Datenschutzrechts einzuhalten sind.

b) Durch Anonymisierung werden personenbezogene Daten so umgewandelt, dass eine Identifizierung der betroffenen Personen dauerhaft ausgeschlossen wird. Wenn die Zwecke einer Datenverarbeitung mit anonymen Daten erreicht werden können, dann sollten die Verantwortlichen die Verarbeitung auf anonyme Daten beschränken. Damit stellt sich die Frage, wie Daten zuverlässig anonymisiert werden können und wann gesichert davon ausgegangen werden kann, dass der Personenbezug von Daten entfernt wurde.

Die durch uns und die französische Aufsichtsbehörde koordinierte Expertengruppe für Technologischen Datenschutz des EDSA hat durch den Ausschuss den Auftrag erhalten, Leitlinien zur Anonymisierung auszuarbeiten. Wir sind die Hauptberichterstatterin für dieses Projekt.

Rechtlich gesehen ist die Grenze zwischen personenbezogenen und anonymen Daten scharf gezogen. Personenbezogene Daten dürfen nur nach den Vorgaben des Datenschutzrechts verarbeitet werden. Anonyme Daten hingegen unterliegen keinerlei Beschränkungen durch das Datenschutzrecht. Ihre Verarbeitung muss nicht gerechtfertigt werden. Es gibt keinerlei Verpflichtung zur datenschutzrechtlichen Transparenz. Auch ihre Vertraulichkeit muss insoweit nicht gesichert werden. Sie können aus Datenschutzsicht ohne Weiteres publiziert werden.

In einem konkreten Fall ist es jedoch nicht immer einfach zu entscheiden, ob Daten anonym sind. Dies trifft jedenfalls dann zu, wenn sich auch nach Hinzuziehung weiterer verfügbarer Informationen aus den Daten keine Aussagen ableiten lassen, die etwas über eine identifizierbare Person verraten und folglich die Möglichkeit geben, diese von anderen Personen in einem

gegebenen Kontext zu unterscheiden und anders zu behandeln. Sowohl für die Hinzuziehung weiterer Informationen, die Ableitung der Aussagen als auch die Identifizierung der betroffenen Person sind nur solche Mittel zu berücksichtigen, die der Verantwortliche oder eine andere Person nach allgemeinem Ermessen wahrscheinlich aufwenden würde. Die Fähigkeiten und Kenntnisse anderer Personen sind insoweit von Belang, als sie die in Frage stehenden Daten erlangen und die Identifizierung in ihren Händen vollziehen können oder wenn sie hierzu in einem nach allgemeinem Ermessen vorhersehbaren Prozess beitragen können.

So hat der Europäische Gerichtshof (EuGH) in einem richtungsweisenden Urteil entschieden, dass IP-Adressen, die zusammen mit Angaben über die Nutzung eines digitalen Diensts (des Webangebots einer Behörde zum Beispiel) durch den Anbieter dieses Diensts gespeichert werden, als personenbezogen einzuordnen sind: Sie werden ja im Fall des Verdachts eines Cyberangriffs, also eines unbefugten missbräuchlichen Zugriffs auf den Dienst, an die zuständige Strafverfolgungsbehörde übergeben und können von dieser mit Angaben über die Person zusammengeführt werden können, der die IP-Adresse zugeordnet wurde.[322] Die Angaben über die Zuordnung zwischen Person und IP-Adresse erlangt die Behörde hierbei in einem durch Gesetz geregelten Prozess von dem zuständigen Internetzugangsanbieter.

Es gibt grundsätzlich zwei Wege für eine Anonymisierung von Daten: Zum einen kann die Struktur der Ausgangsdaten beibehalten, die Daten können aber so verändert werden, dass eine Wiederherstellung der Ausgangsdaten, eine Verknüpfung mit anderen, personenbezogenen Daten und die Ableitung von Angaben über einzelne identifizierbare Personen nicht möglich ist. Zum anderen können die Ausgangsdaten für eine oder mehrere Gruppen von Personen so zusammengefasst (aggregiert) werden, dass Schlussfolgerungen über einzelne Personen nicht gezogen werden können.

Die wissenschaftliche Forschung[323] hat gezeigt, dass es eine Herausforderung darstellt, den ersten Weg ausgehend von den konkret in der Praxis zur Verfügung stehenden Daten zuverlässig zu begehen. Zum einen stellt der technische und wissenschaftliche Fortschritt leistungsstarke Reidentifizierungsmethoden zur Verfügung, die ohne oder mit vergleichsweise wenig zusätzlichen Informationen über die betroffenen Personen

[322]EuGH, Urteil vom 19. Oktober 2016, C-582/14.
[323]Gadotti/Rocher/Houssiau/Creţu/Montjoye, Anonymization: The imperfect science of using data while preserving privacy, Science Advances 10(29), Juli 2024.

auskommen. Zum anderen hat sich der Umfang der öffentlich zugänglichen Informationen über Einzelpersonen dramatisch vergrößert. Eine Anonymisierung von Daten bei Beibehaltung der Struktur der Ausgangsdaten setzt also voraus, dass die Wahrscheinlichkeit eines Erfolgs verfügbarer Reidentifizierungsmethoden unter Berücksichtigung der Informationen eingeschätzt wird, die nach allgemeinem Ermessen wahrscheinlich hinzugezogen werden können, und zwar ggf. auch durch Dritte.

Für den zweiten Weg haben die vergangenen Jahre dagegen neue Ansätze erbracht, die auch im Licht neuerer wissenschaftlicher Erkenntnisse zur Reidentifizierbarkeit von Daten Potenzial aufweisen, diese auszuschließen. Die Leitlinien legen daher voraussichtlich den Schwerpunkt ihrer Darstellung auf diese Methoden. Diese beginnen bei der klassischen einmaligen Zusammenfassung oder statistischen Auswertung von personenbezogenen Daten. Diese kann auch flexibler ausgestaltet werden, indem – jeweils das Vorliegen der hierfür notwendigen Rechtsgrundlagen vorausgesetzt – mehrfach Auswertungen eines personenbezogenen Datenbestands so vorgenommen werden, dass auch eine Zusammenführung der Auswertungsergebnisse keine Schlussfolgerungen über Einzelpersonen ermöglicht.

Schließlich können die Auswertungsergebnisse auch moderne Formen annehmen. Dazu zählen synthetische Daten, also Bestände von Einzeldatensätzen, die jeweils Einzelcharakteristika von mehreren Personen aufnehmen – ggf. in abgewandelter Form –, sodass sich kein Datensatz einer einzelnen Person zuordnen lässt, die statistischen Eigenschaften der Datengesamtheit aber erhalten bleiben. Und es zählen dazu Modelle Künstlicher Intelligenz, die – auf ausreichender Rechtsgrundlage – mit personenbezogenen Daten so trainiert wurden, dass mit keinerlei Abfrage des Modells Aussagen über identifizierbare Einzelpersonen abgeleitet werden können. Dies erfordert Sorgfalt bei der Auswahl der Trainingsmethoden und der für die Trainings verwendeten Daten sowie bei der Ausführung des Trainings, kann dafür jedoch besonders nutzbringende Ergebnisse herbeiführen.

Mit dem Abschluss der Arbeiten an den Leitlinien und deren Veröffentlichung ist im Jahr 2025 zu rechnen.

Anonymisierung bietet die Chance, ehemals personenbezogene Daten in veränderter Form frei und außerhalb der Anforderungen des Datenschutzrechts zu verarbeiten, ohne dass dadurch Risiken für die betroffenen Personen entstehen. Bei vielen Anonymisierungsmethoden verbleiben jedoch Restrisiken, die u. U. schwierig

einzuschätzen sind. Halten sie sich bei Berücksichtigung der vernünftigerweise durch den Verantwortlichen oder eine andere Person eingesetzten Mittel in vernachlässigbarem Rahmen, so kann das Ergebnis als anonym akzeptiert werden. Als vorzugswürdige Mittel bieten sich Verfahren zur (ggf. dynamischen) Aggregation von personenbezogenen Daten mit anonymem Ergebnis an, deren Anwendung jedoch wie jeder Anonymisierungsprozess auf einer ausreichenden Rechtsgrundlage erfolgen muss.

2. Klares Signal zu Consent-or-Pay-Modellen – Datenschutz nicht nur gegen Entgelt

Sog. Consent-or-Pay-Modelle[324] wurden ab 2019 zunächst auf Websites von großen Medienhäusern eingeführt. Im November übernahmen auch große Social-Media-Plattformen diesen neuartigen Ansatz. Inzwischen gibt es kaum noch größere Medienpräsenzen, die nicht auf das Modell setzen.

Im letzten Jahr führten viele Websites sog. Consent-or-Pay-Cookiebanner ein, bei denen sich Nutzer:innen für den Zutritt zur vollständigen Website entweder für ein zahlungspflichtiges Abonnement oder die Zustimmung zu personalisierter Werbung entscheiden mussten. Bei den Datenschutzaufsichtsbehörden regten sich schnell ernste Zweifel an diesem binären Consent-or-Pay-Modell. Zumal der EuGH im Bundeskartellamt-Urteil festgestellt hat, dass Nutzer:innen, die die Einwilligung zu bestimmten Verarbeitungsvorgängen verweigern, „gegebenenfalls gegen ein angemessenes Entgelt, eine gleichwertige Alternative“ anzubieten ist, „die nicht mit solchen Datenverarbeitungsvorgängen einhergeht“.[325]

Auf Anträge der Aufsichtsbehörden in den Niederlanden, Norwegen und Deutschland (Hamburg), in denen sie das Gremium dazu aufforderten, eine Stellungnahme abzugeben,[326] äußerte sich der EDSA zu der Gültigkeit von Einwilligungen zur Verarbeitung personenbezogener Daten zum Zwecke der verhaltensbezogenen Werbung im Rahmen von Consent-or-Pay-Modellen.[327] Die Stellungnahme, an der wir mitgearbeitet haben, beschränkt sich dabei auf große Onlineplattformen.

Der EDSA betont in seiner Stellungnahme, dass nicht nur sämtliche Anforderungen der DSGVO an eine

[324] Auch „Zustimmung oder Bezahlung“- oder „Pay or Okay“-Modelle genannt.
[325] EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 150.
[326] Siehe Art. 64 Abs. 2 DSGVO.
[327] EDSA, Stellungnahme 08/2024 zur Wirksamkeit von Einwilligungen im Kontext von „Consent or Pay“-Modellen großer Onlineplattformen, abrufbar unter https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_de.pdf.

wirksame Einwilligung erfüllt werden müssen. Von besonderer Bedeutung sei der Grundsatz der Rechenschaftspflicht[328]. Der EDSA weist auch darauf hin, dass die Einholung der Einwilligung die Verantwortlichen nicht davon entbindet, alle in Art. 5 Abs. 1 DSGVO genannten Datengrundsätze, wie die Grundsätze der Zweckbindung, der Datenminimierung und von Treu und Glauben, einzuhalten sowie die anderen Verpflichtungen der DSGVO zu erfüllen. Einer rein „binären Wahl“ erteilte der EDSA eine Absage. Denn in den meisten Fällen werde es diesen nicht möglich sein, die Anforderungen an eine wirksame Einwilligung zu erfüllen, wenn sie Nutzer:innen nur vor die Wahl stellen, entweder in die Verarbeitung personenbezogener Daten für Zwecke der verhaltensorientierten Werbung einzuwilligen oder ein Entgelt zu zahlen.

Klarheit schafft die Stellungnahme auch hinsichtlich der Frage, welche Handlungsalternativen Verantwortliche haben. Entscheidend ist das Vorhandensein einer weiteren, unentgeltlichen Alternative, die ohne verhaltensorientierte Werbung auskommt, z. B. in Form von Werbung, bei der weniger (oder keine) personenbezogene Daten verarbeitet werden.

Um Nachteile zu vermeiden, die eine freiwillig erteilte Einwilligung ausschließen würden, müssen Verantwortliche überdies darauf achten, dass ein etwaiges Entgelt nicht so beschaffen ist, die betroffenen Personen wegen dessen Höhe effektiv daran zu hindern, eine freie Wahl zu treffen. Darüber hinaus können Nachteile auch daraus entstehen, dass die betroffenen Personen, die nicht einwilligen und kein Entgelt zahlen, faktisch von dem Dienst ausgeschlossen werden. Dies gilt insbesondere in Fällen, in denen der Dienst für die Teilhabe am gesellschaftlichen Leben oder den Zugang zu beruflichen Netzwerken eine herausragende oder entscheidende Rolle spielt, umso mehr, wenn Lock-in- oder Netzwerkeffekte bestehen. Bei großen Onlineplattformen, die ein Consent-or-Pay-Modell einsetzen, dürfte es wegen ihrer marktbeherrschenden Stellung sehr wahrscheinlich sein, dass solche Nachteile entstehen würden. Der EDSA betont aber auch, dass stets die Besonderheiten eines jeden einzelnen Falls zu bewerten sind.

Das Signal des EDSA ist deutlich: Personenbezogene Daten dürfen nicht als Handelsware betrachtet werden und es muss verhindert werden, dass Datenschutz als Grundrecht nur gegen Entgelt zugestanden wird. Verantwortliche sollten vielmehr von Fall zu Fall bewerten, ob einerseits ein Entgelt überhaupt angemessen ist

[328] Art. 5 Abs. 2 DSGVO.

und andererseits, welche Höhe unter den gegebenen Umständen angemessen ist. Dabei sind mögliche Alternativen zu verhaltensorientierter Werbung, die mit der Verarbeitung von weniger personenbezogenen Daten einhergehen, sowie die Position der betroffenen Personen zu berücksichtigen.

3. EDSA-Leitlinien und EuGH-Rechtsprechung zum berechtigten Interesse

Dieses Jahr hat der EDSA in seinen Expertengruppen unter unserer Beteiligung Leitlinien zur Verarbeitung personenbezogener Daten auf der Basis berechtigter Interessen nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO erarbeitet und beschlossen.[329] Auch der EuGH hat zu dieser Norm geurteilt. Art. 6 Abs. 1 Satz 1 lit. f DSGVO ist eine in der Praxis sehr wichtige Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Die Norm enthält eine Reihe auslegungsbedürftiger Begriffe. EDSA-Leitlinien und EuGH-Rechtsprechung geben nun konkrete Hilfestellungen zur Klärung der Rechtsfragen.

Art. 6 Abs. 1 Satz 1 lit. f DSGVO erlaubt Verantwortlichen die Verarbeitung personenbezogener Daten, wenn ein berechtigtes Interesse verfolgt wird, die Verarbeitung zur Wahrung dieses Interesses erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Auch wenn sämtliche Rechtfertigungsgründe aus Art. 6 Abs. 1 Satz 1 lit. b bis f DSGVO eng auszulegen sind,[330] ist der Begriff des berechtigten Interesses doch weit zu verstehen.[331] Letztlich muss das verfolgte Interesse nur rechtmäßig[332], tatsächlich vorhanden und nicht nur hypothetisch[333] sowie klar und präzise formuliert sein[334]. Um berücksichtigt werden zu können, muss das Interesse der betroffenen Person zum Zeitpunkt der Datenerhebung mitgeteilt werden.[335] Das berechtigte Interesse kann auch wirtschaftliche Interessen umfassen;[336] bei Unternehmen muss das Interesse auch mit der wirtschaftlichen Tätigkeit zu tun haben.[337]

---

[329]EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, abrufbar unter https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de.

[330]EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 31 m. w. N.; EuGH, Urteil vom 12. September 2024, C-17/22 und C-18/22, Rn. 37 m. w. N.

[331]EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 38; EuGH, Urteil vom 12. September 2024, C-17/22 und C-18/22, Rn. 50 m. w. N.; EDSA, Guidelines 1/2024, Rn. 16.

[332]EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 40; EDSA, ebd., Rn. 17.

[333]EuGH, Urteil vom 11. Dezember 2019, C-708/18, Rn. 44; EDSA, ebd., Rn. 17.

[334]EDSA, ebd., Rn. 17.

[335]EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 107, 126; EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 41 m. w. N.; Generalanwalt beim EuGH Szpunar, Schlussanträge vom 11. Juli 2024, C-394/23, Rn. 56.

[336]EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 48 f. m. w. N.

[337]EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 124; EDSA, Guidelines 1/2024, Rn. 19.

Die Datenverarbeitung muss zudem zur Verwirklichung des berechtigten Interesses erforderlich sein. Reine Nützlichkeit genügt nicht,[338] sondern die Verarbeitung muss „zur Verwirklichung dieses berechtigten Interesses unbedingt notwendig“[339], „absolut notwendig“[340] bzw. „objektiv unerlässlich“[341] sein. Die Erforderlichkeit der Datenverarbeitung ist nach der Rechtsprechung des EuGH gemeinsam mit dem Grundsatz der Datenminimierung[342] zu prüfen.[343] Dies bedeutet, dass bereits im Rahmen der Prüfung der Erforderlichkeit eine Interessenabwägung erfolgen muss,[344] was sich am Tatbestandsmerkmal „angemessen“ aus dem Grundsatz der Datenminimierung festmachen lässt. Dabei ist insbesondere zu prüfen, ob Umfang, Intensität, Dauer usw. der Datenverarbeitung „in einem angemessenen Verhältnis zu dem verfolgten Zweck stehen“[345] bzw. im Verhältnis zu diesem Zweck „nicht übermäßig“ sind,[346] was eine Abwägung der einander gegenüberstehenden Rechte und Interessen unter Berücksichtigung des konkreten Zwecks erfordert.[347] Dies bedeutet, dass eine Verarbeitung personenbezogener Daten zwar im Hinblick auf Zwecke und verfolgte berechtigte Interessen unbedingt notwendig und objektiv unerlässlich, dennoch aber als nicht erforderlich anzusehen sein kann, wenn diese Verarbeitung im Hinblick auf den Zweck nicht angemessen ist.

Zu beachten ist, dass der EuGH es als gleich geeignetes, aber milderes Mittel bewertet, wenn die Möglichkeit besteht, die betroffenen Personen im Voraus zu fragen, ob sie die Verarbeitung ihrer Daten möchten.[348] Er bewertet es auch sonst sehr streng, ob mildere Mittel bestehen.[349] Eine gleiche Eignung alternativer Mittel und damit fehlende Erforderlichkeit der Datenverarbeitung setzt nach der Rechtsprechung des EuGH mithin

[338]EuGH, ebd., Rn. 99; EDSA, ebd., Rn. 28.
[339]EuGH, Urteil vom 7. Dezember 2023, C-26/22 und C-64/22, Rn. 88; EDSA, ebd., Rn. 29.
[340]EuGH, Urteil vom 12. September 2024, C-17/22 und C-18/22, Rn. 76.
[341]EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 98.
[342]Art. 5 Abs. 1 lit. c DSGVO.
[343]EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 43 m. w. N.; EuGH, Urteil vom 12. September 2024, C-17/22 und C-18/22, Rn. 52 m. w. N.
[344]EuGH, Urteil vom 7. Dezember 2023, C-26/22 und C-64/22, Rn. 92; EDSA, Guidelines 1/2024, Rn. 12.
[345]EuGH, Urteil vom 5. April 2022, C-140/20, Rn. 93.
[346]EuGH, Urteil vom 30. Januar 2024, C-118/22, Rn. 41.
[347]EuGH, Urteil vom 7. Dezember 2023, C-26/22 und C-64/22, Rn. 92; ähnlich ohne ausdrückliche Bezugnahme auf Art. 5 Abs. 1 DSGVO auch EuGH, Urteil vom 7. März 2024, C-740/22, Rn. 53; EuGH, Urteil vom 22. Juni 2021, C-439/19, Rn. 106.
[348]EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 51 ff., dort bejaht hinsichtlich der entgeltlichen Weitergabe personenbezogener Daten zu Direktwerbezwecken.
[349]So etwa auch in EuGH, Urteil vom 12. September 2024, C-17/22 und C-18/22, Rn. 59 ff.; EuGH, Urteil vom 4. Oktober 2024, C-200/23, Rn. 113.

grundsätzlich nicht voraus, dass diese Mittel denselben Effekt haben.

Für die Abwägung, ob die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, enthalten die EDSA-Leitlinien eine detaillierte Anleitung.[350] Dabei spielen auch die vernünftigen Erwartungen der betroffenen Personen eine besondere Bedeutung.[351] Hierbei kommt es auf den Zeitpunkt der Erhebung der Daten an.[352] Nur dass eine Datenverarbeitung weithin üblich ist, macht diese nicht im rechtlichen Sinne vernünftigerweise erwartbar.[353] Die bloße Erfüllung der Informationspflichten aus Art. 12 bis 14 DSGVO reicht nicht aus, dass die betroffenen Personen vernünftigerweise eine bestimmte Verarbeitung erwarten können.[354] Fehlende oder fehlerhafte Informationen können aber ebenso dazu führen, dass eine Verarbeitung nicht vernünftigerweise erwartbar ist[355] wie der Verarbeitung entgegenstehende vertragliche Regelungen.[356] Von besonderer Bedeutung ist für den EuGH auch das Bestehen einer „maßgebliche[n] und angemessene[n] Beziehung zwischen den betroffenen Personen und dem Verantwortlichen“.[357]

Bei der Anwendung von Art. 6 Abs. 1 Satz 1 lit. f DSGVO sind die neuen klärenden Vorgaben des EuGH und des EDSA in der Praxis zu berücksichtigen: Auf der ersten Stufe der Rechtsprüfung sind die verfolgten berechtigten Interessen präzise festzulegen und den betroffenen Personen mitzuteilen, damit sie berücksichtigt werden können. Auf der zweiten Stufe der Rechtsprüfung muss die Datenverarbeitung auf das absolut Notwendige beschränkt bleiben; alle geeigneten und milderen Alternativen schließen die Erforderlichkeit und damit die Zulässigkeit der Datenverarbeitung aus. Dabei sind an die Eignung der Alternativen keine zu hohen Anforderungen zu stellen. Auf der dritten Stufe, der Interessenabwägung, sind die vernünftigen Erwartungen der betroffenen Personen von besonderer Bedeutung. Insbesondere sind nicht alle branchenüblichen Verarbeitungen rechtlich erwartbar.

[350] EDSA, Guidelines 1/2024, Rn. 31 ff.
[351] Siehe Erwägungsgrund (ErwGr.) 47 Satz 1 DSGVO.
[352] EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 55; EuGH, Urteil vom 12. September 2024, C-17/22 und C-18/22, Rn. 64.
[353] EDSA, Guidelines 1/2024, Rn. 52; siehe auch EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 117.
[354] EDSA, ebd., Rn. 53.
[355] Ebd.
[356] EuGH, Urteil vom 12. September 2024, C-17/22 und C-18/22, Rn. 64.
[357] EuGH, Urteil vom 4. Oktober 2024, C-621/22, Rn. 56.

4. Stellungnahme des EDSA zu Künstlicher Intelligenz

Am Jahresende nahm der EDSA auf Antrag der irischen Datenschutzaufsichtsbehörde eine Stellungnahme zu Künstlicher Intelligenz (KI)[358] an. Unsere Behörde wirkte, insbesondere über die von uns gemeinsam mit der französischen Datenschutzaufsichtsbehörde koordinierte Technology Expert Subgroup, zusammen mit dem Sekretariat des EDSA und anderen deutschen und europäischen Datenschutzaufsichtsbehörden an der Erarbeitung von Antworten auf die aufgeworfenen Fragen mit.

Der Antrag der irischen Aufsichtsbehörde umfasste vier Fragen. Im ersten Teil ging es um das Bestehen des Personenbezugs bei KI-Modellen, die mit personenbezogenen Daten trainiert worden sind, und um die Fragen, unter welchen Bedingungen solche Modelle anonym sind und wie Anonymität nachgewiesen werden kann.

Wenn man personenbezogene Daten mit Verfahren – von denen man nach allgemeinem Ermessen ausgehen kann, dass sie wahrscheinlich angewendet werden – weder auf direktem Wege noch durch geeignete Anfragen aus dem Modell gewinnen kann, dann ist das Modell anonym. Die verfügbaren Methoden wiederum können nach dem Stand der Technik und den vorliegenden wissenschaftlichen Erkenntnissen beurteilt werden. Sie unterliegen ständiger Weiterentwicklung. Daher sind stets sorgfältige Untersuchungen erforderlich, um das Bestehen oder die Abwesenheit des Personenbezugs festzustellen.

Möchte ein Verantwortlicher nachweisen, dass ein von ihm mit personenbezogenen Daten trainiertes Modell anonym ist, dann kommt es in erster Linie darauf an, ob und wie er Techniken im Rahmen des Trainings angewendet hat, die die Privatheit der Personen schützen, auf die sich die Trainingsdaten beziehen. Die Wissenschaft hat Kriterien für die Wirksamkeit dieser Techniken entwickelt, von denen Differential Privacy derzeit als die am besten durchgreifende Methode erscheint. Vereinfacht gesagt erfüllt eine Trainingsmethode das Kriterium, wenn kein signifikanter Unterschied festgestellt werden kann zwischen einem Modell, das mit dem vollen Satz an Trainingsdaten trainiert wurde, und

[358] EDSA, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64-opinion-282024-certain-data-protection-aspects_de.

jedwedem Modell, bei dessen Training auf Daten zu genau einer Person verzichtet wurde.

Ein Verantwortlicher vereinfacht sich diesen Nachweis, wenn er das Training auf die Aufnahme allgemein geltender Sachverhalte orientiert und eine Anpassung des Modells an ungewöhnliche Einzeldaten verhindert. Natürlich hilft es auch, so wenig personenbezogene Daten wie möglich zu verwenden. Dazu können diese so weit wie möglich im Vorhinein anonymisiert oder zumindest pseudonymisiert werden, nur essenzielle personenbezogene Daten in das Trainingsdatenset übernommen und ungeeignete Quellen ausgespart werden.

Darüber hinaus wollte die irische Aufsichtsbehörde wissen, welche Erwägungen für die Verarbeitung Verantwortliche berücksichtigen sollten, wenn die Verarbeitung personenbezogener Daten zur Erstellung, Aktualisierung und Weiterentwicklung von KI-Modellen auf Art. 6 Abs. 1 Satz 1 lit. f DSGVO als Rechtsgrundlage gestützt wird; und zwar in Bezug auf die Verarbeitung von Daten, die sowohl über Dritte als auch bei den betroffenen Personen direkt erhoben werden. Neben der Frage zur Interessenabwägung selbst war zudem zu beantworten, wie Verantwortliche, die sich auf berechtigte Interessen als Rechtsgrundlage berufen, nachwe isen können, dass das berechtigte Interesse eine ang emessene Rechtsgrundlage für die fragliche Datenverarbeitung ist.

Mit Verweis auf die neuen EDSA-Leitlinien zu Art. 6 Abs. 1 Satz 1 lit. f DSGVO[359] stellt der EDSA zur Beantwortung zunächst klar, dass bei der Interessenabwägung stets die besonderen Umstände des Einzelfalls zu berücksichtigen sind. Mit anderen Worten: Unterschiedliche Szenarien können zu unterschiedlichen Ergebnissen führen. Die Verarbeitung personenbezogener Daten, die bei der Entwicklung und dem Einsatz von KI-Modellen stattfindet, kann sich auf unterschiedliche Weise auf die betroffenen Personen auswirken. Wesentliche Faktoren sind die Art der durch die Modelle verarbeiteten Daten (z. B. die Verarbeitung besonderer Kategorien personenbezogener Daten oder sensitiver Daten wie Finanz- oder Standortdaten), der Kontext der Verarbeitung und weitere Folgen, die die Datenverarbeitung für die Betroffenen haben kann.

In Bezug auf den Kontext der Verarbeitung spielen die Art des Modells und die beabsichtigten Verwendungszwecke eine Schlüsselrolle bei der Identifizierung po-

[359] EDSA, Guidelines 1/2024.

tenzieller Folgen und Risiken für die betroffenen Personen (z. B. die Art und Weise, wie das Modell entwickelt wurde, die Art und Weise, wie das Modell eingesetzt werden kann und/oder ob die Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten angemessen sind). In die Waagschale gehören neben möglichen Nachteilen aber auch mögliche Vorteile der Datennutzung für die betroffenen Personen.

Bei der Interessenabwägung sind Schwere und Wahrscheinlichkeit des Eintretens dieser Folgen und Risiken zu berücksichtigen. In Bezug auf die Schwere sind Faktoren wie der Umfang der Verarbeitung und die Menge der verarbeiteten Daten (z. B. die Gesamtmenge der Daten, die Menge der Daten pro betroffener Person, die Anzahl der betroffenen Personen) sowie bspw. auch die Art der betroffenen Person (z. B. wenn die betroffenen Personen Kinder oder andere schutzbedürftige Personen sind) und ihre Beziehung zum Verantwortlichen (z. B. wenn die betroffene Person ein:e Kund:in ist) zu berücksichtigen. Bei der Wahrscheinlichkeit des Eintretens der Folgen und Risiken spielen dem EDSA zufolge insbesondere Maßnahmen zur Verhinderung eines möglichen Missbrauchs des KI-Modells eine Rolle (z. B. seine Verwendung für schädliche Praktiken, etwa die Erstellung von Deepfakes; Chatbots, die zur Desinformation eingesetzt werden; Phishing und andere Arten von Betrug; manipulative KI).

Eine Schlüsselrolle bei der Abwägungsprüfung nehmen die vernünftigen Erwartungen der betroffenen Personen ein; nicht zuletzt aufgrund der Komplexität der Technologie, die in KI-Modellen verwendet wird, und der Tatsache, dass es für die betroffenen Personen schwierig sein kann, die Vielfalt der möglichen Verwendungen eines KI-Modells und die damit verbundene Datenverarbeitung zu verstehen. Hierbei können Datenschutzinformationen in Datenschutzerklärungen, die den betroffenen Personen zur Verfügung gestellt werden, eine Informationsgrundlage schaffen. Allerdings reicht die bloße Erfüllung der Transparenzanforderungen der DSGVO allein nicht aus, um davon ausgehen zu können, dass die betroffenen Personen vernünftigerweise eine bestimmte Verarbeitung ihrer Daten erwarten. Fehlen solche Informationen aber ganz, wird i. d. R. davon auszugehen sein, dass betroffene Personen die betreffende Datenverarbeitung vernünftigerweise nicht erwarten.

Darüber hinaus können die berechtigten Erwartungen auch davon abhängen, ob die betroffenen Personen die Daten dem Verantwortlichen direkt zur Verfügung gestellt haben (z. B. im Zusammenhang mit der Nutzung

des Diensts) oder ob der für die Verarbeitung Verantwortliche die Daten von einer anderen Quelle erhalten hat. Beispielhaft erwähnt der EDSA die Nutzung von Daten, die der Verantwortliche über einen Dritten oder durch Web Scraping erlangt hat. Personen müssen laut EDSA nicht grundsätzlich damit rechnen und es auch nicht generell akzeptieren, dass alle über sie im Internet verfügbaren Daten zum Training von KI frei eingesetzt werden.

Besonders Web Scraping birgt Risiken, die mittels spezifischer Maßnahmen abgemildert werden müssen. Dazu zählen Maßnahmen, die sicherstellen, dass bestimmte Datenkategorien nicht erhoben werden oder dass bestimmte Quellen von der Datenerhebung ausgeschlossen werden. Das ist z. B. der Ausschluss von Websites (oder Teilen von Websites), die sich eindeutig gegen Web Scraping und die Wiederverwendung ihrer Inhalte für den Aufbau von KI-Trainingsdatenbanken aussprechen (z. B. durch die Einhaltung von robots.txt- oder ai.txt-Dateien oder andere anerkannte Mechanismen zum Ausschluss von automatischem Crawling oder Scraping).

All diese besonderen Umstände sind von den für die Verarbeitung Verantwortlichen sorgfältig zu prüfen und zu dokumentieren, um tatsächlich den Nachweis erbringen zu können, dass das berechtigte Interesse eine angemessene Rechtsgrundlage für die fragliche Datenverarbeitung darstellt.

Die letzte Frage des Antrags bezog sich auf die Folgen eines ggf. rechtswidrigen Trainings für den späteren Einsatz eines KI-Modells. Im Rahmen der Frage wurde auf KI-Modelle Bezug genommen, die entweder allein oder als Teil eines KI-Systems eingesetzt werden. Es wurden drei Szenarien entwickelt, wobei sich die ersten beiden auf ein KI-Modell beziehen, das personenbezogene Daten verarbeitet. Das letzte Szenario zielt hingegen auf ein anonymisiertes Modell ab. Vereinfacht zusammengefasst kann hier zunächst festgehalten werden, dass es auf den Einzelfall ankommt. Ein rechtswidriges Training kann sich grundsätzlich auf die datenschutzrechtliche Rechtmäßigkeit des Modelleinsatzes auswirken. Soweit ein KI-Modell genutzt wird, was nicht selbst trainiert wurde, hat bspw. ein Verantwortlicher zu berücksichtigen, ob eine Aufsichtsbehörde das ursprüngliche Training des KI-Modells als Verstoß gegen die DSGVO gewertet hat. Sollte jedoch nachgewiesen werden, dass ein KI-Modell trotz eines rechtswidrigen Trainings anonymisiert wurde, fehlt es beim Einsatz des Modells an der Verarbeitung von den im Modell enthaltenen personenbezogenen Daten.

Die europäisch abgestimmte Stellungnahme steckt einen Rahmen für Verantwortliche und die zukünftige Tätigkeit der Datenschutzaufsichtsbehörden im Bereich Künstlicher Intelligenz. Es hat sich gezeigt, dass ein Personenbezug durch das Training von KI-Modellen mit personenbezogenen Daten entstehen kann, wenn keine zielgerichteten und effektiven Maßnahmen ergriffen werden, um das zu verhindern. Auch wurde festgestellt, dass berechtigte Interessen im Zusammenhang mit der Verarbeitung personenbezogener Daten etwa zum Training eines KI-Modells durchaus herangezogen werden können. Bei der durchzuführenden Interessenabwägung sind dann alle spezifischen Umstände des Einzelfalls zu berücksichtigen, sodass im Hinblick auf das berechtigte Interesse als Rechtsgrundlage unterschiedliche Szenarien zu unterschiedlichen Bewertungen führen können. Die Rechte und Freiheiten der betroffenen Personen können einer Verarbeitung im Zusammenhang mit KI-Modellen im Einzelfall entgegenstehen. Dies ist insbesondere dann der Fall, wenn die Verwendung der personenbezogenen Daten zu KI-Zwecken für die betroffenen Personen nicht vorhersehbar war oder wenn die Verarbeitung vor dem Hintergrund möglicher Folgen und Risiken insgesamt als nicht angemessen erscheint. Des Weiteren kann auch ein rechtswidriges Training eines KI-Modells Folgen für dessen späteren Einsatz haben.

5. Erstes deutsches Zertifizierungsprogramm für Verantwortliche

Dem Landesbeauftragten für Datenschutz und Informationsfreiheit Bremen (LDI Bremen) liegt das erste deutsche Datenschutzzertifizierungsprogramm für verantwortliche Stellen zur Genehmigung vor. Die Genehmigung soll aufgrund der Stellungnahme 26/2024 des EDSA[360] erfolgen, an der wir zunächst als Co-Reviewerin und dann als Berichterstatterin intensiv mitgewirkt haben.

Akkreditierte Zertifizierungsstellen können die Datenschutzkonformität von Verarbeitungen mit einem Zertifikat bestätigen.[361] Ein solches Zertifikat vereinfacht Menschen die Auswahl datenschutzkonformer Anbieter:innen am Markt und sorgt für eine bessere Orientierung. Grundlage hierfür ist neben der Akkreditierung als Zertifizierungsstelle auch ein genehmigtes Zertifizierungsprogramm, das die bei der Zertifizierung anzuwendenden Kriterien und Prüfmethoden festlegt. Die

[360]EDSA, Opinion 26/2024 on the draft decision of the DE Bremen Supervisory Authority regarding the „Catalogue of Criteria for the Certification of IT-supported processing of Personal Data pursuant to art 42 GDPR (GDPR – information privacy standard)“ presented by datenschutz cert GmbH, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-262024-draft-decision-de-bremen_de.

[361]Art. 42 und Art. 43 DSGVO.

Genehmigung solcher Kriterien ist nur mit einer Stellungnahme des EDSA möglich. Die in Bremen ansässige datenschutz cert GmbH hat dem LDI Bremen ein generisches Zertifizierungsprogramm für Verantwortliche und Auftragsverarbeiter zur Genehmigung vorgelegt. In dem mehrjährigen Genehmigungsverfahren war unsere Behörde zunächst als Co-Reviewerin und dann als Berichterstatterin für die Stellungnahme des EDSA beteiligt.

Gemeinsam mit der österreichischen Aufsichtsbehörde haben wir als Berichterstatterin die Rückmeldungen anderer europäischer Aufsichtsbehörden in Form von Empfehlungen in die Stellungnahme des EDSA aufgenommen, sodass z. B. das Kriterium für die Implementierung technischer und organisatorischer Maßnahmen um Maßnahmen ergänzt wurde, die zusätzlich im Auftragsverarbeitungsvertrag festgelegt sind.

Nachdem bereits Anfang 2024 die in Nordrhein-Westfalen ansässige Zertifizierungsstelle EuroPrise GmbH für die Zertifizierung von Auftragsdatenverarbeitung akkreditiert worden war, kann nun voraussichtlich mit der datenschutz cert GmbH die erste deutsche Datenschutzzertifizierungsstelle für verantwortliche Stellen akkreditiert werden. Die datenschutz cert GmbH hat zusätzlich auch eine Akkreditierung für das Zertifizierungsprogramm „Auditor“ für Cloudanbieter:innen beantragt, das im Juni 2024 durch die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) genehmigt wurde. Nach einer mehrjährigen Zusammenarbeit der deutschen und europäischen Aufsichtsbehörden stehen Auftragsverarbeitern und verantwortlichen Stellen in Deutschland nun verschiedene Möglichkeiten offen, ihre Verarbeitungen als datenschutzkonform zertifizieren zu lassen.

Datenschutzzertifizierungen durch unabhängige, akkreditierte Stellen bestätigen die Datenschutzkonformität der zertifizierten Verarbeitung und erleichtern Betroffenen die Orientierung. Mit einer zweiten Zertifizierungsstelle in Deutschland werden nach der Genehmigung auch Verantwortliche die Möglichkeit haben, ihre Datenverarbeitungen zertifizieren zu lassen. Wir haben an der verpflichtenden Stellungnahme des EDSA zur Genehmigung des Zertifizierungsprogramms mitgewirkt.

6. Entscheidung des EDSA zu Zugriffen auf Smartphones

Der EDSA hat nach öffentlicher Konsultation die endgültige Fassung von Leitlinien zum Schutz von Informationen in Smartphones und anderen persönlichen

Endgeräten verabschiedet.[362] Die Erarbeitung erfolgte in der von uns koordinierten Technology Expert Subgroup des EDSA.

Die europäische ePrivacy-Richtlinie schreibt vor, dass Anbieter von digitalen Diensten ohne Einwilligung der betroffenen Person weder Daten in einem Smartphone oder anderen Endgerät speichern, noch auf gespeicherte Daten zugreifen dürfen.[363] Es gelten Ausnahmen für Vorgänge, die zum Erbringen eines Kommunikationsdiensts oder eines anderen durch die nutzende Person angeforderten Diensts notwendig sind. Deutschland hat die europäische Vorgabe in § 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) umgesetzt.

Cookies sind die am weitesten verbreitete Form von Daten, die in Endgeräten gespeichert werden und auf die im weiteren Verlauf zugegriffen wird, wenn die nutzenden Personen mit einem Browser oder einer mobilen Anwendung Inhalte (Websites, Musik, Videos etc.) aus dem Internet abrufen. In den vorliegenden Leitlinien stellt der EDSA dar, auf welche anderen Methoden der Speicherung oder des Zugriffs auf gespeicherte Daten die Regelung ebenfalls anzuwenden ist.

Die Auslegung der Norm orientiert sich an der Intention des Gesetzgebers, die Privatsphäre der betroffenen Personen umfassend zu schützen und insbesondere das Nachverfolgen der Netzaktivitäten einer Person nur mit deren Einwilligung zu gestatten. Seit Hersteller:innen von Browsern die Möglichkeit anbieten, die Speicherung von Cookies zu begrenzen, oder gar den dienstübergreifenden Zugriff auf Cookies in der Standardeinstellung unterbinden, werden immer neue Methoden entwickelt, auf anderem Wege die Nachverfolgung von nutzenden Personen über Websites, über einen langen Zeitraum und ggf. auch über verschiedene von Personen genutzte Endgeräte hinweg zu ermöglichen. Jedwede Information, die auf einem Endgerät gespeichert oder auf die zugegriffen wird, kann für diese Nachverfolgung eingesetzt werden. Auch scheinbar inhaltsleere Zeichenketten können zur Verknüpfung verschiedener Informationen über nutzende Personen verwendet werden. Dementsprechend richten sich die Anforderungen

[362]EDSA, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, Version 2.0, abrufbar unter https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf.

[363]Art. 5 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ePrivacy-Richtlinie). Die gesetzliche Vorgabe erstreckt sich gleichermaßen auch auf den Schutz von Informationen, die sich auf juristische Personen beziehen. Dem Schwerpunkt unserer Tätigkeit folgend fokussiert der Berichtspunkt den Schutz natürlicher Personen.

von Art. 5 Abs. 3 ePrivacy-Richtlinie auf die Speicherung von bzw. den Zugriff auf jegliche Art von Informationen ganz unabhängig von der Aussagekraft, die sie allein betrachtet besitzen.

Die Leitlinien des EDSA stellen weiter klar, dass alle Speicherungen von Daten auf einem Endgerät in den Anwendungsbereich der Norm fallen, auch wenn diese nur kurzfristig erfolgen. Selbstverständlich ist die Speicherung von Seiteninhalten und Medien im Endgerät ein normaler Prozess des Zugriffs auf digitale Dienste. Auch wenn sich die Leitlinien dem nicht näher widmen, ist unstreitig, dass eine solche Speicherung zur Anzeige einer durch die nutzende Person abgerufenen Website notwendig sein kann. Sie unterliegt dann aufgrund der o. g. Ausnahmen für Vorgänge, die zum Erbringen eines Kommunikationsdiensts oder eines anderen durch die nutzende Person angeforderten Diensts notwendig sind, nicht dem Einwilligungsgebot. Vielfach werden jedoch durch die Diensteanbieter:innen zusätzliche Informationen auf dem Endgerät gespeichert, die für die nutzende Person keine Bedeutung haben, sondern der Analyse des Nutzungsverhaltens oder dem Aufbau von Nutzungsprofilen dienen. Diese liegen im Anwendungsbereich von Art. 5 Abs. 3 ePrivacy-Richtlinie. Dabei ist es unerheblich, ob die Speicherung über das Netz erfolgt oder die Daten auf einem anderen Wege, z. B. über eine Installation von Software, auf das Endgerät gelangen, solange das Endgerät selbst mit einem Kommunikationsnetz verbunden ist. In diesem Fall müssen vor der Speicherung eine Einwilligung eingeholt und Methoden zum Widerruf der Einwilligung bereitgestellt werden, deren Anwendung zur Löschung der vormals gespeicherten Daten führen.

Auch bei Zugriffen auf gespeicherte Daten ist ein umfassender Blick nötig, da viele der abgerufenen Daten eine Wiedererkennung der Person oder eine Zuordnung zu einem Nutzungsprofil ermöglichen. Es kommt nicht darauf an, ob die Daten vorher durch den Dienst auf dem Endgerät gespeichert wurden oder aus anderen Gründen dort gespeichert sind (wie z. B. Angaben über die auf dem Endgerät zum Einsatz kommende Software oder über technische Eigenschaften des Endgeräts). Ebenso ist von einem Zugriff auch dann auszugehen, wenn der Dienst, der die Übermittlung der Daten durch das Endgerät auslöst, ein anderer ist als der, der die Daten empfängt.

Die deutschen Aufsichtsbehörden hatten bereits vor Veröffentlichung der europäischen Leitlinien eine eigene Orientierungshilfe für Anbieter:innen von digitalen Diensten herausgegeben, die den Leitlinien weitgehend vorgegriffen hatte und nunmehr auf ihrer Basis

fortgeschrieben wurde.[364] Die Vorgaben des EDSA werden dafür sorgen, dass die europäischen Aufsichtsbehörden einheitliche Maßstäbe bei der Anwendung von Art. 5 Abs. 3 ePrivacy-Richtlinie ansetzen.

Die Durchsetzung der gesetzlichen Vorgaben zum Schutz von natürlichen Personen bei der Interaktion mit digitalen Diensten bedarf eines koordinierten Vorgehens der europäischen Datenschutzaufsichtsbehörden, um negativen Auswirkungen der derzeitigen Praxis der Onlinewerbeindustrie zu begegnen. Wir werden uns weiter dafür einsetzen, dass die Nutzung von digitalen Diensten nur soweit verfolgt wird, wie es gesetzlich erlaubt ist oder die Betroffenen informiert ihr Einverständnis gegeben haben.

II. Internationale -Zusammenarbeit

1. Bericht von der Internationalen Konferenz der Informationsfreiheitsbeauftragten

Unter dem Motto „Befähigung des Einzelnen durch Zugang zu Informationen: Gewährleistung von Transparenz und Integration in einer vernetzten Welt“[365] fand vom 3. bis 5. Juni dieses Jahres die 15. Internationale Konferenz der Informationsfreiheitsbeauftragten (I-CIC) in Tirana statt. An der Konferenz beteiligte sich auch unsere Behörde mit einem Debattenbeitrag zu proaktiven Maßnahmen für Transparenz und Informationsfreiheit by Design.

Im Schwerpunkt ging es in den Paneldiskussionen und Vorträgen während der Konferenz um Möglichkeiten, den Zugang zu öffentlichen Informationen und die Ausübung anderer Menschenrechte für Menschen in prekären Situationen bzw. für vulnerable Gruppen zu verbessern. Themen der Konferenz waren darüber hinaus: die Herausforderungen von Journalist:innen, an Regierungsinformationen zu gelangen, sowie die Auswirkungen auf Informationszugangsrechte durch geopolitische Spannungen, Desinformation, Zensur, Überwachung und durch die Unterdrückung abweichender Meinungen.

In einer Diskussionsrunde zur proaktiven Transparenz durch digitale Werkzeuge und Initiativen für offene Daten erörterten wir u. a. den Stand der proaktiven Transparenzmaßnahmen in Deutschland, die Rolle von Datenschutz und IT-Sicherheit bei der Fort-entwick-

[364]DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten, Version 1.2, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf; siehe B.II.7.
[365]Englischer Originaltitel: Empowering Individuals through Access to Information: Ensuring Transparency and Inclusivity in an Interconnected World.

lung von Open-Data-Initiativen und mögliche Maßnahmen zur Implementierung von Informationsfreiheit by Design in der Digitalen Akte. Technische Beispiele für solche Maßnahmen sind Werkzeuge, die eine umfassende Suche nach Informationen im Besitz einer öffentlichen Stelle ermöglichen, die helfen, Informationen zu identifizieren, die geschwärzt werden müssen (z. B. personenbezogene Daten), oder die die Durchführung von Schwärzungen erleichtern. In diesem Zusammenhang wiesen wir in unserem Beitrag auch auf die Möglichkeiten der Nutzung von Künstlicher Intelligenz (KI) bei der Informationsbereitstellung hin.[366] Hierbei müssen die Ergebnisse überprüft und der Einsatz von KI transparent gehandhabt werden.

Die Themen und Diskussionsrunden der ICIC machen deutlich, dass dem Zugang zu Informationen als fundamentalem Menschenrecht international ein sehr hoher Stellenwert zukommt, um Transparenz, Rechenschaftspflicht und rechtsstaatliche wie demokratische Regierungsführung in Gesellschaften zu fördern und zu fordern. Auch in Ländern, in denen Zugangsrechte und Transparenzvorgaben bereits etabliert sind, muss sich das Verständnis durchsetzen, dass die Bereitstellung von Informationen eine eigene öffentliche Aufgabe darstellt. Hierbei helfen Ansätze, die die Informationsfreiheit bereits bei der Implementierung neuer technischer Systeme mitberücksichtigen, um damit den Aufwand der Informationsbereitstellung zu reduzieren.

2. 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 der Bundesbeauftragten 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 17. bis 19. Juni dieses Jahres in Oslo statt. Dabei wurden Arbeitspapiere, sog. Working Papers, zur Datenweitergabe und zu großen Sprachmodellen verabschiedet. Außerdem wurden Arbeitspapiere zur Neurotechnologie und zur erweiterten Realität diskutiert.

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

Das Arbeitspapier zur Datenweitergabe beschreibt die Praktiken und die damit verbundenen Risiken bei der Weitergabe von Daten zwischen Organisationen für ihre weitere Verarbeitung.[367] Eine Datenweitergabe kann erhebliche wirtschaftliche Vorteile für die Gesellschaft schaffen, indem sie Innovationen fördert, Entscheidungsfindung verbessert und Zusammenarbeit unterstützt. Gleichzeitig bringt sie ggf. erhebliche Risiken mit sich, wie mangelnde Transparenz für Betroffene und Einschränkungen anderer Rechte, die den Betroffenen durch das Datenschutzrecht eingeräumt werden. Ausgehend von diesen Risiken werden in dem Papier technische, organisatorische und rechtliche Maßnahmen diskutiert und konkrete Empfehlungen gegeben, wozu u. a. der „Privacy by Design"-Ansatz und Techniken wie Multi-Party Computation gehören.

Das Arbeitspapier zu großen Sprachmodellen (Large Language Models, LLMs) gibt eine detaillierte Beschreibung der dahinter liegenden Technologie und analysiert diese aus einer datenschutzrechtlichen Perspektive.[368] Risiken wie der Verlust von Betroffenenrechten, Bias und Informationsmanipulierung werden diskutiert und im Anschluss technische Ansätze zur Bewältigung dieser Risiken vorgestellt. Dazu gehören Ansätze wie Datenkuratierung, Differential Privacy und Machine Unlearning. Außerdem werden lokale große Sprachmodelle (Local LLMs) als ein alternativer Lösungsansatz hinsichtlich ihrer Vor- und Nachteile analysiert. Dies ist ein Ansatz, der vorsieht, dass große Sprachmodelle direkt auf den Geräten der betroffenen Personen gehostet und ausgeführt werden, um die Kontrolle über die verarbeiteten personenbezogenen Daten zu stärken.

Die zweite Sitzung der IWGDPT fand vom 18. bis 19. November in Brüssel statt. Das Arbeitspapier zu Neurotechnologien wurde verabschiedet und es wurden weitere Arbeitspapiere zur erweiterten Realität, zu Opt-out-Präferenzsignalen und zum Confidential Cloud Computing diskutiert.

Das Arbeitspapier zu Neurotechnologien beschäftigt sich mit den Auswirkungen der Erhebung und Verarbeitung von Neurodaten auf das Recht auf Privatsphäre und Datenschutz.[369] Es analysiert verschiedene Formen der Neurotechnologien und bettet deren Nutzung im globalen rechtlichen Kontext ein. Die Frage nach der

[367]IWGDPT, Working Paper on Data Sharing vom 6. Dezember 2024, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Berlin-Group/20241206-WP-Data-Sharing.html.
[368]IWGDPT, Working Paper on Large Language Models (LLMs) vom 6. Dezember 2024, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Berlin-Group/20241206-WP-LLMs.html.
[369]IWGDPT, Working Paper on Neurotechnologies, abrufbar unter https://www.bfdi.bund.de/DE/Fachthemen/Gremienarbeit/Berlin-Group/Berlin-Group-node.html.

rechtlichen Grundlage einer Verarbeitung von Neurodaten, insbesondere nach der Eignung von Einwilligungen und den Herausforderungen, die damit einhergehen, werden detailliert dargestellt. Außerdem wird die Anwendung der Neurotechnologien an Kindern und Jugendlichen analysiert und verschiedene Maßnahmen für Sicherheit und Datenschutz diskutiert, die Verantwortliche bei der Entwicklung der Technologien einsetzen können. Anschließend wendet sich das Papier an Regulierer:innen und Entwickler:innen und benennt konkrete Maßnahmen, die zu berücksichtigen sind.

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

D. Anhang

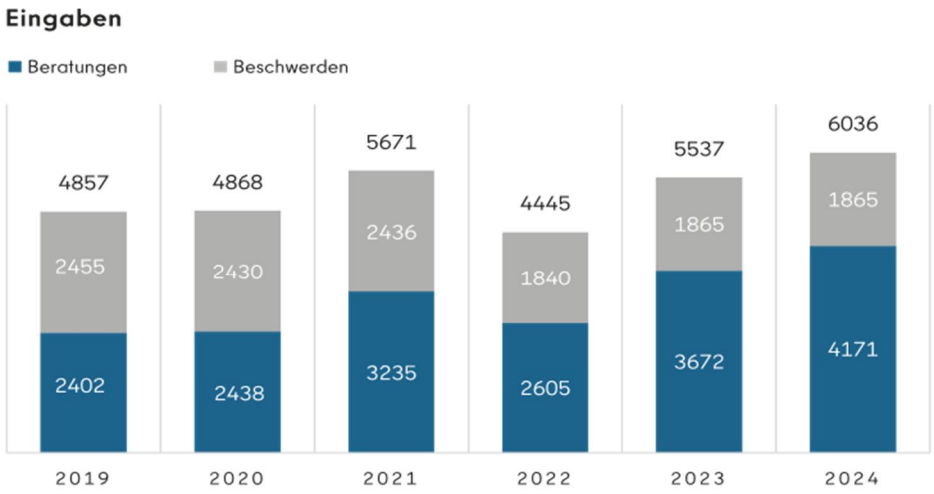
I. Statistik

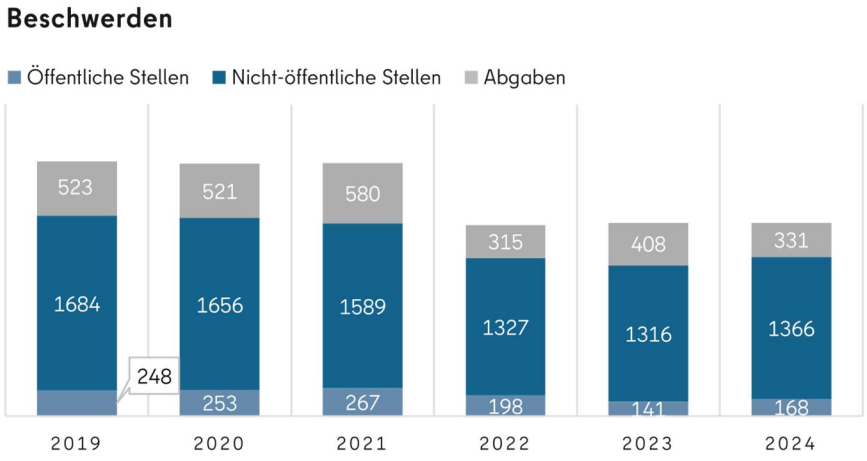
Im diesem Jahr verzeichnete die Behörde eine nach wie vor hohe Anzahl von -Eingaben durch die Bürger:innen, wobei erneut die schriftlichen Beratungen zugenommen haben. Die Zahl der gemeldeten Datenpannen verblieb auf dem hohen Niveau der Vorjahre. Die Darstellung des Kapitels orientiert sich an den einheitlichen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

1. Beratungsanfragen und Beschwerden

In diesem Jahr wurde mit 6.036 Eingaben von Bürger:innen der Höchststand seit Einführung der DSGVO erfasst. Wie bereits im Vorjahr nahmen insbesondere die schriftlichen Beratungen zu. Über das Jahr verteilt wandten sich 4.171 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 brauchten. Dies bedeutet eine weitere Zunahme der Beratungsanfragen um knapp 14 Prozent im Vergleich zum Vorjahr, als bereits 3.672 Anfragen eingingen. Die an uns gerichteten persönlichen Beschwerden von Betroffenen blieben mit 1.865 auf hohem Niveau.

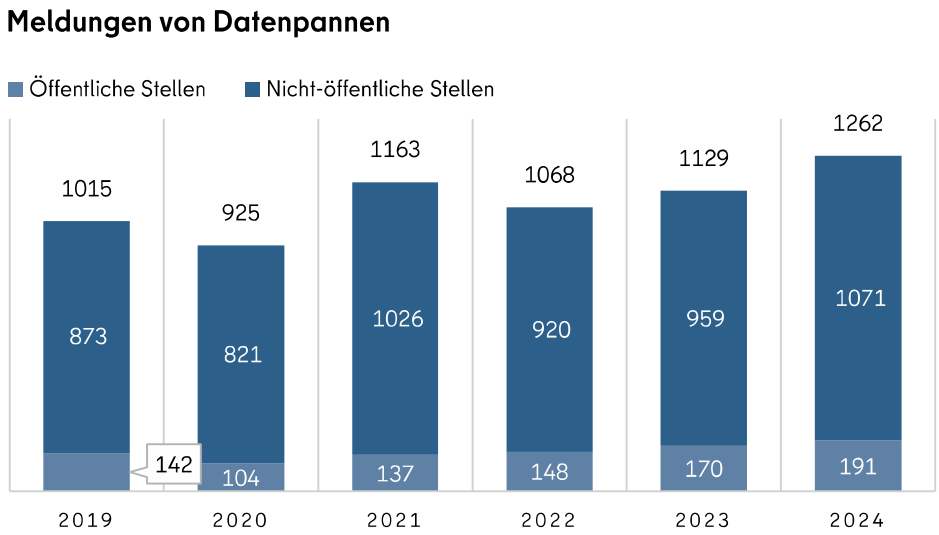
Für den Großteil der Beschwerden eröffneten wir Verfahren in eigener Zuständigkeit. Dies waren in diesem Jahr 1.534 Verfahren. Die meisten davon (1.366) richteten sich gegen private Stellen, die restlichen (168) betrafen Behörden und andere öffentliche Stellen. In 331 Fällen lagen die Beschwerden nicht in unserem Zuständigkeitsbereich, weshalb wir sie an die jeweils zuständigen Aufsichtsbehörden abgegeben haben.


Eingaben
Beratungen
Beschwerden
4857
2455
2402
4868
2430
2438
5671
2436
3235
4445
1840
2605
5537
1865
3672
6036
1865
4171
2019
2020
2021
2022
2023
2024


Beschwerden
Öffentliche Stellen
Nicht-öffentliche Stellen
Abgaben
523
1684
248
521
1656
253
580
1589
267
315
1327
198
408
1316
141
331
1366
168
2019
2020
2021
2022
2023
2024

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 erneut an. Während im Jahr 2023 insgesamt 1.129 Meldungen erfasst wurden, erhöhte sich diese Zahl in diesem Jahr auf 1.262. Die Aufschlüsselung der Zahlen zeigt, dass öffentliche Stellen im diesem Jahr 191 Datenpannen meldeten (Vorjahr: 170). Ebenso stieg die Anzahl der Meldungen von nicht-öffentlichen Stellen von 959 im Jahr 2023 auf 1.071 in diesem Jahr.

3. Anträge und Beschwerden nach dem Informationsfreiheitsgesetz

Während im Jahr 2023 noch 44 Anträge auf Aktenauskunft bzw. Akteneinsicht bei uns eingingen, erhielten wir dieses Jahr insgesamt 69 Anträge auf Aktenauskunft bzw. Akteneinsicht. Dies bedeutet einen Anstieg um fast 57 Prozent. Die Antragsgegenstände betrafen u. a. Informationen zu Datenpannen, Datenschutzbeschwerden und Prüfverfahren.

Wir erhielten 99 Beschwerden, in denen wir von Bürger:innen auf der Grundlage des Informationsfreiheitsgesetz (IFG) um Vermittlung gegenüber angefragten Stellen gebeten wurden, weil eine vermutete bzw. unzureichend erteilte Aktenauskunft oder -einsicht im Raum stand. Die Zahl lag damit niedriger als im Jahr 2023 (111 Fälle), aber höher als im Jahr 2022 (85 Fälle). Die Beschwerden betrafen u. a. acht der elf Senatsverwaltungen, alle zwölf Bezirke sowie nachgeordnete Einrichtungen wie die Polizei, das Landesverwaltungsamt und das Landesamt für Flüchtlingsangelegenheiten.

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 11 Verfahren als federführende Aufsichtsbehörde bestimmt. Eine Betroffenheit ergab sich

in 448 Fällen. In 36 Verfahren erließen wir einen Beschlussentwurf oder einen endgültigen Beschluss.

Europäische Verfahren mit unserer Beteiligung 2024

Verfahren nach Art. 56 DSGVO (betroffen)	448
Verfahren nach Art. 56 DSGVO (federführend)	11
Verfahren nach Art. 60 ff. DSGVO (federführend)	36

5. Abhilfemaßnahmen

Stellen wir einen Verstoß von Verantwortlichen gegen die DSGVO fest, können wir verschiedene Abhilfemaßnahmen ergreifen.[370] Dementsprechend haben wir in diesem Jahr Folgendes veranlasst: Wir haben 104 Verwarnungen ausgesprochen. Wir haben 25 Bußgeldbescheide mit 164 Bußgeldern in Höhe von insgesamt 80.190 Euro erlassen. Die entsprechenden Verfahren waren bis Ende des Jahres jedoch noch nicht alle rechtskräftig abgeschlossen. Zudem sind 18 Zwangsgeldbescheide ergangen. In vier Fällen haben wir einen Strafantrag gestellt. Über das Jahr verteilt wurden 79 Bußgeldverfahren eingestellt und 108 Verfahren neu eröffnet.

Abhilfemaßnahmen 2024

Warnungen	0
Verwarnungen	104
Anweisungen und Anordnungen	0
Geldbußen	164

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

II. Abkürzungen

Abghs.-Drs.	Abgeordnetenhausdrucksache
Abs.	Absatz
AG	Amtsgericht
AGG	Allgemeines Gleichstellungsgesetz
Alt.	Alternative
APPF	Behörde für europäische politische Parteien und europäische politische Stiftungen
Art.	Artikel
ASOG	Allgemeines Sicherheits- und Ordnungsgesetz Berlin
AsylbLG	Asylbewerberleistungsgesetz
ATDG	Antiterrordateigesetz
AufenthG	Aufenthaltsgesetz
AZR	Ausländerzentralregister
BDSG	Bundesdatenschutzgesetz
BEG	Bürokratieentlastungsgesetz
BeherbMeldV	Beherbungsmeldedatenverordnung
BerlHG	Berliner Hochschulgesetz
BESD	Bevölkerungsstatistischer Datenbestand
betr.	Betreffend, betreffs
BfDI	Bundesbeauftragte:r für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGebG	Bundesgebührengesetz
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BlnDSG	Berliner Datenschutzgesetz
BMG	Bundesmeldegesetz
BMGVwV	Allgemeine Verwaltungsvorschrift zur Durchführung des Bundesmeldegesetzes
BMI	Bundesministerium des Innern und für Heimat
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bspw.	Beispielsweise
BT-Drs.	Bundestags-Drucksache
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVG	Berliner Verkehrsbetriebe
BWB	Berliner Wasserbetriebe
bzw.	beziehungsweise
CSD	Christopher Street Day
d.h.	das heißt
DigiG	Digitalgesetz
DigLLV	Digitale Lehr- und Lernmittelverordnung
DMK	Digitalministerkonferenz
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz)

DÜV-AnpassG	Gesetz zur Anpassung von Datenübermittlungsvorschriften im Ausländer- und Sozialrecht
ebd.	Ebenda
EDSA	Europäischer Datenschutzausschuss
EfA-Modell	„Einer für alle“-Modell
EGovG Bln	E-Government-Gesetz Berlin
EHDS	Europäischer Gesundheitsraum
eIDKG	eID-Karte-Gesetz
ErwGr.	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FAQ	häufig gestellte Fragen
GDNG	Gesetz zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz)
GebBtrG BE	Gesetz über Gebühren und Beiträge Berlin (Geodatenzugangsgesetz Berlin)
ggf.	gegebenenfalls
GGO I	Gemeinsame Geschäftsordnung der Berliner Verwaltung – Allgemeiner Teil
GVBl.	Gesetz- und Verordnungsblatt
Hybrid CoE	Europäisches Kompetenzzentrum für die Bekämpfung hybrider Bedrohungen
i.d.R.	In der Regel
ICIC	Internationale Konferenz der Informationsfreiheitsbeauftragten
IFG	Berliner Informationsfreiheitsgesetz
IFG Bund	Informationsfreiheitsgesetz des Bundes
IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
IKT	Informations- und Kommunikationstechnologie
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)
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
KG	Kammergericht
KhsVO	Krankenhaus-Verordnung
KI	Künstliche Intelligenz
KIS	Krankenhausinformationssystem
KI-VO	Verordnung zu Künstlicher Intelligenz
KKG	Gesetz zur Kooperation und Information im Kinderschutz
LG	Landgericht
lit.	littera (Buchstabe)
LLMs	Large Language Models (Sprachmodelle)
LUSD	Lehrkräfte-Unterrichts-Schul-Datenbank
OH	Orientierungshilfe
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz

OZG	Onlinezugangsgesetz
OZGÄndG	Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz)
POLIKS	Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung
RegModG	Registermodernisierungsgesetz
RegZensG-E	Entwurf eines Gesetzes zur Einführung eines Registerzensus
Rn.	Randnummer
SBGG	Gesetz über die Selbstbestimmung in Bezug auf den Geschlechtereintrag
SchuldatenV	Schuldatenverordnung
SchulG	Berliner Schulgesetz
SDM	Standard-Datenschutzmodell
SDÜ	Schengener Durchführungsübereinkommen
SenASGIVA	Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung
SenBJF	Senatsverwaltung für Bildung, Jugend und Familie
SenFin	Senatsverwaltung für Finanzen
SenInnSport	Senatsverwaltung für Inneres und Sport
sog.	sogenannt
StBA	Statistisches Bundesamt
StPO	Strafprozessordnung
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TTPW-VO	Verordnung über die Transparenz und das Targeting politischer Werbung
u.a.	unter anderem
u.U.	unter Umständen
UWG	Gesetz über den unlauteren Wettbewerb
VG	Verwaltungsgericht
VSG	Verfassungsschutzgesetz Berlin
VwGO	Verwaltungsgerichtsordnung
VwVfG Bln	Gesetz über das Verfahren der Berliner Verwaltung
z.B.	zum Beispiel