Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Datenschutz und Informationsfreiheit

Jahresbericht 2025

Jahresbericht

der Berliner Beauftragten für Datenschutz und Informationsfreiheit

zum 31. Dezember 2025

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat nach § 12 Berliner Datenschutzgesetz und § 18 Abs. 4 Berliner Informationsfreiheitsgesetz dem Abgeordnetenhaus und dem Senat von Berlin jährlich einen Bericht über das Ergebnis ihrer Tätigkeit vorzulegen. Der vorliegende Bericht schließt an den Jahresbericht 2024 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2025 ab.

Der Jahresbericht ist auch über unsere Website abrufbar:
www.datenschutz-berlin.de

Impressum

Herausgeberin:	Berliner Beauftragte für Datenschutz und Informationsfreiheit Alt-Moabit 59-61 10555 Berlin Tel.: 030 138 89 0 Fax: 030 215 50 50 mailbox@datenschutz-berlin.de www.datenschutz-berlin.de
Umschlag:	april agentur GmbH
Satz:	werk & satz.
Druck:	Druckhaus Sportflieger GmbH

Inhalt

C. Wir in Deutschland

D. Wir in Europa und der Welt

E. Anhang

Vorwort

Ein intensives und arbeitsreiches Jahr als Vorsitz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) liegt hinter uns. In dieser Zeit haben wir die Gestaltungsmöglichkeiten des Vorsitzes genutzt, viele spannende und aktuelle Themen aus der ersten Reihe heraus behandelt und im Kreise der Datenschutzbehörden koordiniert sowie den Kontakt zu jeder einzelnen Datenschutzbehörde deutlich intensiviert. Ein großer Dank geht an meine Mitarbeiter:innen, die mit großer Motivation und Energie ein erfolgreiches Berliner Vorsitzjahr ermöglicht haben.

Die Europäische Kommission hat zum Ende dieses Jahres Änderungsvorschläge u. a. zur Datenschutz-Grundverordnung (DSGVO) im Rahmen eines sog. Digital-Omnibus-Gesetzgebungsverfahrens mit dem Ziel veröffentlicht, die DSGVO zu simplifizieren und Reibungspunkte zwischen den EU-Digitalgesetzen zu glätten, zugleich aber den Schutzstandard zu erhalten. Es geht insbesondere um den Abbau von Bürokratie und die Entlastung kleiner und mittelständischer Unternehmen.

Diese Diskussionen sind nicht neu: Mit der Einführung der DSGVO erlangte das Thema Datenschutz in Unternehmen und Verwaltungen europaweit erhöhte Aufmerksamkeit. Es entstand einerseits der positive Effekt, dass viele Organisationen ein besonderes Augenmerk auf die Umsetzung von Datenschutzanforderungen in ihren betrieblichen und dienstlichen Abläufen legten. Andererseits konnte mit Datenschutzberatung plötzlich viel Geld verdient werden, so dass Ängste vor vorgeblich hohen Hürden zur Umsetzung der DSGVO-Anforderungen geschürt und Dinge verkompliziert wurden, die eigentlich nicht kompliziert sind. Im Ergebnis konzentrierten sich viele Organisationen auf eine vermeintliche DSGVO-Konformität, indem Dokumentationen und Konzepte zum Selbstzweck erstellt wurden, ohne den Sinn der Übung auch als Korrektiv für

Aufwand und Zielrichtung von Maßnahmen im Blick zu behalten. Dass dies als unnötige Bürokratie wahrgenommen wird, ist nachvollziehbar. Dabei geht leider unter, was die DSGVO eigentlich vorsieht: Es geht in erster Linie darum, tatsächlich zu prüfen, ob eine geplante oder bestehende Verarbeitung personenbezogener Daten rechtskonform ist, daraufhin die Prozesse ggf. anzupassen und technisch-organisatorisch mit Verarbeitungsrisiken umzugehen. Hieran führt auch in Zukunft kein Weg vorbei, wenn der Schutzstandard der DSGVO erhalten bleiben soll.

Um kleine und mittelständische Unternehmen, die risikoarme Datenverarbeitungen durchführen, effektiv zu entlasten, braucht es standardisierte Prüfprozesse und konkrete Handlungsvorgaben. Die Aufsichtsbehörden haben sich hier schon seit längerer Zeit auf den Weg gemacht, konkretere Hilfestellungen zur Verfügung zu stellen. Zwar enthalten auch die Vorschläge der EU-Kommission im Digitalen Omnibus hierfür Ansätze – etwa zu Mustern für Datenschutz-Folgenabschätzungen und Meldungen von Datenschutzvorfällen –, andere vorgeschlagene Anpassungen wurden aber bisher leider nicht aufgegriffen: So appelliert die DSK, auch die Hersteller von IT-Produkten und -Diensten sowie Auftragsverarbeiter – insbesondere mit großer Marktdominanz – stärker in die Verantwortung zu nehmen. Hiervon würden insbesondere auch kleine und mittelständische Unternehmen profitieren, die häufig auf diese Produkte und Dienste in der alltäglichen Verarbeitung von personenbezogenen Daten angewiesen sind, ohne die Verhandlungsmacht zu besitzen, datenschutzkonforme Einstellungen in Verträgen und Diensten zu erwirken, bzw. ohne geeignete Informationen zu erhalten, um ihrer Rechenschaftspflicht nachzukommen.

Hohe Wellen schlägt der Vorschlag der EU-Kommission, die Definition des personenbezogenen Datums in der DSGVO anzupassen. Hier handelt es sich um einen schwergewichtigen Änderungsvorschlag, dessen Folgenabschätzung und Grundrechtswirkung einer vertieften Auseinandersetzung bedarf, die im Schnellverfahren einer Omnibusgesetzgebung nicht gewährleistet werden kann. Die Rechtsprechung des Europäischen Gerichtshofs (EuGH) wird dabei – anders als dargestellt – nicht kodifiziert, sondern ins Gegenteil verkehrt. Es bleibt abzuwarten, welche Änderungsvorschläge sich in den folgenden Trilogverhandlungen durchsetzen werden.

Anknüpfend an die Planungen, die Durchführung der EU-Digitalrechtsakte zentral auf Bundesebene zu organisieren, stehen in der nationalen Datenschutzdiskussion aktuell Überlegungen an, die Datenschutzaufsicht im Bereich der Wirtschaft beim Bund zu bündeln. Dabei wird immer wieder insbesondere von Seiten der datengetriebenen Wirtschaft eingebracht, dass es erhebliche Unterschiede zwischen den bislang zuständigen Landesbehörden in der Auslegung des Rechts gebe.

Natürlich kommt es auch in der Datenschutzaufsicht vor – so wie übrigens in jedem anderen Bereich der in der Regel föderal organisierten staatlichen Aufsicht –, dass unterschiedliche Behörden zu unterschiedlichen Ergebnissen kommen: Zum Teil liegen Behörden – und sei es in kleinen, aber wesentlichen Nuancen – unterschiedliche Sachverhalte vor, zum Teil kommt es zu unterschiedlichen Rechtsauslegungen. Das ist keine Besonderheit des Datenschutzrechts. Warum stehen die Datenschutzbehörden dann in einem solchen besonderen Fokus, so dass ausgerechnet im Datenschutzbereich vom verfassungsrechtlichen Grundsatz, dass die Länder die Gesetze ausführen, abgewichen werden soll? Die unabhängige Stellung der Datenschutzbehörden spielt in dieser Frage sicherlich eine nicht nur untergeordnete Rolle. Diese Stellung unterscheidet die Datenschutzaufsicht von anderen Aufsichtsbereichen und wird von mancher Seite mit Skepsis beäugt. Die Unabhängigkeit dient aber nicht dazu, dass sich die Datenschutzbehörden in der Auslegung des gemeinsamen Rechts voneinander abgrenzen. Vielmehr gilt sie im Verhältnis zu den zu kontrollierenden Stellen in Verwaltung und Wirtschaft. Nur als unabhängige Behörden können die Aufsichtsbehörden ihre wichtige Funktion für den Schutz der Grundrechte erfüllen und ihre Kontrollfunktion unbefangen und unparteiisch ausüben.

Hinzu kommt auch, dass nach wie vor viele ungeklärte Rechtsfragen im Datenschutzrecht u. a. im Bereich der großen IT-Diensteanbieter und digitalen Plattformen bestehen und Unsicherheiten begründen. Auch werden Rechtsverstöße im Sinne eines „Move fast and break things“ in Kauf genommen, um erst dann auf datenschutzkonforme Prozesse umzustellen, wenn entweder aufsichtsbehördliche Verfahren eingeleitet werden oder Gerichtsentscheidungen dazu zwingen. Diese Vorgehensweisen stehen im Widerspruch zu dem Ansatz der DSGVO, die auf Rechenschaftspflicht und proaktives

Datenschutzmanagement setzt, und führen zu langwierigen Verfahren der Rechtsklärungen. Die Zentralisierung der Datenschutzaufsicht ist hier keine Lösung: Die Datenschutzbehörden arbeiten stattdessen daran, ihre Prüfungen zu standardisieren, auch um transparent nachweisen zu können, dass überall die gleichen Maßstäbe angewandt werden. Zudem versuchen die Aufsichtsbehörden mit konkreten Anwendungshilfen, den Einsatz von absichernden und datenschutzfreundlichen Maßnahmen zu erleichtern. Ein Beispiel dafür ist etwa das von uns als Berliner Landesbehörde initiierte und in diesem Jahr unter unserem Vorsitz in die DSK eingebrachte Projekt, konkrete Anwendungshilfen zu erstellen, um Anwender:innen bei der Durchführung von Anonymisierungs- und Pseudonymisierungsverfahren stärker zu unterstützen. Schließlich wird die Durchführung von Anonymisierungs- und Pseudonymisierungsverfahren und die Anwendung dieser Instrumente für die Wahrung von Datenschutzrechten in der Zukunft eine immer bedeutendere Rolle spielen. Zudem dienen diese Instrumente auch einer kohärenteren Anwendung der EU-Digitalrechtsakte an der Schnittstelle zur DSGVO.

Die Informationsfreiheit blieb in diesem Jahr ebenfalls nicht unangetastet. Im Vorfeld der Koalitionsverhandlungen im Bund wurden Forderungen nach der Abschaffung des Informationsfreiheitsgesetzes des Bundes laut. Auch in Berlin wurden Überlegungen angestellt, den Informationszugang in bestimmten Bereichen aus Gründen des Verwaltungsaufwands zu beschränken. Wir alle sollten jedoch ein Interesse daran haben, dass Transparenz und Informationszugang von der Verwaltung als ureigenste Aufgaben und nicht nur als Aufwand wahrgenommen werden, der anderen Aufgaben gegenzurechnen ist. Der Wert des Zugangs zu staatlichen Informationen für eine freie und partizipative Gesellschaft kann nicht hoch genug eingestuft werden. Eine neue Kultur der Geheimniskrämerei und eines falschen/vermeintlichen Besitzanspruchs stellt nicht nur einen gesellschaftlichen Rückschritt dar, sondern schadet auch der Wirtschaft, die auf die proaktive Veröffentlichung von Informationen durch Staat und Verwaltung zählt.

Auch der Einsatz von KI-Systemen und -Anwendungen spielte für unsere Arbeit in diesem Jahr eine große Rolle: Im Land Berlin haben wir dazu intensiv beraten und uns für eine spezifische Rechtsgrundlage eingesetzt. KI beschäftigte uns dabei nicht nur im Rahmen unserer aufsichtsbehördlichen Tätigkeit, sondern auch in Bezug auf den Einsatz in unserer eigenen Behörde. Wir verzeichneten in diesem Jahr einen rasanten Anstieg bei den Beschwerden, Hinweisen und Beratungsanfragen. Dadurch zeigt sich, dass Datenschutz und IT-Sicherheit bei der Einführung und Anwendung digitaler Instrumente einen hohen Stellenwert genießen. Es gilt daher, Unsicherheiten von vornherein zu vermeiden, Datenschutz und Informationsfreiheit von Anfang an mitzudenken und Risiken für betroffene Personen erfassbar und beherrschbar zu machen. In diesem Sinne werden wir uns weiterhin für Freiräume, Souveränität und Unabhängigkeit im digitalen Raum einsetzen.

Eine gute Lektüre des Jahresberichts 2025 wünscht

Meike Kamp
Berliner Beauftragte für Datenschutz und Informationsfreiheit

A.

Wir im Jahr 2025

I. Vorsitz der Datenschutzkonferenz

In diesem Jahr hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit den Vorsitz in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) geführt. Die DSK trägt entscheidend dazu bei, dass europäisches und nationales Datenschutzrecht einheitlich angewendet und fortentwickelt wird, erarbeitet Hilfestellungen für die das Datenschutzrecht anwendenden Stellen und setzt sich dafür ein, dass die Datenschutzgrundrechte gewahrt und geschützt werden. In diesem Zusammenhang erarbeitet und veröffentlicht sie regelmäßig Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Pressemitteilungen und weitere Stellungnahmen. Die DSK wird dabei durch Arbeitskreise (AK) in verschiedenen Fachbereichen unterstützt. Der jährlich wechselnde Vorsitz der DSK setzt für die Arbeit des Gremiums richtungsweisende Impulse, koordiniert die Zusammenarbeit und vertritt die DSK nach außen.

Ein Thema, das die Aufsichtsbehörden und somit auch die DSK in unserem gesamten Vorsitzjahr stark beschäftigt hat, war die Diskussion über eine Bündelung der Datenschutzaufsicht und der damit verbundenen Frage der innerdeutschen Zuständigkeit für die europäischen Digitalrechtsakte. Mit zahlreichen Stellungnahmen und im direkten Austausch mit den Entscheidungsträger:innen hat sich die DSK hierzu positioniert.

Im Rahmen ihrer ersten Zwischenkonferenz im Januar diskutierte die DSK den Einsatz von Systemen, die auf Künstlicher Intelligenz (KI) basieren, und gründete den AK Künstliche Intelligenz.[1] Damit trug sie der Entwicklung Rechnung, dass immer mehr Unternehmen und Behörden KI-Verfahren einsetzen und auch entwickeln. Da eine effektive Anonymisierung und Pseudonymisierung personenbezogener Daten gerade auch in Verbindung mit dem Training und der Nutzung von KI unerlässlich ist und die Digitalrechtsakte der EU in Abgrenzung zur Datenschutz-Grundverordnung (DSGVO) auf Anonymisierung und Pseudonymisierung setzen, hat die DSK auf Initiative Berlins

1 Siehe C.III.1.

zudem beschlossen, hierfür praktische Hilfestellungen für Unternehmen und Behörden zu erarbeiten.[2]

Bei der 109. DSK im März haben die Aufsichtsbehörden unter unserem Vorsitz in ihrem Eckpunktepapier für eine freiheitliche und grundrechtsorientierte digitale Zukunft Forderungen an die neue Bundesregierung formuliert. Kern des Papiers ist die Botschaft, dass eine weitere Digitalisierung und verstärkte Datennutzung nur unter Achtung der Grundrechte gelingen kann. Darüber hinaus hat die DSK insbesondere dazu aufgerufen, wichtige, bereits begonnene, aber momentan zum Teil ruhende Gesetzgebungsvorhaben wieder aufzugreifen: Es muss Rechtssicherheit für diejenigen, die in Wirtschaft und Verwaltung Verantwortung tragen, geschaffen und eine einheitliche Anwendung des Datenschutzrechts in Deutschland gesichert werden. Für das Bundesdatenschutzgesetz (BDSG) forderte die DSK in diesem Zusammenhang ihre Institutionalisierung mit einer Geschäftsstelle.

Auf unsere Anregung hin hat sich die DSK zudem mit der Bundesnetzagentur auf eine für beide Seiten gewinnbringende Zusammenarbeit im Rahmen der Durchsetzung des Digital Services Act (DSA) verständigt. Dafür hat die DSK gemeinsam mit der Bundesnetzagentur einen Prozess für konkrete Einzelfälle im Zusammenhang mit dem DSA entwickelt und eine Schnittstelle eingerichtet, mit der ein regelmäßiger Austausch zu übergeordneten Themen mit Bezug zum DSA möglich ist.

Im Rahmen der zweiten Zwischenkonferenz im Juni hat die DSK zur aktuellen Diskussion über Innere Sicherheit klar Stellung bezogen: In einer Entschließung machte sie deutlich, dass ein starker Datenschutz in diesem Bereich kein Selbstzweck ist, sondern ein wesentliches und unerlässliches Element des Rechtsstaats.[3] Außerdem fasste die DSK in ihrer Sitzung Beschlüsse zum Einsatz von Dienstleistern für die Terminverwaltung in Arztpraxen[4] und zum Confidential Cloud Computing[5]. Informationen für Unternehmen und andere Organisationen hat die DSK ferner in einer Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb

2 Siehe C.I.
3 Siehe C.V.1.
4 Siehe C.VI.2.
5 Siehe C.VIII.1.

von KI-Systemen[6] gegeben und sich auf eine Musterrichtlinie für Bußgeldverfahren der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich[7] geeinigt.

In der dritten Zwischenkonferenz im September hat die DSK den datenschutzrechtlichen Rahmen für den Einsatz automatisierter Datenanalysen durch Polizeibehörden verdeutlicht.[8] Sie betonte in einer entsprechenden Entschließung, dass hierfür spezifische Rechtsgrundlagen geschaffen werden müssen und die Verfahren verfassungskonform ausgestaltet sein sowie die digitale Souveränität wahren müssen.

Im Herbst brachte die DSK auch die Orientierungshilfe zu Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken[9] auf den Weg. Sie zeigt den Forschenden auf, was diese bei der Übermittlung personenbezogener Daten an Partner:innen in Drittländern beachten müssen.

In der 110. DSK im Dezember – zum Abschluss unseres Vorsitzjahres – hat sich die DSK schließlich zu den Vorschlägen der EU-Kommission zur Anpassung der DSGVO, der KI-Verordnung und weiterer Digitalrechtsakte positioniert. Zudem hat sie eigene, darüber hinausgehende Vorschläge für gezielte Anpassungen der DSGVO bei der Plattform- und Herstellerhaftung sowie den Betroffenenrechten im KI-Bereich gemacht. Diese schlossen an ihre Vorschläge im November zur Verbesserung des gesetzlichen Datenschutzes von Kindern in der DSGVO an. Zudem hat die DSK einen neuen, standardisierten Prüfprozess[10] verabschiedet und damit eine gemeinsame Grundlage geschaffen, um den Datenschutz bei länderübergreifenden Onlinediensten von Behörden einheitlich und transparent umzusetzen.

Wir blicken damit auf ein sehr arbeits- und diskussionsreiches DSK-Vorsitzjahr mit vielen Beschlüssen und Anwendungshilfen zurück.

6 Siehe C.III.2.
7 Siehe C.II.1.
8 Siehe C.V.2.
9 Siehe C.VI.1.
10 Siehe C.IV.1.

II. Informationsfreiheit in Gefahr

Vertrauen in staatliches Verwaltungshandeln und dessen Nachvollziehbarkeit ist essenziell für das Funktionieren einer Demokratie. Mit Sorge beobachteten wir daher die Tendenzen in diesem Jahr, die Informationsfreiheit zu beschränken.

Im Anschluss an die Wahlen zum Deutschen Bundestag ist aus den Sondierungsgesprächen zur Bildung einer Regierungskoalition Folgendes bekannt geworden: Es wurde die Forderung aufgestellt, das Informationsfreiheitsgesetz des Bundes (IFG Bund) in der bisherigen Form abzuschaffen.[11] Es folgte eine breite öffentliche Kritik, auch in Form einer Petition, der sich über 430.000 Menschen anschlossen.[12] Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) kritisierte das Ansinnen ebenfalls[13] und brachte deutlich zum Ausdruck, dass in für die Demokratie herausfordernden Zeiten nicht weniger, sondern mehr Transparenz nötig und das Informationsfreiheitsgesetz des Bundes im demokratischen Teilhabeprozess nicht mehr wegzudenken ist. Die IFK wies zugleich darauf hin, dass das Bundesamt für Verfassungsschutz vor den von Desinformation ausgehenden Gefahren für die freiheitliche demokratische Grundordnung in Deutschland warnt. Bürgerinnen und Bürger haben durch ihr Recht auf Informationszugang – gerade in Zeiten der Verbreitung von Fake News und gezielter Desinformation – die Möglichkeit, sich umfassend selbst zu informieren. Auch für Journalistinnen und Journalisten ist dies ein wertvolles Instrument, um an Informationen zu gelangen.

Die Forderung zur Abschaffung des IFG des Bundes wurde zwar fallengelassen. Gleichwohl finden sich im Koalitionsvertrag[14] Aussagen zu diesem Gesetz und zum

11 Siehe https://fragdenstaat.de/dokumente/258024-koalitionsverhandlungen-cdu-csu-spd-ag-9-buerokratierueckbau-staatsmodernisierung-moderne-justiz/?page=4, Rn. 113 f.

12 Siehe https://www.campact.de/blog/2025/04/erfolg-angriff-auf-das-informationsfreiheitsgesetz-abgewehrt/.

13 Pressemitteilung vom 28. März 2025: „Abschaffung der Informationsfreiheit auf Bundesebene völlig falscher Weg!“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk/.

14 Siehe Zeilen 1894 ff. sowie Zeile 1355 des diesjährigen Koalitionsvertrags, abrufbar unter https://www.koalitionsvertrag2025.de.

Umweltinformationsgesetz (UIG), die auf einen Reformbedarf hinweisen, aber nicht konkretisieren, was darunter zu verstehen ist. Zum UIG heißt es etwa, dass das Gesetz verschlankt werden soll. Der gesetzgeberische Gestaltungsspielraum dürfte hier indes begrenzt sein, weil das UIG die Vorgaben der Europäischen Umweltinformationsrichtlinie[15] umsetzt. Zudem zeigen die Diskussionen um den weltweiten Klimaschutz, wie wichtig der Zugang zu Umweltinformationen ist.[16]

Auch in Berlin gibt es Bestrebungen, die Informationsfreiheit einzuschränken und die Ausnahmetatbestände zu erweitern. Geplant ist ein Gesetz, das umfangreiche Ausnahmen vom Recht auf Akteneinsicht und Aktenauskunft nach dem Berliner Informationsfreiheitsgesetz (IFG) vorsieht.[17] Dies überrascht vor dem Hintergrund der Ausführungen in den Richtlinien der Regierungspolitik 2023-2026, wonach die „hohen Standards des Berliner Informationsfreiheitsgesetzes“ erhalten bleiben und das Informationsfreiheitsgesetz eigentlich zu einem Transparenzgesetz ausgebaut werden soll.[18] Ein Transparenzgesetz lässt dagegen trotz zahlreicher Ankündigungen und Gesetzentwürfe weiter auf sich warten.[19]

Zudem wurde das Lebensmittelüberwachungstransparenzgesetz (LMÜTranspG) in diesem Jahr abgeschafft,[20] ein Gesetz, das Transparenzvorgaben zu Hygienekontrollen in Restaurants und anderen Lebensmittelbetrieben vorsah.

Aus gegebenen Anlässen in Bund und Ländern hat sich die IFK, die in diesem Jahr unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit tagte, im Übrigen zu den folgenden Themen zur Stärkung der Informationsfreiheit und der Transparenz öffentlich geäußert:

So forderte sie bereits vor Beginn der o. g. Sondierungsgespräche nach der Bundestagswahl die Parteivorsitzenden auf, das Potenzial von Open Data für Innovation

15 Richtlinie 2003/4/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003 über den Zugang der Öffentlichkeit zu Umweltinformationen und zur Aufhebung der Richtlinie 90/313/EWG des Rates.
16 Deshalb war dies zu Recht Schwerpunktthema bei der diesjährigen Internationalen Konferenz der Informationsfreiheitsbeauftragten (ICIC) in Berlin. Siehe D.III.1.
17 Siehe B.III.2.
18 Abrufbar unter https://www.berlin.de/rbmskzl/politik/senat/richtlinien-der-politik/.
19 Siehe zuletzt JB 2023, A.I.1.
20 Siehe B.III.1.

und Wachstum in der demokratischen Gesellschaft besser nutzbar zu machen. Dazu könnten ein modernes Transparenzgesetz sowie ein effizientes Bundespressegesetz verhelfen, welche bislang nicht existieren.[21] Die IFK forderte zudem die Gesetzgeber des Bundes und der Länder in einer Entschließung auf, Unklarheiten in Bezug auf die Anwendung der Transparenz- und Informationsfreiheitsgesetze auf Wahlleitungen zu beseitigen.[22] Zusätzlich plädierte die IFK in einer Entschließung für eine gesetzliche Pflicht zur proaktiven Bereitstellung von Niederschriften öffentlicher Sitzungen der Kommunalparlamente.[23] Denn dort wird beraten und entschieden, welche öffentlichen Vorhaben im unmittelbaren Lebensumfeld der Menschen umgesetzt werden.[24]

Die IFK forderte die Gesetzgeber des Bundes und der Länder auch auf, einen möglichst weitgehenden Zugangsanspruch zu Informationen über Herkunft und Rahmenbedingungen von Drittmittelforschung an Hochschulen zu gewährleisten.[25]

Anlässlich des Internationalen Tages der Informationsfreiheit[26] appellierte die IFK schließlich erneut an die Entscheidungsträger in Parlamenten und Regierungen, Regeln für Transparenz und Informationsfreiheit fortzuentwickeln und auszubauen. Die jüngste Entwicklung der Informationsfreiheit in Deutschland ginge in die falsche Richtung.[27]

21 Entschließung vom 13. März 2025: „Mehr Transparenz und Open Data nach der Bundestagswahl!“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk/.

22 Entschließung vom 18. Juni 2025: „Transparenz bei Wahlleitungen klar regeln!“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk/.

23 Vergleichbar mit den Kommunalparlamenten in den bundesdeutschen Flächenländern sind im Land Berlin die Bezirksverordnetenversammlungen (BVV).

24 Entschließung vom 18. Juni 2025: „Protokolle der öffentlichen Sitzungen der Kommunalparlamente offenlegen!“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk/.

25 Entschließung vom 26. November 2025: „Privat finanzierte Forschung an Hochschulen muss transparenter werden!“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk/.

26 Die 74. Generalversammlung der Vereinten Nationen hat im Jahr 2019 den 28. September zum jährlich wiederkehrenden Tag für den universellen Zugang zu Informationen erklärt. Einzelheiten dazu unter https://www.unesco.org/en/days/universal-access-information.

27 Pressemitteilung vom 26. September 2025: „Internationaler Tag der Informationsfreiheit: Deutschland braucht mehr Transparenz!“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk/.

III. Vorhaben zur Änderung des Berliner Datenschutzgesetzes und anderer Gesetze

Seit vielen Jahren fordern wir eine Überarbeitung des Berliner Datenschutzgesetzes (BlnDSG).[28] Jetzt hat die Senatsverwaltung für Inneres und Sport einen Entwurf eines Gesetzes zur Änderung des BlnDSG und weiterer Gesetze vorgelegt. Leider wurden unsere Vorschläge zum Großteil in den Entwurf nicht übernommen.

In den Jahren seit dem Inkrafttreten des BlnDSG sind in unserer Arbeit immer wieder Fallkonstellationen aufgetreten, die Defizite in dem Regelwerk – auch im Hinblick auf die Europarechtskonformität – sichtbar gemacht haben, wodurch unsere praktische Aufsichtstätigkeit erschwert wird. Die meisten unserer Änderungsvorschläge betreffen handwerkliche Mängel, deren Behebung wesentlich zur Rechtssicherheit und Handhabbarkeit der datenschutzrechtlichen Normen beitragen würde.

Daneben gibt es allerdings auch Punkte, die von besonderer Bedeutung für den Grundrechtsschutz sind. So fehlen unserer Behörde in den Bereichen Inneres und Justiz nach wie vor wirksame Durchsetzungsbefugnisse. Unsere Behörde soll auch in dem aktuellen Gesetzentwurf gegenüber Behörden in diesen Bereichen keine gesetzlichen Befugnisse für verpflichtende Maßnahmen erhalten. Festgestellte Verstöße können daher weiterhin von uns gegenüber den verantwortlichen Stellen nur unverbindlich beanstandet werden. Dies widerspricht den insoweit eindeutigen Vorgaben der europäischen JI-Richtlinie[29]. Dieses Defizit ist sehr gravierend: Die Gefahrenabwehr- und

28 Siehe JB 2020, 17.1.

29 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

Strafverfolgungsbehörden sollen mit den notwendigen Befugnissen ausgestattet sein, sie verarbeiten aber besonders schutzbedürftige Daten, wie z. B. Daten von Zeug:innen in strafrechtlichen Ermittlungsverfahren. Hinzu kommt, dass die Einbindung unserer Behörde bspw. in Form von regelmäßigen Prüfpflichten in neueren Gesetzen festgelegt wird, um damit die Schaffung bzw. Erweiterung von Eingriffsbefugnissen zu kompensieren, die besonders grundrechtsintensiv sind.[30] Solange unsere Behörde jedoch gar nicht die Möglichkeit besitzt, einer unzulässigen Maßnahme auch mit effektiven Mitteln, etwa durch Unterlassungsanordnungen, entgegenzuwirken, kann unsere Einbindung nicht den beabsichtigten kompensatorischen Effekt entfalten.

In allen anderen Bereichen der öffentlichen Verwaltung können wir zwar förmliche Anordnungen treffen. Hier fehlen jedoch nach wie vor die dazugehörigen Vollstreckungsmöglichkeiten. Ohne die Möglichkeit, Zwangsgelder festzusetzen oder eine Ersatzvornahme zu veranlassen, können solche Anordnungen – etwa zur Löschung rechtswidrig gespeicherter Daten – letztlich nicht zwangsweise durchgesetzt werden. Die effektive Durchsetzung unserer Aufsichtsmaßnahmen ist dadurch nicht gewährleistet. Hinzu kommt, dass wir auch keine Bußgelder gegen Behörden oder sonstige öffentliche Stellen verhängen können. Insbesondere die sonstigen öffentlichen Stellen, wie Eigenbetriebe oder privatrechtlich organisierte Betriebe, die Aufgaben der öffentlichen Verwaltung wahrnehmen und sich mehrheitlich in Landeshand befinden, werden so in nicht begründbarer Weise gegenüber rein privaten Stellen mit vergleichbaren Aufgaben privilegiert.

Mit dem Gesetzesentwurf der Senatsverwaltung für Inneres und Sport sollen im Übrigen neben informationsfreiheitsrechtlichen Vorschriften[31] auch datenschutzrechtliche Spezialvorschriften geändert werden. Dazu gehören Vorschriften des Bäder-Anstaltsgesetzes (BBBG) zur Identitätskontrolle und zur Videoüberwachung: Durch die Pläne zur Ergänzung der Normen des BBBG ergeben sich zwar keine Änderungen gegenüber der bestehenden Rechtslage. Eine Verarbeitung personenbezogener Daten ist schon jetzt zulässig, wenn sie zur Erfüllung der Aufgaben der Berliner Bäder-Betriebe erforderlich ist.[32] Daran ändert auch die Konkretisierung der Aufgaben nichts. Allerdings ist es entgegen der Gesetzesbegründung gerade nicht nachgewiesen, dass die Pflicht,

30 Siehe bspw. § 51b Allgemeines Sicherheits- und Ordnungsgesetz Berlin (ASOG).
31 Siehe auch B.III.2.
32 Siehe § 23 BBBG.

einen Identitätsnachweis mitzuführen, bewirkt, dass mehr Tatverdächtige identifiziert werden können und gewaltbereite Personen daher von der Begehung von Straftaten abgeschreckt werden. Die Identität der in einem Bad angetroffenen Tatverdächtigen kann auch weiterhin zuverlässig nur durch die Polizei festgestellt werden. Darüber hinaus lässt sich der Gesetzesbegründung nicht entnehmen, ob in der gesetzlichen Abwägung berücksichtigt wurde, dass auch potenzielle Badbesucher:innen, die keine Gewalttäter:innen sind, trotz einer reinen Sichtkontrolle durch den Ausweiszwang von einem Badbesuch abgehalten werden.

Die im Gesetzentwurf zudem vorgesehene Regelung zur Videoüberwachung in den Bädern läuft ebenfalls ins Leere. Maßnahmen zur Videoüberwachung lassen sich bereits nach jetziger Rechtslage durchführen.[33] Entscheidend ist auch hier, dass sie geeignet, erforderlich und angemessen sind, um einen störungsfreien Badebetrieb zu gewährleisten, und keine schutzwürdigen Interessen der betroffenen Personen überwiegen.[34] Da die im Gesetzentwurf vorgesehenen Normen insoweit nicht zur Rechtsklarheit beitragen, haben wir sie kritisiert.

Wir setzen uns im weiteren Gesetzgebungsverfahren dafür ein, dass die genannten Defizite ausgeräumt werden und unsere Vorschläge bei der Überarbeitung der genannten Gesetze Berücksichtigung finden. Unser Ziel ist es, dass europarechtskonforme, rechtssichere und in der Praxis handhabbare Regelungen geschaffen werden.

33 Siehe § 20 BlnDSG.
34 Siehe JB 2023, A.VII.3; JB 2024, A.X.4.

B.

Wir in Berlin

I. Gerichtsverfahren

1. Keine Herausgabe von Kopien der Videoaufzeichnungen bei Auskunftsersuchen

Das Oberverwaltungsgericht (OVG) Berlin-Brandenburg stellte fest, dass Videoaufzeichnungen in Bahnen der Berliner S-Bahn eine Verarbeitung personenbezogener Daten sind, und revidierte damit die Auffassung des Verwaltungsgerichts (VG) Berlin. Die Videosequenzen müssten als Kopien personenbezogener Daten jedoch nicht herausgegeben werden, wenn es dem Verantwortlichen, wie hier, nicht zumutbar sei, den Auskunftssuchenden zu identifizieren, oder die Herausgabe der Sequenzen zu unzumutbarem Aufwand für den Verantwortlichen führe. Das Urteil ist nicht rechtkräftig und zwischenzeitlich beim Bundesverwaltungsgericht (BVerwG) rechtshängig.

Die zu der Deutschen Bahn AG gehörende S-Bahn Berlin GmbH verweigerte als Betreiberin der S-Bahn Berlin gegenüber einem Bürger die Herausgabe von Sequenzen aus einer ihn betreffenden Videoüberwachung in ihren Zügen. Wir verwarnten deshalb die Verantwortliche, die hiergegen Klage erhob. Darin machte sie insbesondere geltend, dass die Videosequenzen für sie keine personenbezogenen Daten darstellten, da sie die darin abgebildeten Personen nicht identifizieren könne. Das VG Berlin gab der Klage statt.[35]

Im Berufungsverfahren machte nun das OVG Berlin-Brandenburg deutlich, dass die vom VG Berlin angeführten Gründe der Entscheidung nicht tragen.[36] Insbesondere folgte das OVG unserer Rechtsauffassung, dass die durch die Videoaufzeichnung verarbeiteten Daten personenbezogen sind, weil sie sich auf identifizierbare Personen beziehen. Dabei ließ das OVG offen, ob für die Frage des Personenbezugs ein absoluter oder relativer Ansatz anzulegen ist: Es war hier im Rahmen des Verarbeitungsprozesses gerade vorgesehen, dass Personen mithilfe Dritter, d. h. durch das Einschalten von Strafverfolgungsbehörden, identifiziert werden können.

35 VG Berlin, Urteil vom 12. Oktober 2023, VG 1 K 561/21; siehe auch JB 2023, A.II.3.
36 OVG Berlin-Brandenburg, Urteil vom 13. Mai 2025, OVG 12 B 14/23.

Das OVG verwarf zudem weitere Erwägungen, die das VG Berlin unter Nichtanwendung des Unionrechts auf der Grundlage nationaler Normen angestellt hatte. Diese betrafen das sog. allgemeine Günstigkeitsprinzip, welches der Beweislastverteilung der Datenschutz-Grundverordnung (DSGVO) widerspricht, sowie die Anwendung des Unmöglichkeitsausschlusses gem. § 275 Bürgerliches Gesetzbuch (BGB) auf den Auskunftsanspruch. Schließlich sprach das OVG unter Heranziehung der neueren Rechtsprechung des Europäischen Gerichtshofs (EuGH)[37] den Aufsichtsbehörden bei Vorliegen eines datenschutzrechtlichen Verstoßes ein intendiertes Auswahlermessen hinsichtlich der Abhilfemaßnahmen zu.

Dennoch kam das OVG Berlin-Brandenburg zu dem Ergebnis, dass unsere Verwarnung rechtswidrig sei, und vertrat die Auffassung, dass der Anspruch auf eine Kopie der personenbezogenen Daten gem. Art. 11 Abs. 2 i. V. m. Art. 12 Abs. 2 Satz 2 DSGVO ausgeschlossen sei. Ein Verantwortlicher kann die Auskunft verweigern, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren. Dies sei vorliegend der Fall. Die Klägerin erfasse die Daten ohne gezielten Personenbezug und könne betroffene Personen mit den ihr unmittelbar zur Verfügung stehenden Mitteln nicht identifizieren. Eine Identifizierung könne nur bei entsprechendem Anlass unter Zuhilfenahme der Strafverfolgungsbehörden erfolgen. Dabei kommt es nach dem OVG Berlin-Brandenburg für die Möglichkeit der Identifizierung nicht auf die theoretische Machbarkeit an, sondern auf eine Zumutbarkeitsprüfung. Insbesondere sei bei der Verantwortlichen zu berücksichtigen, dass das ansonsten auf Datensparsamkeit und -minimierung ausgelegte Datenschutzkonzept eine eigene Durchsicht und Analyse der Videoaufzeichnungen nicht vorsehe. Auch würde eine Durchsicht und Analyse von Videoaufzeichnungen zu einer längeren Speicherdauer und weiteren Eingriffen in die Datenschutzrechte von Mitfahrer:innen führen. Eine Abkehr vom Datenschutzkonzept sei der Klägerin auch unter Berücksichtigung des Transparenzinteresses des Auskunftssuchenden nicht zumutbar.

Das geringe Auskunftsinteresse des Auskunftssuchenden, die Eingriffe in die Freiheitsrechte Dritter sowie die personellen, technischen, rechtlichen und organisatorischen Maßnahmen, die zur Herausgabe der Kopie der Videoaufzeichnungen durch die Verantwortliche umgesetzt werden müssten, führten laut OVG im Rahmen der

37 Siehe EuGH, Urteil vom 26. September 2024, C-768/21, Rn. 41 ff.

Güterabwägung gem. Art. 15 Abs. 4 DSGVO ebenfalls zu einem Ausschluss der Herausgabe von Videosequenzen. Der Auskunftssuchende ist, als Beigeladener, gegen das Urteil in Revision gegangen. Das Urteil ist daher nicht rechtskräftig.

Das OVG Berlin-Brandenburg stärkt mit seinem Urteil eine eng an der DSGVO, der EuGH-Rechtsprechung und EDSA-Leitlinien orientierte Rechtsfindung. Die Klarstellungen bezüglich des Personenbezugs sowie zum intendierten Ermessen bestätigen unsere Aufsichtspraxis. Die vom OVG Berlin-Brandenburg erörterten Ausschlussgründe in Art. 11 DSGVO sind sicherlich auch vor dem Hintergrund der speziellen Fallkonstellation zu bewerten. Gleichwohl sind wir gespannt, welche weiteren Erkenntnisse das Revisionsverfahren vor dem BVerwG insbesondere im Hinblick auf die Auslegung der Ausschlussgründe von Betroffenenrechten bringen wird.

2. Gemeinsame Verantwortlichkeit im Lettershop-Verfahren

Das VG Berlin hält Werbende, die sozioökonomische Merkmale für Adressat:innen von Werbung vorgeben, und Adresshändler:innen bei Nutzung eines sog. Lettershop-Verfahrens nicht für gemeinsam Verantwortliche. Die Entscheidung betrifft die Frage, ob das auftraggebende Unternehmen, das eine Zielgruppe für seine Werbung nach Wohnort und Kaufkraft auswählt, datenschutzrechtlich gemeinsam mit der Adresshändlerin für die Auswahl und Nutzung der konkreten Adressdaten verantwortlich ist. Das VG verneint dies und hat unsere darauf bezogene Verwarnung gegen das auftraggebende Unternehmen aufgehoben.[38] Das Urteil ist nicht rechtskräftig.

Das Gericht stellte zunächst fest, dass Auslesen und Verwenden der postalischen Adressdaten für den Versand des Werbeschreibens Verarbeitungen personenbezogener Daten darstellen.[39] Eine gemeinsame Verantwortlichkeit[40] verneinte es jedoch in diesem Zusammenhang.[41] Zwar beeinflusse das auftraggebende Unternehmen im eigenen wirtschaftlichen Interesse den Zweck der Verarbeitung, es nehme jedoch

38 VG Berlin, Urteil vom 14. Oktober 2025, 1 K 74/24.
39 Siehe Art. 4 Nr. 1, 2 DSGVO.
40 Siehe Art. 4 Nr. 7 und Art. 26 Abs. 1 DSGVO.
41 VG Berlin, Urteil vom 14. Oktober 2025, 1 K 74/24, Rn. 24 ff.

keinen Einfluss auf die Mittel der Verarbeitung. Die gesamte organisatorische und technische Ausgestaltung des Werbeverfahrens – von der Anreicherung der Adressdaten mit sozioökonomischen Merkmalen über die Adressselektion bis zur Versendung – liege allein bei der Adresshändlerin. Die Vorgabe einer Zielgruppe genüge nicht als Mitbestimmung der Mittel i. S. v. Art. 4 Nr. 7 DSGVO.

Unsere Behörde teilt diese Rechtsauffassung nicht. Die Adresshändler:innen und die Werbenden sind nach unserer Bewertung gemeinsam verantwortlich. Die DSGVO geht von gemeinsam Verantwortlichen aus, wenn zwei oder mehr Verantwortliche gemeinschaftlich die Zwecke der und die Mittel zur Verarbeitung festlegen.[42] Mit der Entscheidung, einer anhand von sozioökonomischen Merkmalen definierten Zielgruppe Werbung zur Neukundengewinnung zuzusenden, initiiert das auftraggebende Unternehmen die damit verbundene Verarbeitung personenbezogener Daten und entscheidet insofern auch über den Zweck der Datenverarbeitung (mit). Das auftraggebende Unternehmen lässt die Werbemaßnahme durchführen, um davon wirtschaftlich zu profitieren. Für den Erfolg der Werbeaktion des auftraggebenden Unternehmens ist wesentlich, wer beworben wird.

Gleiches gilt auch für die Wahl der wesentlichen Mittel der Verarbeitung, bei der das Verfahren durch die Adresshändlerin und der konkrete Inhalt des Werbeschreibens sowie die Auswahl der Adressat:innen durch die Werbenden (mit)festgelegt werden. Das beauftragende Unternehmen hat in eigenem wirtschaftlichen Interesse mithilfe von Kriterien der Adresshändlerin die Adressat:innen der Werbemaßnahme abstrakt bestimmt und damit letztlich entschieden, wessen Daten verarbeitet werden. Mit dieser Entscheidung legte es die wesentlichen Mittel der Verarbeitung fest. Dabei kommt es nicht darauf an, dass das beauftragende Unternehmen die konkreten Namen und Adressen der Personen kennt, die von der Adresshändlerin ausgewählt werden, oder dass es Zugang zu den jeweiligen personenbezogenen Daten hat. Nach der Rechtsprechung des EuGH kann über die Zwecke und Mittel der Datenverarbeitung auch entscheiden, wer die Daten nicht selbst verarbeitet, also selbst keinen Zugriff auf sie hat.[43] Entscheidend ist aus unserer Sicht vielmehr, dass das auftraggebende Unternehmen individuelle Wirkung bei den ausgewählten Adressat:innen erzeugen möchte, wofür die personenbezogene Datenverarbeitung Grundlage ist.

42 Art. 26 Abs. 1 Satz 1 DSGVO.
43 EuGH, Urteil vom 5. Juni 2018, C-210/16, Rn. 38.

Das Gericht lässt im Übrigen ausdrücklich offen, ob sich die Datenverarbeitung auf eine Rechtsgrundlage stützen lässt.[44]

Das VG Berlin verneinte bei einer selektiven Neukundengewinnung mittels einer Adresshändlerin eine gemeinsame Verantwortlichkeit von Werbenden und Adresshändler:innen. Nach unserer Auffassung legen beide Seiten Zweck und wesentliche Mittel der Verarbeitung gemeinsam fest. Weder der Einsatz von abstrakten Selektionskriterien noch ein fehlender Datenzugang schließen aus unserer Sicht eine gemeinsame Verantwortlichkeit aus. Im Gegenteil, durch eine künstliche Aufspaltung des Datenverarbeitungsprozesses darf nicht in den Hintergrund treten, wer von der personenbezogenen Datenverarbeitung profitiert und diese daher auch initiiert. Wegen der grundsätzlichen Bedeutung für Art. 26 DSGVO im Adresshandelsbereich haben wir Berufung eingelegt. Die Berufung war vom Gericht ausdrücklich zugelassen worden. Eine obergerichtliche Klärung steht damit noch aus.

3. Juristische Personen zu umfassender Auskunft gegenüber Datenschutzaufsichtsbehörden verpflichtet

Die Aufsichtsbehörden dürfen von Verantwortlichen und Auftragsverarbeitern umfassende Auskünfte zur Verarbeitung personenbezogener Daten verlangen. Weder braucht es einen Verdacht auf einen Datenschutzverstoß noch ist das Auskunftsrecht beschränkt, wenn ein Datenschutzverstoß bereits feststeht. Juristische Personen können die Auskunft auch nicht mit Verweis auf die Selbstbelastungsfreiheit verweigern. Diese Auffassung bestätigte das VG Berlin in einem noch nicht rechtskräftigen Urteil.

Ein Buchverlag vermietete an Geschäftskunden Adressdaten für postalische Werbung. Da die betroffenen Personen in die Vermietung ihrer Daten zu Werbezwecken nicht eingewilligt hatten und die Verarbeitung auch nicht auf eine sonstige gesetzliche Grundlage gestützt werden konnte, verwarnten wir das Unternehmen.[45] Wir verpflichteten das Unternehmen u. a. mitzuteilen, wie viele Kundendaten es in bestimmten Quartalen nach Bestandskraft der Verwarnung zu Werbezwecken an Dritte vermietete. Nachdem das Unternehmen sich weigerte, diese Auskünfte zu erteilen, erließen wir einen

44 Siehe Art. 6 Abs. 1 Satz 1 DSGVO.
45 Zum Adresshandel siehe auch B.I.2.; JB 2024, A.I.1.; JB 2020, 10.2.; JB 2019, 1.3.

Auskunftsheranziehungsbescheid und drohten für den Fall der Nichtbeantwortung ein Zwangsgeld in Höhe von 500 Euro an. Dagegen erhob das Unternehmen Klage vor dem VG Berlin.

Das VG Berlin wies die Klage ab.[46] Es stellte fest, dass unsere Befugnis, nach Art. 58 Abs. 1 lit. a DSGVO Auskunft zu verlangen, auf die zur Erfüllung unserer Aufgaben erforderlichen Informationen gerichtet ist. Aufgrund unserer Aufgabe, die Anwendung der DSGVO zu überwachen und durchzusetzen,[47] sind wir dabei auch befugt, Auskünfte zu verlangen, wenn noch kein Verdacht auf einen Datenschutzverstoß vorliegt. Auch wenn bereits ein Datenschutzverstoß feststeht, gilt die Befugnis fort, etwa um das Ausmaß des Verstoßes oder die Beteiligung weiterer Akteure am Verstoß festzustellen.

Des Weiteren stellte das VG fest, dass juristische Personen – wie das betroffene Unternehmen – nicht die Auskunft verweigern können. Der Grundsatz der Selbstbelastungsfreiheit[48] gelte nur, wenn natürliche Personen zur Auskunft verpflichtet werden. Zwar ist der Grundsatz der Selbstbelastungsfreiheit verfassungsrechtlich verankert, doch er ist Ausfluss der Menschenwürde und des allgemeinen Persönlichkeitsrechts.[49] Auf diese Grundrechte können sich juristische Personen, wie das verpflichtete Unternehmen, nicht berufen. Ein Zwang zur Selbstbezichtigung berührt die Würde des Menschen, dessen Aussage als Mittel gegen ihn selbst verwendet wird. Eine Lage, wie sie dieser Zwang für natürliche Personen darstellt, kann bei juristischen Personen nicht eintreten. Sie bilden ihren Willen durch Organe und unterliegen im Hinblick auf Straftaten und Ordnungswidrigkeiten nur einer eingeschränkten Verantwortlichkeit. Juristische Personen können sich nicht selbst strafbar machen und das Festsetzen einer Geldbuße gegen sie enthält – für den Schutz vor Selbstbezichtigung wesentlich – weder einen Schuldvorwurf noch eine ethische Missbilligung.

Die Klägerin hat die Zulassung der Berufung beantragt. Damit ist das Urteil noch nicht rechtskräftig.

46 VG Berlin, Urteil vom 9. Oktober 2025, VG 1 K 607/22.
47 Siehe Art. 57 Abs. 1 lit. a DSGVO.
48 Siehe § 40 Abs. 4 Satz 2 BDSG.
49 Siehe Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG).

Das VG Berlin bestätigt unsere Praxis und stärkt damit die effektive Durchführung unserer aufsichtsbehördlichen Tätigkeiten. Unternehmen sind uns gegenüber zur umfassenden Auskunft bezüglich ihrer Datenverarbeitungsvorgänge verpflichtet. Diese Auskünfte sind elementarer Bestandteil unserer Arbeit und dienen dazu, sowohl be- als auch entlastende Informationen zu erhalten und die Verarbeitungsvorgänge abschließend rechtlich bewerten zu können. Kommt ein Verantwortlicher einem formlosen Auskunftsersuchen nicht nach, erlassen wir in der Regel einen sog. Auskunftsheranziehungsbescheid. Weigern sich Verantwortliche des nicht-öffentlichen Bereichs weiterhin, können wir gegen sie Zwangsgelder festsetzen, um eine Auskunft zu erzwingen. Eine solche Weigerung kann zugleich auch einen bußgeldbewehrten Verstoß gegen die Kooperationspflicht gem. Art. 31 DSGVO darstellen.

4. Medienprivileg gilt auch für Beiträge auf Wikipedia

Für die Prüfung der Veröffentlichung eines Fotos von einem Wohnhaus und dessen Adresse im Rahmen einer Auflistung von Kulturdenkmälern auf der Website de.wikipedia.org sind wir als datenschutzrechtliche Aufsichtsbehörde nicht zuständig. Das VG Berlin bestätigte unsere Auffassung, dass in diesem Fall eine Datenverarbeitung zu literarischen Zwecken vorliegt.

Ein Bürger beschwerte sich bei uns über die Veröffentlichung eines Fotos seines Wohnhauses und der dazugehörigen Adresse. Das Foto befand sich in einer Liste von Kulturdenkmälern einer Stadt, in der auch eine Beschreibung des Hauses und der Bauzeit aufgeführt waren. Die Auflistung erschien als Beitrag auf der Website de.wikipedia.org. Wir teilten dem Bürger mit, dass wir mangels Zuständigkeit in diesem Fall nicht tätig werden können. Gegen unsere Entscheidung erhob der Bürger Klage vor dem VG Berlin.

Das VG Berlin bestätigte unsere Auffassung, dass das Foto des Wohnhauses und dessen Adresse zu literarischen Zwecken veröffentlicht wurden.[50] Die Veröffentlichung unterfällt daher dem sog. Medienprivileg.[51] Danach werden Verarbeitungen zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken u. a. privilegiert und sind

50 VG Berlin, Urteil v. 10. Dezember 2024, VG 1 K 463/23.
51 Siehe § 19 Abs. 1 Satz 1 BlnDSG i. V. m. Art. 85 Abs. 2 DSGVO.

von unserer Aufsicht ausgenommen. Das VG Berlin stellte des Weiteren fest, dass der Berliner Gesetzgeber die Meinungsfreiheit und Informationsfreiheit mit dem Recht auf Schutz personenbezogener Daten im Berliner Datenschutzgesetz (BlnDSG) in Einklang gebracht habe und das Gesetz insofern den unionsrechtlichen Anforderungen genüge.

Das VG Berlin wies darauf hin, dass dem Medienprivileg auch Sammlungen, wie eine Auflistung von Denkmälern, unterfallen können. Auf das Privileg kann sich ein Verantwortlicher jedoch nur dann berufen, wenn die meinungsbildende Wirkung für die Allgemeinheit prägender Bestandteil des Angebots ist. Dieses Maß an literarischer Bearbeitung konnte die Denkmalliste aufweisen, denn sie ist strukturiert und mit erläuternden Hinweisen sowie Verweisen auf Quellen versehen. Die Veröffentlichung ist daher Teil eines Nachschlagewerks und damit Sachliteratur.

Der Antrag auf Zulassung der Berufung wurde durch Beschluss des OVG Berlin-Brandenburg abgelehnt.[52]

Das sog. Medienprivileg bringt das Spannungsverhältnis zwischen den Medien- und Kommunikationsfreiheiten und der informationellen Selbstbestimmung in Ausgleich. Es nimmt dabei den Schutz personenbezogener Daten im Journalismus, der Wissenschaft, der Kunst und der Literatur von staatlicher Aufsicht aus. Bürger:innen sind gleichwohl nicht schutzlos gestellt. Ihnen steht bspw. der Weg zu den Zivilgerichten offen. Für unsere Kontrollbefugnis kommt es darauf an, ob die jeweilige Datenverarbeitung Ausdruck der vorgenannten Grundrechtsausübung und damit privilegiert ist. Dies dürfte bei reinen Bilddatenbanken ohne journalistische Prägung oder der einfachen, unstrukturierten Auflistung von Informationen regelmäßig nicht der Fall sein.

52 OVG Berlin-Brandenburg, Beschluss vom 28. Mai 2025, OVG 12 N 9/25.

5. Umfassende Auskunftspflicht auch bei Identitätsdiebstahl

Verlangt die betroffene Person nach einem Identitätsdiebstahl Auskunft von der verantwortlichen Stelle, so ist diese umfassend zu erteilen. Dabei sind auch Informationen über den widerrechtlich handelnden Dritten zu beauskunften, sofern sich diese Informationen auf die Person des Auskunftssuchenden beziehen. Diese Rechtsauffassung hat das VG Berlin bestätigt. Das Urteil ist noch nicht rechtskräftig, die Klägerin hat einen Antrag auf Zulassung der Berufung gestellt.

Aufgrund einer Abbuchung bei seiner Bank wurde ein Bürger auf einen Identitätsdiebstahl aufmerksam. Offensichtlich hatte ein Dritter unter seiner Identität dem Anbieter einer Lern-App ein Lastschriftmandat erteilt. Der Bürger wandte sich an den Kundenservice der Lern-App-Betreiberin, widerrief das Lastschriftmandat und forderte Auskunft über seine personenbezogenen Daten. Nach einem Monat erhielt der Bürger per E-Mail aber nur Auskunft über seinen Namen, den Profilnamen, die Zahlungsmethode, die IBAN und das Buchungsdatum. Die IBAN wurde dabei ungekürzt im Klartext angegeben. Nicht beauskunftet wurden u. a. die übrigen zum Benutzerkonto gehörenden Daten, wie Registrierungsdatum, Newsletter-Aktivierung, Letzte Anmeldung, Browser, Buchungsdaten, Lernfortschritt, IP-Adresse und Transaktionsdaten. Nach Ansicht der verantwortlichen Stelle handele es sich dabei um Daten des widerrechtlich vorgehenden Dritten, die nicht zu beauskunften seien.

Aufgrund unserer Intervention sah sich die Verantwortliche gezwungen, den Beschwerdeführer auch über die übrigen Daten zu informieren. Wir stellten abschließend einen Verstoß fest, da die vollständige Auskunft mehr als zwei Jahre später erfolgte und nicht unverzüglich, wie gesetzlich vorgesehen.[53] Da wir auch in der ungekürzten Wiedergabe der IBAN des Beschwerdeführers bei Auskunftserteilung per unverschlüsselte E-Mail einen Verstoß sahen,[54] verwarnten wir die Verantwortliche. Gegen die Verwarnung erhob die Verantwortliche Klage vor dem VG Berlin.

53 Siehe Art. 12 Abs. 3 DSGVO.
54 Siehe Art. 32 DSGVO.

Das VG Berlin stellte in seinem Urteil[55] daraufhin klar, dass es für die Frage des Personenbezugs nicht darauf ankommt, aus welcher Quelle die Daten über eine Person stammen oder ob sie auch mit einer anderen Person verknüpft sind. Weil zahlreiche Informationen in dem, mit dem im Namen des Beschwerdeführers erstellten, Benutzerkonto gespeichert waren, hätten diese rechtzeitig beauskunftet werden müssen. Das Gericht bestätigte des Weiteren unsere Auffassung, dass die Verantwortliche im Falle des Identitätsdiebstahls die Auskunft nicht nach Art. 15 Abs. 4 DSGVO wegen der Rechte und Freiheiten des widerrechtlich handelnden Dritten beschränken kann.[56] Die vorzunehmende Güterabwägung fällt zugunsten des Auskunftssuchenden aus, denn der Dritte hat seine personenbezogenen Daten mit denen des Auskunftssuchenden widerrechtlich verknüpft.

Schließlich stellte das VG Berlin klar, dass eine Verwarnung kein Verschulden voraussetzt und wir diese auch dann erlassen können, wenn unsere Rechtsansicht zu der zugrundeliegenden Fallkonstellation zuvor nicht publiziert worden ist. Es bestätigte auch, dass wir nicht zu Rechtsberatungsleistungen in laufenden Aufsichtsverfahren verpflichtet sind.

Das Urteil konkretisiert den Umfang des Auskunftsanspruchs und gibt klare Leitlinien für die Güterabwägung mit den Rechten und Freiheiten anderer Personen in Fällen von Identitätsdiebstahl. Es zeigt auch, dass Verantwortliche selbst, unabhängig von den Hilfestellungen der Aufsichtsbehörde, verpflichtet sind, rechtzeitig Rechtskonformität herzustellen, auch in ungewöhnlichen Fällen.

6. Sachverständigenrolle nach dem Unterlassungsklagengesetz

Verstöße gegen das Datenschutzrecht können auch nach dem Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (UKlaG) von Verbänden vor Gericht gebracht werden. In zwei Klageverfahren von Verbraucherverbänden haben wir gegenüber dem Landgericht (LG) Berlin II sachverständige Stellungnahmen abgegeben.

55 VG Berlin, Urteil vom 9. Oktober 2025, VG 1 K 463/22.
56 Dazu bereits JB 2020, 10.1.

Wer gegen Vorschriften verstößt, die dem Schutz von Verbraucher:innen dienen, kann nach § 2 UKlaG auf Unterlassung und Beseitigung in Anspruch genommen werden. Klagebefugt sind u. a. verschiedene Verbraucher- und Wirtschaftsverbände.[57] Die Unterlassungsklagen werden nicht vor dem VG, sondern vor Zivilgerichten verhandelt. Nach § 12a UKlaG sind bei bestimmten Unterlassungsklagen die zuständigen Aufsichtsbehörden anzuhören. Wir haben in diesem Zusammenhang im Berichtsjahr in zwei Fällen Stellungnahmen gegenüber dem LG Berlin II abgegeben.

In einem Fall ging es um einen Onlinehändler, der nicht nur eigene Waren vertreibt, sondern auch eine Handelsplattform für Angebote Dritter betreibt. Der Händler erlaubte Käufe nur nach dem Eröffnen eines Kundenkontos. Bestellungen „als Gast", also ohne ein Kundenkonto, waren nicht möglich.[58] Das Unternehmen berief sich u. a. darauf, dass die Registrierung zur Vertragsdurchführung erforderlich sei. Man verkaufe nicht nur Waren, sondern betreibe eine umfassende Modeplattform.

Das Gericht sah es als unzulässig an, dass die Nutzer:innen verpflichtet wurden, ein Kundenkonto anzulegen, und folgte damit auch unserer Stellungnahme.[59] Es betonte, dass das Setzen von Vertragszwecken nicht dazu missbraucht werden dürfe, begründete Gedanken der DSGVO in ihr Gegenteil zu verkehren, etwa durch gezielte „datenintensive" Zwecksetzungen, die in dem Angebot keinen ausreichenden Niederschlag finden. Eine möglichst ausufernde Gestaltung des Vertragsinhalts könne sonst auch solche Datenverarbeitung als „erforderlich" erscheinen lassen, mit denen die Kund:innen wegen des äußeren Erscheinungsbilds der Leistungsbeziehungen typischerweise nicht rechneten. Dass das Unternehmen in beträchtlichem Umfang eine Modeerlebnisplattform sei, könne nichts daran ändern – wesentlicher Vertragsgegenstand sei der Abschluss von Kaufverträgen und gerade dieser Vertragszweck müsse im Rahmen von Art. 6 Abs. 1 Satz 1 lit. b DSGVO die Datenverarbeitung rechtfertigen können. Auch für die Vermittlung von Verkäufen Dritter sei eine Registrierung nicht erforderlich. Auch hier gelte der Grundsatz, dass der einzelne Vertrag in den Blick zu nehmen sei.

In einem anderen Fall ging es um einen Kurzvideodienst, der personenbezogene Daten der Nutzenden auf Basis einer Einwilligung zu Werbezwecken verwendete. Der

57 § 3 UKlaG.
58 Siehe auch D.II.2.
59 LG Berlin II, Urteil vom 31. Januar 2025, 15 O 486/22.

klagende Verbraucherverband behauptete, dass hierfür auch Daten Minderjähriger verwendet würden und die Einwilligungen insoweit unwirksam seien. Das Unternehmen bestritt dies: Es frage bei jeder Anmeldung das Geburtsdatum ab. Wissentlich verarbeite man keine Daten von Minderjährigen zu Werbezwecken.

In unserer Stellungnahme wiesen wir darauf hin, dass das Unternehmen in jedem Einzelfall die Wirksamkeit einer Einwilligung nachweisen können muss. Da das Unternehmen aber das Alter offenbar nur auf Basis des von den Nutzenden selbst angegebenen Geburtsdatums bewertete, konnte es den Nachweis nicht führen. Die im Übrigen angegriffenen Datenverarbeitungen waren schon in der Datenschutzerklärung für uns kaum verständlich beschrieben. Auch im Prozess – bis zu unserer Stellungnahme – legte das Unternehmen nicht näher dar, welche Daten es in welchem Umfang und zu welchen konkreten Zwecken verarbeitete und warum diese Datenverarbeitung jeweils erforderlich war. Somit kam es auch hier seiner Beweislast nicht nach.

Das Gericht verneinte mangels nachgewiesener Einwilligung, die durch die Erziehungsberechtigten der zwischen 13 und 16 Jahre alten Nutzenden hätte erteilt werden müssen,[60] das Vorhandensein einer Rechtsgrundlage[61] des Unternehmens für die Verarbeitung.[62] In seinem Urteil folgte das Gericht ausdrücklich unserer Auffassung, dass die Abfrage des Geburtsdatums der Nutzenden im Registrierungsprozess nicht ausreichend ist, um den datenschutzrechtlichen Anforderungen[63] gerecht zu werden. Diese Abfrage sei angesichts der einfachen Umgehungsmöglichkeiten und der allseits bekannten und diskutierten hohen Risiken für Kinder und Jugendliche nicht ausreichend. Sie kann nicht sicherstellen, dass tatsächlich Daten von Nutzenden unter 16 Jahren nicht für personalisierte Werbung und zur Versendung von Marketingnachrichten verarbeitet werden.

Im Verbandsklageverfahren bietet die in § 12a UKlaG vorgesehene Anhörung für uns als Aufsichtsbehörde eine gute Möglichkeit, unser Wissen aus der Aufsichtspraxis und aufsichtsbehördliche Positionen in das zivilgerichtliche Verfahren einzubringen und bei der Rechtsfindung zu unterstützen.

60 Siehe Art. 8 Abs. 1 Satz 2 DSGVO.
61 Siehe Art. 6 Abs. 1 Satz 1 DSGVO.
62 LG Berlin II, Urteil vom 23. Dezember 2025, 15 O 271/23.
63 Siehe Art. 24 Abs. 1, Art. 25 Abs. 1 und Art. 8 Abs. 2 DSGVO.

II. Bußgeldentscheidungen

1. Unbefugte Abfragen im Polizeiinformationssystem POLIKS

Zahlreiche Bußgeldverfahren betrafen erneut Fälle, in denen Polizist:innen personenbezogene Daten unbefugt, d. h. ohne dienstlichen Anlass, aus polizeiinternen Datenbanken abgerufen und teilweise weitergenutzt haben.

Das Polizeiliche Landessystem zur Information, Kommunikation und Sachbearbeitung (POLIKS) stellt als zentrales IT-Verfahren der Polizei ein äußerst wichtiges Arbeitsmittel dar. Es werden personenbezogene Daten zu Tatverdächtigten, Beschuldigten, Betroffenen von Straftaten etc. zu Zwecken der Vorgangsbearbeitung und als Informationssystem verarbeitet. Aufgrund der Sensibilität dieser Daten gelten für den Zugriff besonders hohe rechtliche und organisatorische Anforderungen.

Auch in diesem Jahr beschäftigten unsere Behörde wiederholt Fälle, in denen Polizeibedienstete ohne dienstlichen Anlass Abfragen in POLIKS vorgenommen hatten. Teilweise betrafen diese Abfragen Personen aus dem privaten Umfeld der jeweiligen Bediensteten oder Personen aus dem eigenen Kolleg:innenkreis.

- 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 tätigte mehrere Abfragen, um unbefugt die Arbeitsleistungen ihrer Kollegin zu kontrollieren, für deren Qualitätssicherung sie nicht zuständig war.

- Ein weiterer Polizeibeamter leitete eine von seinem Kollegen erstattete Strafanzeige an die Führungskräfte des Anzeigenden weiter, um diesen wegen vermeintlich mangelnder Fachkenntnisse bloßzustellen.

Solche unbefugten Zugriffe stellen einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der davon Betroffenen dar. Dabei begründet schon das

bloße Abfragen von personenbezogenen Daten ohne Berechtigung einen Datenschutzverstoß, unabhängig davon, ob die Informationen weitergegeben oder anderweitig verwendet werden.[64]

Jede Abfrage in POLIKS erfordert also einen klaren, dokumentierten, dienstlichen Anlass. Das Prinzip der Zweckbindung sowie das Erforderlichkeitsprinzip sind dabei strikt einzuhalten. Zugriffe „aus Neugier", aus privaten Motiven oder zur Befriedigung persönlicher Interessen sind in jedem Fall unzulässig.

Zur Verbesserung der Zusammenarbeit zwischen uns – als Ordnungswidrigkeitenbehörde – und der Polizei – als für die disziplinarrechtliche Ahndung unzulässiger Datenabfragen zuständige Behörde – wurde in diesem Jahr gemeinsam mit dem Justiziariat und den Disziplinarstellen der Polizei ein einheitliches Verfahren etabliert: Die jeweiligen Disziplinarstellen werden von uns sowohl nach Anhörung der Betroffenen als auch nach Abschluss unseres Verfahrens informiert. Nach Erlass eines Bußgeldbescheids wird ihnen jeweils die Verfahrensakte in Kopie übersandt, damit etwaige dienst- oder disziplinarrechtliche Maßnahmen geprüft werden können. Auf diese Weise soll ein verlässlicher Informationsfluss gewährleistet werden, sodass keine Lücken bei der disziplinarrechtlichen Verfolgung entstehen.

64 Siehe Oberlandesgericht (OLG) Stuttgart, Beschluss vom 25. Februar 2025, 2 ORbs 16 Ss 336/24, Rn. 12.

2. Testimonial-Werbung im Bundestagswahlkampf 2021 mit Geldbußen geahndet

Zur Ansprache von Wähler:innen im Bundestagswahlkampf 2021 erhielt ein Kreisverband einer Partei Adressdatensätze aus dem Melderegister.[65] Der Kreisverband nutzte die Daten, um die Wähler:innen anzuschreiben. Allerdings wurden in diesen Anschreiben weder die Identität des datenschutzrechtlich verantwortlichen Kreisverbands als Absender noch die weiteren obligatorischen Datenschutzinformationen mitgeteilt. Vielmehr wurde der Eindruck erweckt, dass die Schreiben von Berliner Persönlichkeiten aus Politik und Wirtschaft stammten, die an die Wähler:innen appellierten, den Bundestagskandidaten des Kreisverbandes zu wählen (sog. Testimonials).[66] Der Kreisverband übermittelte die Daten zudem an einen Dienstleister zum Versand und Druck der Werbung, ohne dabei eine Auftragsverarbeitungsvereinbarung abzuschließen. Wir haben daraufhin ein Bußgeld verhängt. Dagegen legte der Kreisverband Einspruch ein.

Betroffen waren 55.640 bzw. 77.540 Personen, deren Datensätze (in zwei Chargen) mit Familiennamen, Vornamen, Doktorgrad und den derzeitigen Anschriften aus dem Melderegister abgerufen und für die Testimonial-Werbung verwendet worden waren. Die Gestaltung der Testimonial-Werbung und die damit einhergehende Intransparenz über die Identität des Verantwortlichen stellten Verstöße gegen das Transparenzgebot[67] dar. Die Identität des echten Verantwortlichen blieb den betroffenen Personen bewusst verborgen und es entstanden dadurch erhebliche Unsicherheiten. Die fehlende Mitteilung an die betroffenen Personen über die Informationen nach Art. 14 Datenschutz-Grundverordnung (DSGVO) – wie z. B. woher die Daten stammen, zu welchem Zweck sie verwendet werden und welchen Empfänger:innen sie offengelegt wurden – stellte ebenfalls einen Verstoß dar, der den betroffenen Personen die Ausübung ihrer Rechte deutlich erschwerte.

Zudem beauftragte der Kreisverband einen Dienstleister zum Druck und der Versendung der Wahlwerbung. Die Offenlegung der Meldedatensätze gegenüber diesem

65 Nach § 50 Abs. 1 Satz 1 Bundesmeldegesetz (BMG) dürfen die Meldebehörden Parteien vor Wahlen Auskünfte aus dem Melderegister erteilen.
66 Siehe JB 2022, 14.2.
67 Art. 5 Abs. 1 lit. a DSGVO.

Unternehmen wäre vorliegend nur dann rechtmäßig gewesen, wenn das Unternehmen für den Kreisverband als Auftragsverarbeiter tätig gewesen wäre. Wesentliches Merkmal der Auftragsverarbeitung ist die Weisungsgebundenheit des Auftragsverarbeiters.[68] Es fehlte an einer Bindung des Dienstleisters an die Weisungen des Kreisverbandes, insbesondere lag kein diesbezüglicher Auftragsverarbeitungsvertrag vor, der z. B. auch eine Verpflichtung zur Löschung der Daten nach Abschluss des Auftrages hätte enthalten müssen. Gegen den Kreisverband verhängten wir daher insgesamt sechs Geldbußen in einer Gesamthöhe von 65.000 Euro.

Personenbezogene Daten gewinnen im Wahlkampf zunehmend an Bedeutung. Daher sollten sich auch Parteien und deren Einheiten mit den datenschutzrechtlichen Grenzen der Wahlwerbung vertraut machen. Aufgrund der hohen Anzahl von Betroffenen und des Umstands, dass gleich gegen mehrere Vorschriften der DSGVO verstoßen wurde, haben wir uns entschlossen, in diesem Fall ein Bußgeld zu verhängen. Dabei haben wir auch berücksichtigt, dass durch die Transparenzverstöße die Betroffenen getäuscht und die Ausübung ihrer Rechte erschwert wurde. Dies wurde auch an den zahlreichen Beschwerden zu dieser Wahlwerbung deutlich. Insbesondere die Offenlegung von amtlichen Daten an einen externen Dienstleiter ohne jegliche Weisungsbefugnis des Kreisverbands einer Partei stellte für uns einen vergleichsweise schweren Verstoß dar. Bußgeldmildernd haben wir u. a. berücksichtigt, dass der Kreisverband mit uns kooperierte und der Verstoß einige Zeit zurücklag.

68 Siehe Art. 28 Abs. 3 lit. a DSGVO.

3. Mitarbeiterexzesse im Gesundheitsbereich

Wir hatten eine Reihe von Fällen, in denen Mitarbeitende im Gesundheitsbereich Patient:innen- bzw. Beschäftigtendaten, auf die sie im Rahmen ihrer arbeitsvertraglichen Tätigkeit berechtigt zugreifen durften, zu privaten Zwecke verwendeten (sog. Mitarbeiterexzess). Die Motivationslage der Mitarbeitenden war dabei unterschiedlich. Wenn Gesundheitsdaten rechtswidrig verarbeitet werden, ahnden wir solche Fälle in der Regel mit Bußgeldern.

Verarbeiten Mitarbeitende im Rahmen ihrer Beschäftigung personenbezogene Daten, wird ihr Handeln nach datenschutzrechtlichen Bestimmungen dem Arbeitgeber als Verantwortlichem zugerechnet. Wenn Beschäftigte hingegen Daten, auf die sie im Arbeitskontext berechtigt zugreifen dürfen, zu eigenen, privaten Zwecken verarbeiten, werden sie selbst zu Verantwortlichen. Da für die Verarbeitung der Daten dann kein beruflicher Anlass besteht, fehlt es auch regelmäßig an einer Rechtsgrundlage, um diese Verarbeitungen zu rechtfertigen.[69] In diesem Jahr haben wir mehrere Bußgeldverfahren gegen Beschäftigte im Gesundheitsbereich wegen solcher Mitarbeiterexzesse geführt.

In einem Verfahren ging es um Filmaufnahmen aus einer Klinik, die ein Mitarbeiter privat aufgenommen und weitergeleitet hatte. Der deshalb von uns erlassene Bußgeldbescheid ist zwischenzeitlich rechtskräftig.

Ein weiteres Bußgeld verhängten wir in diesem Jahr gegen einen Arzt. Dieser rief die Gesundheitsdaten einer ihm fachlich unterstellten Beschäftigten im Krankenhausinformationssystem ohne erkennbaren Grund ab. Derselbe Arzt überprüfte nach einer Krankmeldung seines Assistenzarztes ohne Befugnis auch dessen Infektionsstatus im Krankenhausinformationssystem.

Im vergangenen Jahr verhängten wir zudem ein Bußgeld gegen einen Rezeptionisten in einer psychiatrischen Ambulanz. Dieser verwendete nach mehrfachen erfolglosen Versuchen der Kontaktaufnahme die E-Mail-Adresse einer Patientin, um ihr mitzuteilen, dass er sie bei einem Treffen näher kennenlernen möchte.

69 Siehe Art. 6 Abs. 1 DSGVO.

Rechtswidrige Datenverarbeitungen im Mitarbeiterexzess stellen keine Verstöße des Arbeitgebers dar. Dieser ist jedoch nach Kenntnisnahme unverzüglich zur Meldung des Datenschutzvorfalles verpflichtet, sofern die Anforderungen von Art. 33 Abs. 1 DSGVO gegeben sind. Um das Risiko unbefugter Datenverarbeitungen im Mitarbeiterexzess zu verringern, muss der Arbeitgeber zudem die erforderlichen technisch-organisatorischen Maßnahmen ergreifen. Dazu gehören Maßnahmen, die den Mitarbeitenden verdeutlichen, dass sie personenbezogene Daten nur nach Weisung des Arbeitgebers verarbeiten dürfen, und Maßnahmen, die bspw. das Risiko unbefugter Ausleitung von Daten technisch verhindern. Gerade in Bereichen, in denen besondere Kategorien von personenbezogenen Daten verarbeitet werden, ist es für Arbeitgeber zudem unabdingbar, ihre Mitarbeitende regelmäßig ausführlich zu sensibilisieren und zu schulen.

4. Unzureichende Absicherung eines E-Mail-Postfachs mit Gesundheitsdaten

Unsere Behörde verhängte gegen ein Medizinunternehmen ein Bußgeld wegen eines Verstoßes gegen die Pflicht, geeignete technisch-organisatorische Maßnahmen zur Gewährleistung der Sicherheit bei der Datenverarbeitung zu ergreifen. Das Unternehmen nutzte das E-Mail-Postfach des Geschäftsführers zur Kommunikation mit Patient:innen und Kund:innen. Dieses Postfach war zumindest im Zeitraum von einem Monat über einen Webmail-Zugang erreichbar, ohne dass eine schlüsselbasierte oder Zwei-Faktor-Authentifizierung eingesetzt wurde.

Durch die alleinige Absicherung des Postfachs mit Benutzername und Passwort bestand das Risiko, dass unbefugte Dritte Zugang erlangen und auf die im Postfach gespeicherten personenbezogenen Daten zugreifen konnten. Angesichts der über das Konto abgewickelten Kommunikation, die – wie zu erwarten – auch Gesundheitsdaten beinhaltete, bestand hier ein erhöhter Schutzbedarf. Das Risiko bestätigte sich dann auch, als das Konto kompromittiert und unter Nutzung der bestehenden Kommunikationsverläufe Phishing-Nachrichten versendet wurden.

Das Betreiben eines solchen E-Mail-Postfachs ohne schlüsselbasierte oder Zwei-Faktor-Authentifizierung ist ein Verstoß gegen die Pflicht zur Gewährleistung eines dem

Risiko angemessenen Schutzniveaus nach Art. 32 Abs. 1 lit. b DSGVO. Unter Bezugnahme auf den Stand der Technik, insbesondere auf die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Mehr-Faktor-Authentisierung bei erhöhtem Schutzbedarf,[70] ist hier eine stärkere Authentifizierung als zumutbare und geeignete Maßnahme angeraten.

Bei der Bußgeldzumessung wurde der Verstoß als mittelschwer eingestuft. Erschwerend war insbesondere die Sensibilität der verarbeiteten Gesundheitsdaten zu berücksichtigen. Bußgeldmildernd haben wir das unmittelbare Ändern der Passwörter nach Bekanntwerden des Angriffs, die Kooperation im Verfahren sowie die lange Verfahrensdauer gewürdigt.

70 https://www.bsi.bund.de/dok/1032220.

III. Informationsfreiheit

1. Abschaffung des Lebensmittelüberwachungstransparenzgesetzes

Nachdem das sog. Lebensmittelüberwachungstransparenzgesetz (LMÜTranspG), über das wir in der Vergangenheit wiederholt als positives Beispiel für mehr Transparenz berichtet haben,[71] im Jahr 2023 in Kraft getreten ist, plant der Senat bereits wieder das Aus für die Transparenzvorgaben zu Hygienekontrollen in Restaurants und anderen Lebensmittelbetrieben.[72] Das Gesetz stellte im Bereich der Transparenz staatlichen Wissens und Handelns eine richtungsweisende Neuerung der letzten Jahre in Berlin dar. Wir haben uns daher dafür eingesetzt, dass es beibehalten wird.

Das Gesetz schreibt vor, dass die Bezirksämter die Ergebnisse ihrer Hygienekontrollen im Internet veröffentlichen. Lebensmittelunternehmen sind zudem verpflichtet, diese Ergebnisse in Form einer Farbskala in der Nähe der Eingangstür der Betriebsstätte oder an einer vergleichbaren von außen gut sichtbaren Stelle anzubringen. Mit der Schaffung einer Rechtsgrundlage für die verpflichtende Veröffentlichung der Ergebnisse der amtlichen Lebensmittelkontrolle hat Berlin bundesweit eine Vorreiterrolle eingenommen. Durch die transparente Kommunikation vor dem Betreten von Bäckereien, Gaststätten und anderen Lebensmittelbetrieben können sich Verbraucher:innen besser über den dortigen Hygienezustand informieren und vor unsicheren Lebensmittelangeboten schützen.

Mit Verweis auf die Überlastung der Behörden möchte der Senat das Gesetz nun nach nicht einmal drei Jahren Gültigkeit wieder abschaffen. Wir haben empfohlen, das LMÜTranspG im Hinblick auf etwaige Aspekte, die sich in der Praxis als zu aufwändig erwiesen haben, anzupassen, aber die Transparenzverpflichtungen nicht vollständig abzuschaffen. Lebensmittelkontrollen müssen sowieso durchgeführt werden und die Veröffentlichung der Ergebnisse könnten auch durch Automatisierung unterstützt werden.

71 JB 2020, 19.2.3; JB 2021, 17.2.1; JB 2022, 16.3.

72 Siehe Entwurf des Gesetzes zur Aufhebung des Lebensmittelüberwachungstransparenzgesetzes vom 9. Oktober 2025, Abghs.-Drs. 19/2702.

Zu berücksichtigen ist zudem, dass auch nach Abschaffung des LMÜTranspG weiterhin Transparenz über Informationsanfragen auf Grundlage des Verbraucherinformationsgesetzes (VIG) eingefordert werden kann. Aufgrund der dann fehlenden proaktiven Veröffentlichung von Informationen könnte das in der Summe einen größeren Verwaltungsaufwand zur Folge haben. Zudem zeigt Dänemark, dass ein Mehr an Transparenz bei der Lebensmittelkontrolle zu einer geringeren Beanstandungsquote und damit im Ergebnis zu weniger Aufwand bei den Kontrolleur:innen führen kann.[73] Das LMÜTranspG könnte bei vollständiger Umsetzung die Verwaltung dann sogar entlasten.

Das LMÜTranspG sollte nicht abgeschafft, sondern auf Grundlage der bisher gewonnen Erkenntnisse evaluiert und überarbeitet werden. Die proaktive Veröffentlichung von Informationen kann nicht nur einen transparenten Staat und die Teilhabe von Bürger:innen voranbringen. Sie kann auch die Verwaltung selbst entlasten; sei es, indem die Verwaltung schnell und unbürokratisch selbst an Informationen anderer Ressorts gelangt, oder sei es, weil etwa transparent gemachte aufsichtsbehördliche Tätigkeit zur besseren Umsetzung der Gesetze durch die Beaufsichtigten führt.

2. Geplante gesetzliche Beschränkungen der Reichweite der Informationsfreiheit

Während im aktuellen Koalitionsvertrag der Regierungsparteien Reformversprechen in Bezug auf das aus dem Jahr 1999 stammende Berliner Informationsfreiheitsgesetz (IFG) hin zu einem modernen Transparenzgesetz formuliert sind, hat die Senatsverwaltung für Inneres und Sport uns in diesem Jahr über gegenläufige Reformbestrebungen in Kenntnis gesetzt. Es ist geplant, die Ausschlussgründe des IFG zum Schutz öffentlicher Belange in erheblichem Umfang auszudehnen. Diesen Bestrebungen zur Begrenzung von möglichen Informationsansprüchen sind wir in mehreren Stellungnahmen entgegengetreten.

Zukünftig sollen bspw. sämtliche Vorgänge der Steuerverwaltung umfassend von der Informationspflicht ausgenommen werden. Gründe für eine solche Sonderbehandlung

73 Siehe Bericht von foodwatch e. V. vom 29. März 2017: „Dänemark: Smiley-System sorgt für weniger Beanstandungen“, abrufbar unter https://www.foodwatch.org/de/informieren/politik-lobby/lebensmittelkontrollen/vorbild-daenemark.

sind nicht ersichtlich. Auch Vorgänge der Steuerverwaltung können von öffentlichem Interesse sein, z. B. allgemeine Dienstanweisungen sowie Steuerberechnungsmodelle in den Finanzämtern. Im Hinblick auf schützenswerte Interessen des Einzelnen sieht das IFG[74] im Übrigen vor, dass das bundesgesetzlich geregelte Steuergeheimnis[75] beim Informationszugang Berücksichtigung findet. Insoweit sind also bereits jetzt nach Berliner Landesrecht Steuerpflichtige davor geschützt, dass Informationen, die sie in Erfüllung ihrer steuerlichen Offenbarungs- und Auskunftsverpflichtungen der Finanzverwaltung preisgeben müssen, außerhalb des Besteuerungsverfahrens bekannt werden.

Weiterhin soll die Informationsfreiheit pauschal und dauerhaft bei Geheimhaltungs- und Vertraulichkeitsvorschriften bzw. -anordnungen und -kennzeichnungen eingeschränkt werden. Auch diese Regelungen sind nicht erforderlich, weil die bestehenden Regelungen des IFG, die öffentliche Interessen schützen, insofern bereits hinreichende Ausschlussgründe bieten.[76] Für sicherheitskritische Informationen informationstechnischer Systeme wird bspw. regelmäßig anzunehmen sein, dass deren Offenbarung eine schwerwiegende Gefährdung des Gemeinwohls zur Folge hätte, weshalb insoweit kein Informationsrecht besteht.

Besonders problematisch ist in diesem Zusammenhang der geplante Ausschluss von Informationen, „die [...] als vertraulich zu behandeln besonders gekennzeichnet sind“. Eine vergleichbar weite Regelung existiert aus guten Gründen in keinem der beispielhaft im Rahmen der Gesetzesbegründung aufgeführten Informationsfreiheits- bzw. Transparenzgesetze. Unklar bleibt insbesondere, welche Anforderungen an eine solche Kennzeichnung zu stellen sind. Es besteht insoweit die Gefahr der uferlosen Ausdehnung des Geheimnisschutzes durch die Verwaltung; ggf. auch, um Unterlagen dem Informationsfreiheitsrecht zu entziehen.

Eine Reform des IFG ist nach über 30 Jahren zwar angezeigt, allerdings hin zu einem modernen Transparenzgesetz mit proaktiven Veröffentlichungspflichten. Die geplanten Gesetzesanpassungen sind ein erheblicher Rückschritt für die Transparenz staatlichen Handelns.

74 § 17 Abs. 4 IFG.
75 Steuergeheimnis nach § 30 Abgabenordnung (AO).
76 Siehe §§ 9 bis 11 IFG.

3. Mehr Transparenz bei Umweltinformationen

In diesem Jahr erreichten uns mehrere Beschwerden von Personen, die zunächst erfolglos Informationszugangsanträge mit direktem oder indirektem Bezug zum Klima- bzw. Umweltschutz bei Behörden, aber auch bei landeseigenen Unternehmen gestellt hatten. Wir nehmen dies zum Anlass, auf eine Berliner Besonderheit im Landesrecht hinzuweisen, die bereits seit 20 Jahren gilt, aber von den Adressat:innen der Offenlegungsanträge in aller Regel übersehen wird.

Nach der Sonderregelung in § 2 Abs. 2 IFG bestimmt sich der Zugang zu Informationen über die Umwelt nach den Regelungen in § 18a IFG, der wiederum in Abs. 1 auf das Umweltinformationsgesetz (UIG) verweist.[77] Das bedeutet, dass die materiell-rechtlichen Bestimmungen des UIG im Land Berlin entsprechend gelten – und zwar sowohl im Hinblick auf öffentliche informationspflichtige Stellen als auch im Hinblick auf private informationspflichtige Stellen.[78]

Entscheidend ist zunächst, welche Art von Informationen beantragt sind. Handelt es sich um „allgemeine" Informationen (also nicht um Umweltinformationen), ist nach derzeitiger Rechtslage kein Informationszugang bei landeseigenen Unternehmen möglich, und zwar auch dann nicht, wenn das Land Berlin öffentliche Aufgaben auf diese Unternehmen übertragen hat. Denn sie unterliegen auch in solchen Fällen nicht dem IFG – eine Regelungslücke, die der Gesetzgeber noch immer nicht geschlossen hat. Die mit einer Aufgabenübertragung einhergehende „Flucht ins Privatrecht" kritisieren wir seit langem.[79]

Anders sieht es aus, wenn die Offenlegung von Umweltinformationen beantragt ist, wobei Antragstellende sie nicht als solche bezeichnen müssen. Nach der inzwischen höchstrichterlich etablierten Definition ist der Begriff denkbar weit zu verstehen und umfasst alle Informationen, die einen auch nur mittelbaren Bezug zur Umwelt aufweisen.[80] Dazu gehören u. a. Tätigkeiten, die sich auf Umweltbestandteile wie Luft, Wasser

77 Ausgenommen sind die §§ 11 bis 14 UIG, die u. a. Verfahrens- und Gebührenvorschriften vorsehen.
78 Das ergibt sich aus § 18a Abs. 2, 3 und 5 IFG.
79 Siehe zuletzt JB 2017, 15.2.2.
80 Siehe BVerwG, Urteil vom 23. Februar 2017, 7 C 31.15, Rn. 55.

oder Boden wahrscheinlich auswirken.[81] Es genügt zudem die Bezugnahme auf das IFG als Rechtsgrundlage, weil § 18a IFG – als Sonderregelung für Umweltinformationen und Rechtsgrundverweisung auf das UIG – Bestandteil des IFG ist. Insofern können in Berlin ansässige bzw. landeseigene Unternehmen nicht pauschal darauf verweisen, dass sie nicht dem Anwendungsbereich des IFG unterliegen, denn die angefragte Stelle muss bei einem IFG-Antrag als Erstes – gewissermaßen die „Einstiegsfrage" – klären, ob es sich bei den angefragten Informationen um solche mit Umweltbezug handelt. Geht es um Umweltinformationen bei einer juristischen Person des Privatrechts, muss diese prüfen, ob sie private informationspflichtige Stelle i. S. d. UIG[82] ist. Das dürfte in jedem Fall bei hundertprozentig landeseigenen Unternehmen, die umweltbezogen agieren und der Kontrolle des Landes Berlin unterliegen, zu bejahen sein.[83]

Einem Zugang zu Umweltinformationen können Ausschlusstatbestände des UIG[84] entgegenstehen. Es handelt sich beim UIG um vorrangiges Bundesrecht. Die landesrechtlichen Ausschlusstatbestände des IFG[85] sind auf den Zugang zu Umweltinformationen daher nicht ergänzend anwendbar.[86]

Zu beachten ist, dass die Bescheidung des Antrages auf Zugang zu Umweltinformationen grundsätzlich binnen Monatsfrist erfolgen muss.[87] Idealerweise wäre Anfragenden die Akteneinsicht in die Umweltinformationen vor Ort anzubieten, zumal eine solche

81 Siehe § 2 Abs. 3 Nr. 3a i. V. m. Nr. 1 UIG.

82 § 2 Abs. 1 Nr. 2 UIG.

83 Bei landeseigenen Unternehmen, die in ihren Publikationen und auf ihrer Website z. B. mit dem Aufgabengebiet Klimaschutz werben, liegt insoweit die Vermutung nahe, dass dort angefragte Informationen auf der Grundlage des § 18a IFG i. V. m. UIG offenzulegen sind. Siehe beispielhaft die Aussage der Grün Berlin GmbH auf ihrer Website unter dem Titel „Nachhaltige Stadtentwicklung für Berlin ... Wir entwickeln, bauen und betreiben nachhaltige grüne und blaue Infrastrukturen für Berlin."

84 §§ 8, 9 UIG.

85 §§ 6 ff. IFG.

86 Siehe VG Berlin, Urteil vom 10. Mai 2021, 2 K 220/19, Rn. 57: „Mit Ausnahme der Regelungen in § 18a Abs. 2 – Abs. 5 IFG sind die Vorschriften des IFG nicht anwendbar. Ein punktueller Rückgriff auf einzelne landesrechtliche Ausschlussgründe ist weder nach Wortlaut, Systematik oder Entstehungsgeschichte geboten und stünde der von dem Gesetzgeber bezweckten Schaffung bundeseinheitlicher Regelungen über den Zugang zu Umweltinformationen (Abghs.-Drs. 15/4227, S. 2) entgegen."

87 Ausnahmsweise auch binnen zwei Monaten; siehe § 3 Abs. 3 Satz 2 und § 5 Abs. 1 Satz 1 UIG.

gebührenfrei ist,[88] und zwar auch dann, wenn die angefragte Stelle zuvor erforderliche Vorbereitungshandlungen durchführen muss.[89]

Für Streitigkeiten und Ansprüche gegen private informationspflichtige Stellen ist der Rechtsweg zu den Verwaltungsgerichten gegeben.[90] Unsere Kontrollbefugnis erstreckt sich nicht auf diese Stellen, sondern besteht lediglich in Bezug auf die öffentlichen Stellen des Landes Berlin.[91]

Der jüngst vom Senat beschlossene Klimapakt 2025–2030 sieht im Übrigen eine Vereinbarung mit 22 landeseigenen Unternehmen vor, die bis 2030 rund 13,8 Milliarden Euro in den Klimaschutz investieren müssen. Bis dahin stellt ihnen der Senat zusätzlich 2,3 Milliarden Euro zur Verfügung.[92] Einzelheiten zu diesem Klimapakt und dazu, welche 22 der zahlreichen landeseigenen Unternehmen[93] konkret beteiligt sind, waren bis Redaktionsschluss nicht allgemein bekannt.

Umweltinformationen – insbesondere solche zum Klimaschutz – sind von wachsender Bedeutung für die Menschheit[94] und von den informationspflichtigen öffentlichen und privaten Stellen entsprechend zu behandeln. Die Rechtsgrundlagen für die erforderliche Transparenz sind seit zwei Jahrzehnten im Landesrecht angelegt und müssen konsequent angewendet werden. Insofern können auch juristische Personen des Privatrechts, insbesondere hundertprozentig landeseigene Unternehmen, informationspflichtige Stellen sein, die auf einen IFG-Antrag reagieren müssen.

88 Siehe § 18a Abs. 4 Satz 3 Nr. 1 IFG; bei privaten informationspflichtigen Stellen i. V. m. § 18a Abs. 5 Satz 1, 2. Hs. IFG.

89 Z. B. Schwärzung schutzbedürftiger Informationen; vgl. VG Mainz, Urteil vom 5. April 2017, 3 K 569/16.MZ.

90 Siehe § 6 Abs. 5 UIG i. V. m. § 18a Abs. 3 IFG. Zum vorgerichtlichen Verfahren siehe § 6 Abs. 3 und 4 UIG.

91 Siehe § 18 Abs. 2 Satz 1 IFG.

92 Pressemitteilung der Senatskanzlei vom 18. November 2025: „Senat beschließt Klimapakt in Milliardenhöhe“, abrufbar unter https://www.berlin.de/rbmskzl/aktuelles/pressemitteilungen/2025/pressemitteilung.1617589.php.

93 Eine Übersicht mit den sog. Beteiligungsunternehmen des Landes Berlin ist im Internetauftritt der Senatsverwaltung für Finanzen veröffentlicht und abrufbar unter https://www.berlin.de/sen/finanzen/vermoegen/beteiligungen/beteiligungsunternehmen/.

94 Siehe auch D.III.1.

4. Gebührenfreie Akteneinsicht in Umweltinformationen vor Ort

Ein Bürger beantragte zunächst bei der Senatsverwaltung für Mobilität, Verkehr, Klimaschutz und Umwelt Akteneinsicht in den Genehmigungsvorgang zu einem festliegenden Schiff samt Gutachten zur Umweltverträglichkeit. Da er seinen IFG-Antrag später jedoch wieder zurücknahm, vereinbarte er mit der Verwaltung, dass im Gegenzug die Gebühr in Höhe von 60 Euro für die vor Ort angebotene, aber nicht wahrgenommene Akteneinsicht von der Verwaltung ebenfalls zurückgenommen wird. Zwar erfolgte die zugesagte Gebührenrücknahme; allerdings verlangte die Verwaltung nun eine Gebühr in Höhe von 30 Euro „für die Rücknahme des Antrages".

Wir haben der zuständigen Verwaltung mitgeteilt, dass es sich bei den angefragten und für die Akteneinsicht vorgesehenen Informationen um sog. Umweltinformationen handelt. Dieser Begriff ist laut Bundesverwaltungsgericht (BVerwG) weit auszulegen und umfasst alles, was ggf. auch nur mittelbare Auswirkungen auf die Umwelt haben kann.[95] Das war bei der in Rede stehenden Akte zum festliegenden Schiff der Fall. Der Antrag wurde vom Bereich „Gewässerschutz" in der Abteilung „Integrativer Umweltschutz, Wasserbehörde" der angefragten Senatsverwaltung bearbeitet.

Die Akteneinsicht in Umweltinformationen vor Ort ist gebührenfrei.[96] Die zunächst festgesetzte, aber später zurückgenommene Gebühr in Höhe von 60 Euro war also bereits unzulässig; die Vorlage der begehrten Akte in einem Ortstermin hätte gebührenfrei erfolgen müssen. Wenn aber für die beantragte Amtshandlung – die Offenlegung der Akte zum Schiff – keine Gebühr erhoben werden durfte, ist nicht nachvollziehbar, warum bei Rücknahme des Antrages eine anteilige Gebühr[97] in Betracht kommen sollte. Vor diesem Hintergrund war der nachgeschobene Gebührenbescheid in Höhe von 30 Euro aufzuheben.

Öffentliche Stellen, die Vorgänge mit Umweltinformationen führen, sollten bei diesbezüglichen Informationszugangsanträgen von sich aus auf die Möglichkeit der gebührenfreien Akteneinsicht vor Ort hinweisen.

95 Siehe BVerwG, Urteil vom 23. Februar 2017, 7 C 31.15, Rn. 55.; siehe auch B.III.3.
96 § 18a Abs. 4 Satz 3 Ziff. 1 IFG; siehe auch B.III.3.
97 Siehe § 6 Abs. 1 Satz 2 Verwaltungsgebührenordnung (VGebO).

5. Fehler bei der Antragsbearbeitung durch die Senatsverwaltung für Finanzen

Ein Bürger beantragte bei der Senatsverwaltung für Finanzen eine Übersicht aller bestehenden Verträge zur Auftragsdatenverarbeitung, die das Land Berlin mit dem Technischen Finanzamt (TFA) Cottbus abgeschlossen hat. Auch wesentliche Vertragsinhalte wie z. B. die Bezeichnung der jeweiligen Auftragsverarbeiter sowie Laufzeiten und Kündigungsregelungen sollten offengelegt werden. Die Senatsverwaltung lehnte dies ab. Der IFG-Antrag beziehe sich auf Akteninhalte über Angaben und Mitteilungen mit unmittelbarem Bezug zum TFA Cottbus, eine öffentliche Stelle des Landes Brandenburg, die nicht in den Anwendungsbereich des IFG falle. Der Bürger erhob gegen die Ablehnung seines Antrags Widerspruch und wandte sich zusätzlich hilfesuchend an uns.

Nach § 10 Abs. 3 Nr. 2 IFG, auf den sich die Senatsverwaltung bei der Ablehnung berief, besteht das Recht auf Akteneinsicht oder -auskunft nicht, soweit durch das Bekanntwerden des Akteninhalts Angaben und Mitteilungen öffentlicher Stellen, die nicht dem Anwendungsbereich des IFG unterfallen, ohne deren Zustimmung offenbart werden. Wir haben die Senatsverwaltung darauf hingewiesen, dass sie sich nur dann auf diesen Ablehnungsgrund berufen kann, wenn sie erfolglos versucht hat, die Zustimmung des TFA Cottbus zu erhalten.[98] Ein solcher Versuch wurde offenbar nicht unternommen, sodass wir gebeten haben, dies nachzuholen. Auch wiesen wir darauf hin, dass in jedem Fall zu prüfen ist, ob ein teilweiser Informationszugang gem. § 12 IFG möglich ist, also trotz womöglich verweigerter Zustimmung Informationen zugänglich gemacht werden können, die keine Angaben und Mitteilungen des TFA Cottbus i. S. v. § 10 Abs. 3 Nr. 2 IFG darstellen. Denkbar war dies z. B. im Hinblick auf die Titel der Verträge bzw. die jeweiligen Vertragsgegenstände, die in der beantragten Übersicht hätten benannt werden können.

Die Senatsverwaltung für Finanzen hat dem Widerspruch nach ca. drei Monaten abgeholfen, weil sich herausstellte, dass zwischen dem Land Berlin und dem TFA Cottbus keine Verträge zur Auftragsdatenverarbeitung bestehen.

98 Siehe OVG Berlin-Brandenburg, Urteil vom 11. März 2008, OVG 12 B 1.07, abrufbar unter https://www.juris.de/perma?d=NJRE000903130, Rn. 18.

Wir empfehlen, die Offenlegung unter Bezugnahme auf IFG-Ausschlusstatbestände erst dann zu verweigern, wenn zuvor geprüft wurde, ob und wenn ja welche der beantragten Unterlagen im Aktenbestand der Verwaltung vorhanden sind. Darüber hinaus muss bei Angaben und Mitteilungen anderer Behörden, die nicht dem IFG unterliegen, zumindest der Versuch unternommen werden, die Zustimmung zur Offenlegung zu erlangen.

6. Offenlegung von Prüfungsunterlagen durch die Charité

Ein Bürger beschwerte sich bei uns darüber, dass sein IFG-Antrag auf Offenlegung von Aufgaben und Lösungen einer zurückliegenden medizinischen Semesterabschlussklausur von der Charité abgelehnt worden war. Zur Begründung führte die Charité an, dass die angefragten Informationen kein eigenständiger Aktenteil seien, sondern sich im Vorgang zum jeweiligen Prüfling befänden. Zudem sei der Informationszugang durch die in § 9 IFG normierten Ausschlussgründe gesperrt, da die Antwort-Wahl-Aufgaben und deren Lösungen zur wiederholten Verwendung vorgesehen seien und durch die Bekanntgabe derselben ihren Zweck nicht mehr erfüllen können. Dadurch seien die Funktionsfähigkeit und die effektive Aufgabenerfüllung staatlicher Einrichtungen in Form eines funktionierenden Prüfungswesens berührt.

Wir haben der Charité mitgeteilt, dass ein (dauerhaftes) Vorenthalten der gewünschten Informationen aus Gründen der Praktikabilität wünschenswert sein mag, jedoch nach geltender Rechtslage nicht haltbar ist. Die beabsichtigte Wiederverwendung der Aufgabentexte und Musterlösungen sprach aus unserer Sicht zudem bereits dafür, dass die begehrten Informationen in einer gesonderten (General-)Akte[99] nicht personenbezogen abgelegt sein müssen und damit grundsätzlich dem IFG unterliegen. Der Hinweis darauf, dass der begehrte Informationszugang „durch die in § 9 IFG normierten Ausschlussgründe gesperrt wäre“, war zu pauschal. Es fehlte die konkrete Bezugnahme auf einen der Ausschlussgründe in Abs. 1 des § 9 IFG, bei dessen Bejahung im Übrigen die Vorgaben von Abs. 2 des § 9 IFG zu beachten gewesen wären. Der

99 Siehe § 3 Abs. 2 IFG.

Hinweis auf die Funktionsfähigkeit und die effektive Aufgabenerfüllung staatlicher Einrichtungen in Form eines funktionierenden Prüfungswesens passte zu keinem dieser Ausschlussgründe.

Die Charité änderte ihre Auffassung im Ergebnis nicht und wies den Widerspruch des Beschwerdeführers zurück.

Anders als etwa in Brandenburg[100] hat der Landesgesetzgeber in Berlin keine generelle Bereichsausnahme für sämtliche Prüfungseinrichtungen und deren Prüfungsunterlagen vorgesehen. Eine Sonderregelung gilt im Land Berlin allein für Prüfungen beim Gemeinsamen Juristischen Prüfungsamt der Länder Berlin und Brandenburg.[101]

100 Siehe § 2 Abs. 2 Satz 2 Akteneinsichts- und Informationszugangsgesetz (AIG).
101 Siehe § 23 Abs. 3 Berliner Juristenausbildungsgesetz (JAG).

IV. Künstliche Intelligenz

1. KI in der Berliner Verwaltung

Auch in diesem Jahr haben wir uns mit unserer Expertise an der von der Senatskanzlei eingesetzten Taskforce KI[102] beteiligt. Insbesondere haben wir uns in die neu gegründete Unterarbeitsgruppe (UAG) Datenschutz eingebracht. Wesentliche Themen waren die Erarbeitung einer Rechtsgrundlage für die Nutzung von KI-Systemen durch die Berliner Verwaltung sowie die Analyse von risikomindernden technischen und organisatorischen Maßnahmen. Darüber hinaus berieten wir die Verwaltung bei Projekten, in denen KI-Systeme zum Einsatz kommen sollen.

Eigenständige Rechtsgrundlage für den Einsatz von KI-Systemen

Unter Berücksichtigung der Positionen des Europäischen Datenschutzausschusses (EDSA) zur Verarbeitung personenbezogener Daten in KI-Systemen[103] haben wir die Senatskanzlei zur Notwendigkeit einer separaten Rechtsgrundlage für die Verarbeitung personenbezogener Daten bei der Nutzung von KI-Systemen durch die Verwaltung beraten.

Zentral war für uns dabei, wesentliche risikominimierende Maßnahmen, die im nichtöffentlichen Bereich aufgrund von Anforderungen aus der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f Datenschutz-Grundverordnung (DSGVO) zu implementieren sind, für das Land Berlin gesetzlich zu verankern.[104] Wichtig ist in diesem Zusammenhang die Nichtveränderbarkeit des KI-Modells durch die Verarbeitung personenbezogener Daten. Hierdurch wird sichergestellt, dass die Daten nur für den konkreten

102 Siehe JB 2024, A.IV.1.

103 Siehe EDSA, Stellungnahme Nr. 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_de; siehe auch JB 2024, C.I.4.

104 Nach Art. 6 Abs. 1 Satz 2 DGSVO gilt Art. 6 Abs. 1 lit. f DSGVO nicht für Behörden bei der Verarbeitung personenbezogener Daten in Erfüllung ihrer Aufgaben.

Anwendungsfall genutzt werden. Außerdem werden so unkontrollierbare Lerneffekte, die Entstehung von Verzerrungen (Bias) und eine Zweckentfremdung der Daten als Trainingsmaterial verhindert. Zusätzlich war es uns wichtig, die Erfüllung der datenschutzrechtlichen Gewährleistungsziele explizit im Gesetzeswortlaut zu verankern und der Verwaltung damit die Bereiche und Zielsetzungen aufzuzeigen, die je nach KI-System mit entsprechenden risikominimierenden Maßnahmen abzudecken sind.

Die für das Gesetzgebungsverfahren zur Schaffung einer KI-Rechtsgrundlage im Berliner E-Government-Gesetz (EGovG Bln) federführende Senatskanzlei hat zwar wesentliche, jedoch nicht alle von uns unterbreiteten Vorschläge in die Regelung aufgenommen. Besonders wichtig ist es für uns, dass die Behörden KI-Systeme einsetzen, die für sie auch beherrschbar sind, und sie die Kontrolle über die darin verarbeiteten personenbezogenen Daten als Verantwortliche behalten, damit die Rechte und Freiheiten der betroffenen Personen dauerhaft gewährleistet werden können.

Wir begrüßen es sehr, dass die Senatskanzlei uns so frühzeitig beteiligt und die Anpassung des EGovG Bln kurzfristig in das parlamentarische Gesetzgebungsverfahren eingebracht hat.[105] Gleichwohl bedauern wir, dass die von uns vorgeschlagene Evaluationsklausel nicht in den Gesetzestext übernommen wurde. Wir hätten eine gesetzliche Festschreibung etwa zur Neubewertung von Risiken in dem sehr dynamischen und von rasanter technischer Fortentwicklung geprägten KI-Bereich für äußerst sinnvoll erachtet.

Neben der Schaffung einer Rechtsgrundlage für den Einsatz von KI-Systemen in § 16a EGovG Bln ist auch eine Änderung des Berliner Datenschutzgesetzes (BlnDSG)[106] geplant, die die Norm für unsere Behörde, die aufgrund ihrer Unabhängigkeit nicht dem unmittelbaren Anwendungsbereich des EGovG Bln[107] unterliegt, für entsprechend anwendbar erklärt und es damit auch uns ermöglicht, personenbezogene Daten in einem KI-System zu verarbeiten.

105 Abghs.-Drs. 19/2823.
106 Konkret des § 13 Abs. 6 Satz 3 BlnDSG.
107 Siehe § 1 Abs. 1 EGovG Bln i. V. m. § 1 Abs. 3 Landesorganisationsgesetz Berlin (LOG).

Notwendige technisch-organisatorische Maßnahmen für KI-Assistenzsysteme

In der UAG Datenschutz der Taskforce KI wurden auch die wesentlichen datenschutzrechtlichen Herausforderungen für KI-Assistenzsysteme diskutiert. Im Fokus stand für uns dabei, auf Maßnahmen zur Verringerung von Datenschutzrisiken aufmerksam zu machen (mitigierende Maßnahmen). Sie sind notwendig, um einen datenschutzkonformen Einsatz großer Sprachmodelle (Large Language Models, kurz LLMs), deren Training mit personenbezogenen Daten nicht vollständig nachvollziehbar und rechtlich bewertbar ist, innerhalb solcher Systeme überhaupt ermöglichen zu können. Orientiert haben wir uns an der Stellungnahme des EDSA zur Verarbeitung personenbezogener Daten in KI-Modellen.[108] Der EDSA weist darauf hin, dass unter bestimmten Bedingungen der datenschutzkonforme Einsatz eines potenziell rechtswidrig trainierten KI-Modells möglich sein kann. Voraussetzung hierfür sind risikomindernde technische und organisatorische Maßnahmen, die für das Gesamtsystem, in das ein solches Modell integriert ist, die Gewährleistung eines angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten ermöglichen.

Die Entwicklung eines KI-Assistenten erfolgt idealerweise modellunabhängig. Da bei den heute am Markt verfügbaren Modellen nicht ausgeschlossen werden kann, dass ein Modell rechtswidrig trainiert worden ist, müssen Entwickler:innen risikomindernde technische und organisatorische Maßnahmen i. S. d. Datenschutzes durch Technikgestaltung[109] von Anfang an mitdenken.

Ein erster Anwendungsfall eines solchen KI-Assistenzsystems in der Berliner Verwaltung ist BärGPT. Es soll ermöglichen, Texte zu erstellen, Übersetzungen zu fertigen oder auf spezifisches Berliner Verwaltungswissen zuzugreifen. Darüber hinaus soll das System Funktionen zur Text- und Dokumentenanalyse haben, die es erlauben, innerhalb von Dateien semantisch nach Inhalten und Zusammenhängen zu suchen. BärGPT wird

108 Siehe EDSA, Stellungnahme Nr. 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_de; siehe auch JB 2024, C.I.4.

109 Siehe Art. 25 DSGVO; DSK, Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen, Stand: Juni 2025, abrufbar unter https://www.datenschutzkonferenz-online.de/orientierungshilfen.html.

durch das CityLAB, ein durch die Technologiestiftung Berlin betriebenes und von der Senatskanzlei gefördertes Innovationslabor, in Kooperation mit der Senatskanzlei entwickelt und steht seit November 2025 im Probeechtbetrieb zu Verfügung, zunächst ohne dass personenbezogene Daten darin verarbeitet werden dürfen.

Im Fall von BärGPT haben wir gemeinsam in der UAG Datenschutz anhand der konzeptionellen Architektur der Anwendung sowie der geplanten Funktionalitäten vorhersagbare Risiken bei der Verarbeitung personenbezogener Daten herausgearbeitet. Mithilfe des Standard-Datenschutzmodells (SDM) haben wir anschließend technische und organisatorische Maßnahmen identifiziert, die geeignet scheinen, diese Risiken bezüglich der Gewährleistungsziele Vertraulichkeit, Verfügbarkeit, Transparenz, Nichtverkettbarkeit, Integrität, Intervenierbarkeit und Datenminimierung maßgeblich zu mindern. Wir werden die Weiterentwicklung des KI-Assistenten datenschutzrechtlich begleiten und mit Erlass der neuen Rechtsgrundlage prüfen, ob die Anforderungen eingehalten werden und folglich auch personenbezogene Daten mit BärGPT verarbeitet werden dürfen.

Datenschutzrechtliche Beratung bei der Einführung von KI-Projekten

In der Taskforce KI haben wir einen Überblick über einige der (geplanten) Einsatzszenarien von KI-Systemen in der Verwaltung gewonnen. Zum einen geht es um universelle Arbeitshilfen, wie z. B. die Zusammenfassung von Dokumenten und die Erstellung von Vermerken. Zum anderen sollen Fachverfahren um KI-Assistenten ergänzt werden. Immer wieder hat sich auch gezeigt, dass es der Verwaltung wichtig ist, beim Einsatz der für die Behörden neuen Technologie von vornherein die Datenschutzanforderungen zu berücksichtigen.

Um unsere beschränkten personellen Ressourcen bei der Beratung solcher Projekte gezielt einsetzen zu können, legen wir Projektverantwortlichen nahe, die datenschutzrechtlichen Themen zunächst auf der Grundlage unseres Standardprozesses Datenschutz bei öffentlichen Digitalisierungsvorhaben[110] selbstständig zu bearbeiten und unsere Beratung bei ungeklärten oder für die Verwaltung nicht allein lösbaren Fragen

110 Siehe JB 2024, A.VI.2.

in Anspruch zu nehmen. Dieser Prozess ist auch für Projekte, in denen es um die Einführung von KI-Systemen geht, geeignet. Es stellen sich dort im Wesentlichen die gleichen Fragen wie bei herkömmlichen Digitalisierungsprojekten. Werden keine personenbezogenen Daten verarbeitet, findet die DSGVO keine Anwendung und es stellen sich in der Regel keine datenschutzrechtlichen Folgefragen. Werden jedoch potenziell personenbezogene Daten im KI-System verarbeitet, muss u. a. geklärt werden, welche Institution welche personenbezogenen Daten zu welchen Zwecken verarbeitet.

Ist beim Einsatz eines KI-Systems zur Verarbeitung personenbezogener Daten von einem voraussichtlich hohen Risiko auszugehen, muss eine Datenschutz-Folgenabschätzung durchgeführt werden.[111] Bezüglich jeder Verarbeitung personenbezogener Daten muss geprüft werden, wie das damit einhergehende Risiko mittels technischer und organisatorischer Maßnahmen reduziert werden kann.

Das EGovG Bln wird um eine Rechtsgrundlage für den Einsatz von KI-Systemen ergänzt. Sie soll für eine rechtssichere Verarbeitung personenbezogener Daten sorgen, unter der Maßgabe, diese Verarbeitung durch risikomindernde technische und organisatorische Maßnahmen zu flankieren, die ein angemessenes Schutzniveau gewährleisten. Von der Verwaltung eingesetzte KI-Systeme und geplante Projekte mit KI-Komponenten werden künftig dahingehend zu bewerten sein, ob sie neben den allgemeinen Anforderungen der DSGVO auch diese neu geschaffenen landesrechtlichen Vorgaben erfüllen.

111 Siehe Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO, für die gemäß Art. 35 Abs. 1 DSGVO eine Datenschutz-Folgenabschätzung von Verantwortlichen im öffentlichen Bereich durchzuführen ist, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/dokumente/2018-BlnBDI_DSFA-oeffentlich.pdf.

2. Anonymisierung und Transparenz beim KI-Training

Um die Zahlungsquote im Inkassoverfahren zu erhöhen, werden durch die Einbeziehung von Verhaltensforschung und KI personenbezogene Daten von Schuldner:innen verarbeitet, um herauszufinden, was der passende Kanal, der richtige Ton und die richtige Uhrzeit sind, um sie individuell anzusprechen. Dies soll die Kund:innenbeziehung schonen und Kosten senken. Eine unserer Prüfungen zeigte hierbei jedoch Mängel beim Datenschutz.

Ein Unternehmen verwendet Schuldner:innendaten KI-gestützt nicht nur zum eigentlichen Forderungsmanagement. Die Personen-, Forderungs- und Nutzungsdaten werden in einer speziellen Analyse-Umgebung vielmehr auch zum Training bzw. zur Optimierung der vom Unternehmen eingesetzten KI-Modelle weiterverwendet. Im Zuge einer Vor-Ort-Prüfung bei dem Unternehmen haben wir uns dies genauer angeschaut und dabei verschiedene Verstöße gegen die DSGVO festgestellt.

Ein Verstoß betraf das Transparenzdefizit bei der Verwendung der Schuldnerdaten zum Zwecke des KI-Trainings.[112] Die Schuldner:innen erhielten zwar mit Versand einer ersten Zahlungsaufforderung per Brief oder E-Mail einen Datenschutzhinweis, der sich – da die betreffenden Daten nicht direkt bei den betroffenen Personen, sondern in erster Linie bei den beauftragenden Gläubiger:innen erhoben wurden – nach Art. 14 DSGVO richtet. Das Unternehmen informierte dort jedoch nicht darüber, dass eine Weiterverarbeitung der Schuldner:innendaten zweckändernd auch erfolgt, um die von dem Unternehmen eingesetzten KI-Modelle zu trainieren bzw. zu optimieren. Eine solche Information erfolgte erst in der Website-Datenschutzerklärung, auf die in dem Datenschutzhinweis verwiesen wurde, die aber nicht bereits in dem ersten Datenschutzhinweis selbst enthalten war.

Zwar können Verantwortliche mit sog. Mehrebenen-Datenschutzhinweisen den Transparenzanforderungen der DSGVO genügen. Die wichtigsten Informationen müssen aber mit der ersten Kontaktaufnahme auf erster Ebene vermittelt werden. Das sind insbesondere die Einzelheiten zu Verarbeitungszwecken zusammen mit den Informationen über die wichtigsten Auswirkungen der Verarbeitung bzw. Verarbeitungsvorgänge, mit denen

112 Siehe Art. 25 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO.

die betroffenen Personen möglicherweise nicht rechnen.[113] Das Unternehmen hätte bereits mit dem Datenschutzhinweis in der ersten Zahlungsaufforderung[114] darüber informieren müssen, dass Schuldnerdaten auch zum KI-Training verwendet werden. Für die betroffenen Personen war nicht damit zu rechnen, dass das Unternehmen, das in keiner Kundenbeziehung zu den Schuldner:innen stand, die Daten zu diesem Zweck verwendet.

Der Fall zeigt auch: Nicht alle Daten, die als anonym – und damit nicht mehr der DSGVO unterliegend – deklariert werden, sind es tatsächlich auch. Das Unternehmen hat zwar offenbar Maßnahmen getroffen, um in der oben genannten Analyseumgebung personenbezogene Daten nunmehr anonym zum KI-Training weiterzuverarbeiten. Hierzu hat das Unternehmen im Wesentlichen die Verknüpfung der für die KI-Modelle erforderlichen Daten zu persönlich identifizierbaren Informationen wie Namen, Adressen, bestimmten Aktenzeichen oder IBAN-Nummern gelöscht. Unsere technische Prüfung hat jedoch ergeben: Dies führte zwar dazu, dass der Aufwand einer Re-Identifizierung der betroffenen Personen erhöht wurde, aber nicht dazu, dass die betroffenen Personen nicht mehr identifiziert werden konnten. Tatsächlich kann ein Großteil der Personen anhand gespeicherter Hash-Werte[115] von Namen, Adressen und Geburtsdaten und unabhängig davon auch mittels Informationen aus aufbewahrungspflichtigen Geschäftsbriefen re-identifiziert werden.

Schließlich prüften wir, ob ein Transparenzdefizit bei der Verarbeitung von personenbezogenen Daten zum KI-Training letztlich auch zu Folgendem führen kann: Das Unternehmen kann sich nicht mehr darauf berufen, dass berechtigte Unternehmensinteressen gegenüber den schutzwürdigen Interessen der betroffenen Personen überwiegen.[116] Denn im Rahmen dieser Interessenabwägung ist auch zu berücksichtigen, inwieweit der Verantwortliche seinen Transparenz- und Informationspflichten nachgekommen ist. Das gänzliche Fehlen von essenziellen Datenschutzinformationen auf erster Ebene und irreführende Angaben zum KI-Training in der Datenschutzerklärung auf der Website können dazu führen, dass Betroffene weder widersprechen noch durch sonstige Weise rechtzeitig zum Ausdruck bringen können – sie wünschen diese Art der Verarbeitung nicht.

113 Siehe Artikel 29-Gruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, Rz. 38, abrufbar ist diese vom EDSA bestätigte Leitlinie unter https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html.

114 Vgl. Art. 14 Abs. 3 lit. b DSGVO.

115 Hash-Wert ist ein berechneter Wert, der als Fingerabdruck für digitale Daten dient.

116 Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

Wir werden die festgestellten Verstöße u. a. aufgrund der hohen Zahl betroffener Personen an unsere Sanktionsstelle zur Prüfung der Einleitung eines Bußgeldverfahrens abgeben.

Der Fall zeigt: Die starke Betonung einer transparenten Datenverarbeitung durch die DSGVO ist kein Selbstzweck. Ihr liegt der Gedanke zugrunde, dass ohne hinreichende Transparenz der Datenschutz leerlaufen würde, weil Betroffenen eventuelle Rechtsverstöße nicht bekannt wären, sie ihre Rechte nicht geltend machen könnten und damit ohne Interventionsmöglichkeiten sind. Daneben unterstreicht der Fall: Die Unternehmen sollten sorgfältig prüfen, ob ihre KI-Trainingsdaten tatsächlich anonym sind.

3. KI-Training mit Kundenanfragen

Im Onlinegeschäftsverkehr geht eine Vielzahl an Nachrichten beim Kundenservice von Unternehmen ein. Eine hohe Antwortgeschwindigkeit und -genauigkeit beeinflussen dabei maßgeblich die Kundenzufriedenheit. Um hier einen besseren Service zu bieten, nutzte eine Immobilienvermittlungsplattform die Anfragen an den Kundenservice für das Training eines unterstützenden KI-Systems, ohne darüber zu informieren.

Eine Immobilienvermittlungsplattform wollte die Qualität ihres Kundenservices verbessern. Hierfür sollte ein KI-System durch maschinelles Lernen eine Klassifizierung der Eingaben durchführen, damit diese im Kundenservice zielorientierter bearbeitet werden können. Das Unternehmen griff dabei auf eingehende Originalanfragen und -kommunikation zurück, informierte darüber jedoch nicht in seiner Datenschutzerklärung und wies auch sonst nicht auf diese Verarbeitung hin. Insgesamt sammelte das Unternehmen so eine mittlere sechsstellige Anzahl an Anfragen, wodurch schätzungsweise eine niedrige fünfstellige Anzahl an natürlichen Personen betroffen war. Es ist insofern mit mehreren Anfragen in einer laufenden Geschäftsbeziehung zu rechnen. Diese zweckändernde Verarbeitung stützte das Unternehmen nach eigenen Angaben auf berechtigte Interessen.[117]

117 Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

Im vorliegenden Fall wurde für die Bewertung der Rechtmäßigkeit der Verarbeitung das gesetzliche Transparenzerfordernis besonders relevant. So muss die Informationspflicht nach Art. 13 DSGVO eingehalten werden, wozu hier die Information über ggf. verfolgte berechtigte Interessen gehört.[118] Wenn diese Information nicht gegeben wird, dann schließt dies die Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 lit. f DSGVO für eine Verarbeitung aus.[119] Dieser Informationspflicht kam die Immobilienvermittlungsplattform nicht nach. In der Folge war die Datenverarbeitung damit nicht nur intransparent, sondern auch rechtswidrig.

Aufgrund der hohen Anzahl an Betroffenen und der intransparenten Weiterverarbeitung, die zudem in einem Verbraucher:innenkontext stattfand, haben wir den Fall an unsere Sanktionsstelle zur Prüfung der Einleitung eines Bußgeldverfahrens abgegeben.

Für die Erleichterung von Büroarbeit sind KI-Systeme auf Grundlage von maschinellem Lernen derzeit stark im Trend. Diese benötigen jedoch eine entsprechende Trainingsgrundlage in Form von Daten. Sofern diese aus dem laufenden Betrieb gewonnen werden und sich auf natürliche Personen beziehen, müssen die Vorgaben der DSGVO für diesen Bereich eingehalten werden. Hierzu gehört insbesondere die Einhaltung der Transparenzpflicht zur Information über berechtigte Interessen nach Art. 13 DSGVO. Wenn diese nicht erfüllt wird, kann ein entsprechendes Training auch nicht auf berechtigten Interessen i. S. d. Art. 6 Abs. 1 Satz 1 lit. f DSGVO basieren.

118 Siehe Art. 13 Abs. 1 lit. d DSGVO.

119 Europäischer Gerichtshof (EuGH), Urteil vom 9. Januar 2025, C-394/23, Rn. 46, 52, 64; Schlussanträge des Generalanwalts Maciej Szpunar vom 11. Juli 2024, C-394/23, Rn. 55 f., der auch Bezug nimmt auf EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 126; Österreichisches Bundesverwaltungsgericht (BVwG), Erkenntnis vom 11. Juni 2025, W211 2308914-1; Landgericht (LG) Berlin II, Urteil vom 19. Juni 2025, 52 O 65/23, unter II.1.d) dd)(1).

4. Widerspruch gegen KI-Training bei Änderung von KI-Entwicklungsplänen

In unserer Aufsichtspraxis sehen wir vermehrt Unternehmen, die KI-Modelle auf der Grundlage ihrer Nutzerdaten entwickeln und dabei die Nutzer:innen vorab ausdrücklich auf ein Widerspruchsrecht hinweisen. Soweit dann ein Widerspruch eingelegt wird, wird dieser im weiteren Verlauf bei Änderung der ursprünglichen KI-Entwicklungspläne jedoch teilweise nicht länger beachtet. Ein solches Verhalten missachtet das weit auszulegende Widerspruchsrecht der Betroffenen.

Immer mehr Unternehmen entscheiden sich dafür, unter Verwendung ihrer umfangreichen Nutzerdaten eigene KI-Modelle zur entwickeln. Dabei wählen sie zum Teil die Möglichkeit, die betroffenen Nutzer:innen vor der Verwendung ihrer personenbezogenen Daten zum Training der Modelle explizit (z. B. durch ein Banner auf ihrer Website oder in ihrer App) auf ein Widerspruchsrecht gegen diese Verarbeitung hinzuweisen. Sofern keine Einwilligung der betroffenen Personen für das Training erforderlich ist und die Unternehmen sich auf eine Interessenabwägung für die Verarbeitung[120] stützen, kann eine im Unterschied zu Art. 21 Abs. 1 DSGVO bedingungslos eingeräumte Widerspruchsmöglichkeit notwendig sein, um den betroffenen Personen eine Interventionsmöglichkeit zu geben und mit dieser Maßnahme die schutzwürdigen Interessen zu wahren.

Unsere Aufsichtspraxis zeigt jedoch, dass einige Unternehmen bereits eingelegte Widersprüche bei sich ändernden Plänen zur KI-Entwicklung nicht länger berücksichtigen. Zum Teil wird bspw. von Unternehmen das Training eines KI-Modells zunächst ausgesetzt, um dann später doch ein (ggf. leicht abgeändertes) KI-Modell zu trainieren. Einige Unternehmen entscheiden sich in dieser Situation, die bereits erteilten Widersprüche nicht länger als gültig anzusehen und stattdessen neue Widerspruchsmöglichkeiten zu implementieren. Das heißt, die betroffenen Nutzer:innen müssen dann mehrfach der Verwendung ihrer Daten zu KI-Trainingszwecken widersprechen, obwohl sie eigentlich hätten davon ausgehen können, dass ihr vorheriger Widerspruch nach wie vor wirksam ist. Zum Teil wird dagegen argumentiert, dass die Verarbeitung nicht wie ursprünglich geplant stattgefunden habe. Es habe also auch keine Verarbeitung

120 Siehe B.IV.3.

gegeben, gegen die betroffene Personen Widerspruch hätten einlegen können, und der Widerspruch der betroffenen Personen nach Art. 21 DSGVO sei somit nicht mehr gültig. Es besteht damit die Gefahr, dass durch das ständige Ändern der KI-Trainingspläne das Widerspruchsrecht konterkariert wird.

Nach Art. 21 Abs. 1 DSGVO können betroffene Personen jederzeit gegen die Verarbeitung sie betreffender Daten Widerspruch einlegen. Das bedeutet, dass der Widerspruch auch vor einer Verarbeitung eingelegt werden kann und – wie eine nicht erteilte Einwilligung – die (zukünftige) Verarbeitung der personenbezogenen Daten rechtlich verhindert. Nach Art. 21 Abs. 1 Satz 2 DSGVO ist der Verantwortliche dann grundsätzlich für die Zukunft verpflichtet, die personenbezogenen Daten nicht mehr zu verarbeiten.

Gerade im KI-Kontext kann dies wesentlich sein, da der Widerspruch ansonsten ggf. ganz wirkungslos ist: So kann es im Zusammenhang mit dem während des Trainings in ein LLM aufgenommenes personenbezogenes Datum zu der Situation kommen, dass das Datum aus diesem nicht mehr gelöscht werden kann, ohne dass das gesamte LLM – und nach Veröffentlichung sämtliche seiner Kopien, insbesondere bei Open-Source-LLM – gelöscht wird bzw. mithilfe von „machine unlearning"-Maßnahmen neu trainiert wird. Ein Widerspruch vor der Verarbeitung muss folglich ein Training mit den personenbezogenen Daten wirksam ausschließen.

Haben Betroffene gegenüber KI-Entwickler:innen von ihrem explizit eingeräumten Widerspruchsrecht Gebrauch gemacht, bleibt der Widerspruch grundsätzlich auch dann gültig, wenn der Verantwortliche die Verarbeitung nicht wie geplant aufnimmt bzw. unterbricht und zu einem späteren Zeitpunkt ein abgewandeltes KI-Training durchführt. Widersprüche sind auch dann beachtlich, wenn die Verarbeitung noch nicht begonnen hat. Sie stellen für die Verarbeitung dann ein rechtliches Hindernis dar, ebenso wie eine nicht erteilte Einwilligung.

5. Beantragte Sperrung der chinesischen KI-App DeepSeek

Um die rechtswidrige Übermittlung personenbezogener Daten von Nutzer:innen in Deutschland in die Volksrepublik China zu beenden, beantragten wir die Sperrung der chinesischen KI-Anwendung DeepSeek in den App-Stores von Google und Apple für Deutschland. Dabei machten wir vom Melde- und Beschwerdemechanismus des Digital Services Act (DSA) Gebrauch und zeigten die Möglichkeiten der europäischen Digitalgesetzgebung auf.

DeepSeek ist ein KI-gestützter, multifunktionaler Chatbot[121], der von dem chinesischen Unternehmen Hangzhou DeepSeek Artificial Intelligence Co., Ltd., betrieben wird. Eine Niederlassung des Unternehmens in der Europäischen Union (EU) besteht nicht. Die Anwendung wird deutschen Nutzer:innen über den Google Play-Store und den Apple App-Store mit deutschsprachiger Beschreibung zum Download angeboten. Auch die App selbst kann in deutscher Sprache genutzt werden. Damit ist die DSGVO anwendbar.[122]

Laut eigenen Angaben verarbeitet der Dienst umfangreiche personenbezogene Daten der Nutzer:innen, darunter alle Texteingaben, Chatverläufe und hochgeladene Dateien sowie Informationen zum Standort, den benutzten Geräten und Netzwerken. Die gesammelten personenbezogenen Daten der Nutzer:innen übermittelt der Dienst an chinesische Auftragsverarbeiter und speichert diese auf Servern in China.

Wir kamen zu dem Ergebnis, dass diese Drittstaatenübermittlungen rechtswidrig sind, und forderten das Unternehmen daher im Mai auf, die Datenübermittlungen in die Volksrepublik China einzustellen, die gesetzlichen Voraussetzungen für eine rechtmäßige Drittstaatenübermittlung zu erfüllen oder die App selbständig aus den App-Stores für Deutschland zu entfernen. Nach der Weigerung des Unternehmens meldeten wir die App nach Art. 16 DSA als „rechtswidrigen Inhalt“ bei den App-Stores von Google sowie Apple und beantragten eine Sperrung der DeepSeek-App.

121 Chatbots sind Programme, die mit großen Mengen von Textdaten trainiert werden, um natürliche Gespräche zu führen und auf eine Vielzahl von Fragen zu antworten.

122 Siehe Art. 3 Abs. 2 lit. a DSGVO.

In unserer Meldung nach dem DSA legten wir ausführlich dar, dass die Übermittlung personenbezogener Daten der Nutzer:innen in die Volksrepublik China gegen europäisches Datenschutzrecht verstößt. Die DSGVO verlangt, dass die hohen Datenschutzstandards der EU auch bei der Übermittlung personenbezogener Daten in andere Länder gewahrt bleiben. Dafür braucht es entweder einen Angemessenheitsbeschluss der EU oder weitere Schutzmaßnahmen, sog. geeignete Garantien. Für die Volksrepublik China hat die EU keinen Angemessenheitsbeschluss erlassen.

Die Hangzhou DeepSeek Artificial Intelligence Co., Ltd., verstößt mit ihrem Dienst DeepSeek gegen Art. 46 Abs. 1 DSGVO. Sie konnte uns gegenüber nicht nachweisen, dass das erforderliche Schutzniveau auch bei der Weitergabe der Daten an chinesische Auftragsverarbeiter gewährleistet wird. Dies gilt insbesondere vor dem Hintergrund, dass nicht dargelegt wurde – den Nutzer:innen von DeepSeek in China stehen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung, wie sie in der EU garantiert sind.

Unsere Maßnahme erfolgte in enger Abstimmung mit den Landesdatenschutzbeauftragten von Baden-Württemberg, Rheinland-Pfalz und der Freien Hansestadt Bremen sowie nach Unterrichtung der Koordinierungsstelle für digitale Dienste in der Bundesnetzagentur, die in Deutschland für die Durchsetzung des DSA zuständig ist.

Google und Apple lehnten eine Sperrung in ihren App-Stores ab. Wir werden nun gegen die Ablehnung unseres Antrags Beschwerde nach Art. 20 DSA einlegen und wiederholt die Rechtswidrigkeit der massenhaften Übermittlungen personenbezogener Daten in die Volksrepublik China darlegen. Sollten die Betreiber:innen der App-Stores auch auf die Beschwerde hin nicht tätig werden und wir weiterhin von einem rechtswidrigen Inhalt ausgehen, könnten wir nachfolgend noch ein Streitbeilegungsverfahren nach Art. 21 DSA einleiten.

Die Meldung der rechtswidrigen DeepSeek-App nach dem DSA stellt einen pragmatischen Ansatz dar, schwerwiegende Datenschutzverstöße über das Zusammenspiel der europäischen Digitalrechtsakte zu adressieren. Vor dem Hintergrund der zunehmenden Übermittlungen personenbezogener Daten in die Volksrepublik China und den damit verbundenen Risiken für die Rechte Betroffener werden wir derartige Verarbeitungen auch in Zukunft genau prüfen.

V. Digitalisierung in der Verwaltung

1. Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben

Wir haben Ende vergangenen Jahres den Standardprozess Datenschutz für öffentliche Digitalisierungsvorhaben veröffentlicht.[123] Die Erfahrungen in der Praxis zeigen nun, dass die konkreten Prüfschritte und ihre Orientierung an den Phasen des Projektmanagements den Behörden die Umsetzung des Datenschutzes im Rahmen von Digitalisierungsprojekten erleichtern. Wir entwickeln den Standardprozess auf Grundlage dieser Erfahrungen stetig weiter.

Die Erfahrungen des ersten Jahres in der praktischen Anwendung des Standardprozesses fallen positiv aus. Sie bestätigen den Bedarf nach standardisierten, handlungsanleitenden Vorgaben der Aufsichtsbehörden zur Umsetzung des Datenschutzes in Digitalisierungsprojekten. Insbesondere die Orientierung der konkreten Prüfschritte an den bundesweit etablierten Phasen des Projektmanagements[124] halten wir für besonders praxistauglich. Denn hierdurch wird verhindert, dass der Datenschutz zu spät in der Projektplanung und -umsetzung Berücksichtigung findet. Konkret gibt der Standardprozess einen Fragenkatalog zu den wichtigsten Datenschutzaspekten vor, der bereits zu Beginn der Projekte im Rahmen der Projektumfeldanalyse und Machbarkeitsprüfung zu berücksichtigen ist. Auf dieser Grundlage wurden uns bereits Machbarkeitsprüfungen zu komplexen Projekten vorgelegt. Dadurch wird sichtbar, dass der Standardprozesses in der Praxis auch als Frühwarnsystem dient.

123 Siehe JB 2024, A.VI.2. und A.VI.3.

124 Siehe z. B. DIN-Normenreihe DIN 69901; Praxisleitfaden der Bundesregierung zum Projektmanagement für die Öffentliche Verwaltung, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderne-verwaltung/praxisleitfaden-projektmanagement.pdf?__blob=publicationFile&v=6.

Darüber hinaus schärft der Standardprozess auch die Rollen- und Aufgabenverteilung zum Datenschutz in Digitalisierungsvorhaben. So stellt er klar, dass zunächst das Projektpersonal der Verantwortlichen, und nicht z. B. der behördliche Datenschutzbeauftragte (DSB), für die Umsetzung der Datenschutzvorgaben zuständig ist. Der Standardprozess wirkt auch dem häufigen Missverständnis entgegen, dass Digitalisierungsprojekte pauschal durch die DSB oder gar die Aufsichtsbehörden „freigegeben" werden müssen. Dieses Missverständnis führt in der Praxis regelmäßig zu Verzögerungen in der Projektumsetzung.

Schließlich dient der Standardprozess auch als Grundlage für die Einbeziehung von externer Beratung, soweit diese erforderlich ist. So können die konkreten Prüfschritte und strukturellen Vorgaben des Standardprozesses von den Behörden genutzt werden, um eine präzise Beauftragung und spätere Qualitätssicherung der Beratungsleistung durch externe Unternehmen sicherzustellen.

Die Anwendung des Standardprozesses kann zukünftig weiter ausgebaut werden. Voraussetzung hierfür ist auch ein weiterer Aufbau von Datenschutzkompetenz innerhalb der Verwaltung. Der Standardprozess kann die Behörden hierbei unterstützen, indem diese die Prüfmethode und die vertiefenden Handreichungen als Grundlage für die Schulung des Fachpersonals nutzen. Um die Anwendung in der Praxis zusätzlich zu erleichtern, bieten wir den Standardprozess in seiner überarbeiteten Version nun interaktiver und niedrigschwelliger an.

Auch über die Grenzen Berlins hinaus hat der von uns bei der Entwicklung des Standardprozesses zugrunde gelegte Ansatz Berücksichtigung gefunden. So hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder DSK nach diesem Vorbild speziell für länderübergreifende Onlinedienste nach dem Onlinezugangsgesetz (OZG) einen standardisierten Prüfprozess entwickelt. Daran waren wir maßgeblich beteiligt.[125]

Der Standardprozess hilft in der Praxis dabei, den Datenschutz in Digitalisierungsprojekten besser und rechtzeitiger zu berücksichtigen. Er wirkt sich zudem klarstellend auf die Rollen- und Aufgabenverteilung bei der Umsetzung datenschutzrechtlicher

125 Siehe C.IV.1.

Vorgaben aus und kann Behörden dabei unterstützen, eine präzise Beauftragung und spätere Qualitätssicherung der Beratungsleistung von Externen sicherzustellen sowie eigene Fachkompetenz im Datenschutz aufzubauen. Wir möchten diese positiven Effekte des Standardprozesses zukünftig weiter steigern und die Anwendung durch eine interaktivere und intuitivere Gestaltung erleichtern.

2. Open Data und Datenschutz

Im Rahmen unserer Beratungstätigkeit für öffentliche Stellen gewinnt das Thema Open Data zunehmend an Bedeutung. Um das Wissen bezüglich des Verhältnisses von Open Data und datenschutzrechtlichen Fragestellungen in der Verwaltung zu fördern, haben wir uns mit Vorträgen bei der Arbeitsgemeinschaft (AG) Open Data[126] eingebracht und auch bei einer Podiumsdiskussion am Berlin-Open-Data-Day 2025 beteiligt. Zudem haben wir schon im vergangenen Jahr die Zentrale Verantwortliche für Open Data im Land Berlin hinsichtlich möglicher Anpassungen der Open-Data-Verordnung (OpenDataV) in Bezug auf datenschutzrechtliche Fragestellungen beraten.

Wir stellen fest, dass insbesondere seit der Verabschiedung der neuen Open-Data-Strategie im Jahr 2023,[127] die u. a. auch den Nutzen von offenen Daten im Bereich der Verwaltungsdigitalisierung stärker in den Blick nimmt, die Bereitstellung von Verwaltungsdaten an Relevanz gewonnen hat. Im Hinblick auf die Bereitstellung der Daten treten aber in der Verwaltung zunehmend Unsicherheiten auf, die den Balanceakt zwischen Datenschutz und innovativer Datennutzung betreffen. Auch die Podiumsdiskussion bei dem Berlin-Open-Data-Day 2025 beschäftigte sich mit diesem Thema. Zudem werfen die neuen Rechtsakte der EU, wie der Data Act, hinsichtlich der Datenbereitstellung neue Fragen auf. Bei der AG Open Data haben wir uns in diesem Jahr deshalb im Rahmen eines Vortrags hiermit auseinandergesetzt, nachdem wir bereits im vergangenen Jahr die Mitglieder der AG im Rahmen eines Impulsvortrags über das Zusammenspiel von Open Data und Datenschutz aufgeklärt haben.

126 Ein Arbeitsgremium, das sich aus behördlichen Open-Data-Beauftragten zusammensetzt.
127 Siehe Berliner Open-Data-Strategie 2023, abrufbar unter https://www.berlin.de/moderne-verwaltung/e-government/opendatastrategie_2023.pdf?ts=1756800217.

Soweit Daten auf dem Open-Data-Portal[128] im Internet bereitgestellt werden sollen, ist immer zu berücksichtigen, dass mit der Bereitstellung von Daten mit Personenbezug ein erheblicher Eingriff in das Recht auf informationelle Selbstbestimmung verbunden sein kann. Eine Bereitstellung von besonders schützenwerten Daten i. S. d. Art. 9 Datenschutz-Grundverordnung (DSGVO) ist deshalb bspw. regelmäßig unzulässig.

Soweit für die Einordnung bzw. das Verständnis der im Open-Data-Portal bereitgestellten offenen Daten auf den Personenbezug nicht verzichtet werden kann, ist immer eine Rechtsgrundlage i. S. d. Art. 6 Abs. 1 DSGVO ggf. i. V. m. Art. 6 Abs. 3 DSGVO erforderlich. Die Rechtsgrundlage muss vorsehen, dass personenbezogene Daten dauerhaft allgemein zugänglich gemacht werden können. Dauerhaft bedeutet, dass keine gesetzlichen Lösch- oder Veröffentlichungsfristen entgegenstehen dürfen. Allgemein zugänglich bedeutet, dass diese Rechtsgrundlage einen freien Zugang ohne zusätzliche Begründungserfordernisse für die Öffentlichkeit vorsieht und nicht auf einen bestimmten Personenkreis beschränkt ist. Darüber hinaus ist im Einzelfall eine Abwägung zwischen dem öffentlichen Interesse an der Veröffentlichung und dem schutzwürdigen Interesse der betroffenen Person vorzunehmen. Eine Veröffentlichung ist nur dann zulässig, wenn der Schutz personenbezogener Daten nicht überwiegt. Eine Weiterverarbeitung der betroffenen personenbezogenen Daten aufgrund der Voraussetzungen des Art. 6 Abs. 4 DSGVO ohne eine Rechtsgrundlage, die den genannten Anforderungen entspricht, ist nicht möglich.

Wenn Datensätze, die für die Veröffentlichung im Open-Data-Portal vorgesehen sind, Daten mit Personenbezug enthalten, sollten diese anonymisiert werden. Hierzu sind die Daten irreversibel in einer Weise zu verändern, dass sie sich nicht mehr auf eine identifizierte oder identifizierbare natürliche Person beziehen oder, soweit der Bezug zu einer natürlichen Person erhalten bleibt, diese betroffene Person nicht oder nicht mehr identifiziert werden kann.[129] In Fällen, in denen für die sinnvolle Nachnutzung der offenen Daten eine Personenbeziehbarkeit erforderlich ist und hierfür eine Rechtsgrundlage besteht, sollte regelmäßig durch eine pseudonymisierte Bereitstellung der Daten dem Schutz der Betroffenen Rechnung getragen werden. Unter Pseudonymisierung versteht man „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht

128 https://daten.berlin.de/.
129 Siehe Erwägungsgrund (ErwGr.) 26 Satz 5 DSGVO.

mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern 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".[130] DSK erarbeitet momentan konkrete Anwendungshinweise für die Durchführung von Anonymisierungs- und Pseudonymisierungsverfahren.[131]

Für die Bereitstellung von Datensätzen, die auch personenbezogene Daten enthalten, in einem Open-Data-Portal bedarf es einer geeigneten Rechtsgrundlage nach der DSGVO. Auch wenn die Bereitstellung in personenbezogener Form erlaubt ist, sollte immer geprüft werden, ob die Daten zum Schutz betroffener Personen vor der Bereitstellung pseudonymisiert werden können. Sofern die Veröffentlichung der Daten gesetzlich nicht erlaubt ist, müssen personenbezogene Daten vor der Bereitstellung anonymisiert werden, wobei zu beachten ist, dass die Anforderungen an Anonymisierungsverfahren im Fall einer Veröffentlichung der Daten regelmäßig sehr hoch sind.

130 Art. 4 Nr. 5 DSGVO.
131 Siehe C.I.

3. Datenschutzrechtliche Verantwortlichkeit bei IKT-Basisdiensten

Die zentrale Entwicklung und Bereitstellung einheitlicher Informations- und Kommunikationstechnologie (IKT) für Behörden ist ein wichtiger Baustein bei der Verwaltungsdigitalisierung. Die Einführung von E-Government und IKT sowie die Weiterentwicklung und die zentrale Steuerung erfolgt durch die Senatskanzlei.[132] IKT-Basisdienste wie die Digitale Akte[133] werden zentral von der Senatskanzlei entwickelt und bereitgestellt und sind dann von sämtlichen Behörden zu nutzen. Da am Einsatz dieser IT-Verfahren mehrere Verwaltungen beteiligt sind und diese jeweils unterschiedliche Rollen einnehmen, stellten sich im Projekt zur Einführung des Basisdienstes Digitale Akte Fragen nach der datenschutzrechtlichen Verantwortlichkeit[134].

Die Bereitstellungen einheitlicher technischer Dienste und Komponenten als sog. IKT-Basisdienste kommen in der digitalen Abwicklung von Verwaltungsverfahren und Geschäftsprozessen zur Anwendung. Hierbei gibt es regelmäßig mehrere Beteiligte: Auf der einen Seite die Senatskanzlei, die die wesentlichen Designentscheidungen getroffen hat und einen Dienst zur Nutzung zur Verfügung stellt und betreibt; auf der anderen Seite die den Dienst nutzenden Behörden der Haupt- oder Bezirksverwaltung oder nachgeordnete Behörden. Daneben kommt eine weitere Rolle zum Tragen, nämlich die des IT-Dienstleistungszentrums Berlin (ITDZ), das als zentraler Dienstleister der Verwaltung die jeweiligen Verfahren in technischer Hinsicht, d. h. auf Ebene der Infrastruktur, betreibt. Die Behörden sind wiederum verpflichtet, diese Leistungen beim ITDZ abzunehmen.[135]

Im Zuge unserer Beratungen im Projekt zur Einführung der Digitalen Akte haben wir uns mit der Frage der Verantwortlichkeit näher befasst: Die für die datenschutzrechtliche Verantwortlichkeit maßgebende Vorschrift[136] definiert den Verantwortlichen als die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung

132 Siehe §§ 20 ff. E-Government-Gesetz Berlin (EGovG Bln).
133 Siehe JB 2023, A.IV.1; JB 2024, A.VI.3.
134 Siehe Art. 4 Nr. 7 DSGVO.
135 Siehe § 24 EGovG Bln.
136 Art. 4 Nr. 7, 1. Hs. DSGVO.

von personenbezogenen Daten entscheidet. Bei den IKT-Basisdiensten werden die Entwicklung und der Betrieb durch die Senatskanzlei vorgenommen; die eigentliche inhaltliche Verarbeitung personenbezogener Daten erfolgt jedoch im Regelfall im Rahmen der Nutzung des Dienstes durch die Fachbehörden; und der Betrieb wird wiederum technisch durch das ITDZ realisiert. Es kann hier also nicht davon ausgegangen werden, dass lediglich eine Stelle über die Mittel und Zwecke der Datenverarbeitung entscheidet.

Da weder die Senatskanzlei noch die den Dienst nutzenden Behörden jeweils allein darüber entscheiden, warum und auf welche Weise die Verarbeitung erfolgt, kann nicht ohne Weiteres von einer getrennten Verantwortlichkeit der Beteiligten ausgegangen werden. Die Senatskanzlei trifft in Wahrnehmung ihrer gesetzlichen Aufgaben u. a. die Architekturentscheidungen, stellt die Nutzerkonten zur Verfügung und trifft allgemeine Datensicherheitsmaßnahmen. Damit nimmt sie eigene gesetzliche Aufgaben wahr und ist nicht wie eine Auftragsverarbeiterin[137] bzw. Dienstleisterin lediglich auf Weisung der nutzenden Behörden tätig. Die Behörden wiederum sind verpflichtet, den Dienst zu nutzen,[138] während sich die Zwecke der Verarbeitung personenbezogener Daten maßgeblich nach ihren gesetzlichen Aufgaben und den für sie geltenden inhaltlichen Datenverarbeitungsvorschriften bemessen. Gleichzeitig haben sie auch Einfluss auf individuelle Konfigurationseinstellungen.

Im Rahmen unserer Beratungen sind wir zu dem Ergebnis gekommen, dass aufgrund des Zusammenwirkens zwischen Senatskanzlei und den nachnutzenden Behörden sowohl im Hinblick auf die Wahrnehmung der den Beteiligten zugewiesenen Aufgaben als auch im Hinblick auf die praktische Ausgestaltung der Datenverarbeitungsprozesse eine getrennte Betrachtung der Verantwortlichkeit nicht praxisgerecht wäre. Die Annahme einer gemeinsamen Verantwortlichkeit[139] erscheint damit der zielführendere Weg zu sein.

Das ITDZ wird daneben als Dienstleister für die Senatskanzlei und damit als Auftragsverarbeiter tätig und verarbeitet hierbei im Rahmen des technischen Betriebs auch personenbezogene Daten für die nutzenden Behörden.

137 Siehe Art. 28 DSGVO.
138 Siehe dazu § 7 Abs. 1 Satz 3 und § 24 Abs. 2 Satz 2 EGovG Bln.
139 Siehe Art. 26 DSGVO.

Im Ergebnis unseres Beratungsprozesses haben wir empfohlen, die datenschutzrechtliche Verantwortlichkeit für den Dienst Digitale Akte zwischen der Senatskanzlei und den nachnutzenden Behörden als gemeinsame Verantwortlichkeit i. S. v. Art. 26 DSGVO auszugestalten. In einer Vereinbarung[140] ist nun festzulegen, wer konkret welcher Verpflichtung nach der DSGVO, insbesondere im Hinblick auf die Erfüllung der Betroffenenrechte, die Einhaltung der Datenschutzgrundsätze sowie die notwendigen Sicherheitsmaßnahmen, nachkommt. Mit dem ITDZ sind entsprechende Vereinbarungen zur Auftragsverarbeitung abzuschließen.[141] Wir empfehlen, bei der anstehenden Anpassung der Regelungen des E-Government-Gesetzes Berlin (EGovG Bln) und des Onlinezugangsgesetzes Berlin (OZG Bln) in einem neu zu schaffenden Digitalgesetz die Verantwortlichkeit in Bezug auf die Rollen und Aufgaben der Beteiligten gesetzlich festzulegen. Damit kann die für die Praxis der Verwaltung notwendige Rechtssicherheit geschaffen werden. Gleichzeitig sollten diese Grundsätze auf alle IKT-Basisdienste und weitere zentral bereitgestellte IT-Fachverfahren übertragen werden.

140 Siehe Art. 26 Abs. 1 Satz 2, Abs. 2 DSGVO.
141 Siehe Art. 28 Abs. 3 DSGVO.

VI. Schule und Bildung

1. Fortführung der Schuldigitalisierung

Auch in diesem Jahr haben wir den mittlerweile etablierten Austausch mit der Bildungsverwaltung sowohl auf der Fach- als auch auf der Leitungsebene fortgesetzt und intensiviert.[142] Schwerpunkt war erneut die frühzeitige Beratung bei der Fortführung der Projekte zur Schuldigitalisierung mit dem gemeinsamen Ziel, von vornherein eine datenschutzkonforme Umsetzung sicherzustellen.

Die Erweiterung der Funktionalitäten des Berliner Schulportals bildete den Schwerpunkt unserer Beratung. Das Schulportal, mit dem der Zugang zu digitalen Lehr- und Lernmitteln, digitalen Kommunikationswerkzeugen und weiteren Anwendungen für die Organisation des Schulalltags ermöglicht wird, nimmt im Ausbau der digitalen Bildungsinfrastruktur einen besonderen Platz ein.

Während 2024 mit der Novellierung des Schulgesetzes (SchulG) zunächst die rechtlichen Grundlagen für die Verarbeitung personenbezogener Daten im Schulportal geschaffen wurden, arbeitete die Bildungsverwaltung in diesem Jahr weiterhin mit Hochdruck daran, die digitalen Anwendungen technisch umzusetzen. Beispiele hierfür sind die Einführung eines digitalen Klassenbuchs sowie digitaler Vertretungspläne und die Erstellung digitaler Schülerausweise. Da der Ausbau der Funktionalitäten des Schulportals eng mit der Erweiterung von Schnittstellen zur Lehrkräfte-Unterrichts-Schul-Datenbank (LUSD) verbunden ist, haben wir unser Augenmerk weiterhin auf die Gesamtarchitektur des Portals – insbesondere im Hinblick auf die IT-Sicherheitsarchitektur – gerichtet. Die Bildungsverwaltung hat auf unsere Hinweise hin bereits diverse Nachbesserungen vorgenommen.

Wir haben der Bildungsverwaltung die Nutzung unseres Standardprozesses Datenschutz bei öffentlichen Digitalisierungsvorhaben[143] zur Anwendung empfohlen. So lassen sich insbesondere bei kleineren Digitalisierungsprojekten viele Fragen im

142 Siehe auch JB 2023, A.IV.3.; JB 2024, A.VII.1 f.
143 Siehe B.V.1.

Projektverlauf bereits durch die Bildungsverwaltung selbst klären. Gleichzeitig helfen uns die Erfahrungen und Erkenntnisse aus der Anwendung bei der Evaluation und Optimierung des Standardprozesses. Bei umfangreichen datenschutzrelevanten Projekten und konkretem Beratungsbedarf in Datenschutzfragen stehen wir selbstverständlich weiterhin mit unserer Expertise zur Verfügung.

2. Einsatz von Künstlicher Intelligenz in Schulen

Im Herbst 2024 hat die Bildungsverwaltung den Lehrkräften über das Berliner Schulportal die KI-Anwendung Microsoft Copilot zur Verfügung gestellt. Da der Einsatz von KI-Anwendungen im Schulkontext eine Reihe komplexer Fragen aufwirft und die Bildungsverwaltung uns hier nicht im Vorhinein eingebunden hat, haben wir ein formelles Verfahren eröffnet.[144]

Bei Microsoft Copilot handelt es sich um einen KI-Assistenten, der ein Sprachmodell aus dem Bereich der Künstlichen Intelligenz (KI) nutzt. Den Lehrkräften wurde Microsoft Copilot über das Schulportal zur Verfügung gestellt, zur Vorbereitung ihres Unterrichts. Hierzu müssen sich die Lehrkräfte über ihre sog. L-Kennung – eine sechsstellige Zahlenkombination, die individuell für jede im Land Berlin pädagogisch beschäftigte Person durch die Bildungsverwaltung erstellt wird und die nur von dieser Person genutzt werden darf – bei Microsoft Copilot verifizieren.

Durch die Kombination der L-Kennung, der jeweiligen Berliner Schulnummer und der Beschäftigtenart lassen sich Rückschlüsse auf die Lehrkräfte ziehen, sodass beim Einsatz von Microsoft Copilot von einer Verarbeitung personenbezogener Daten auszugehen ist. Durch unsachgemäße Benutzung des KI-Assistenten, etwa wenn die Lehrkräfte – ggf. auch nur indirekt und nicht offensichtlich bzw. versehentlich – personenbezogene Daten von Schüler:innen in sog. Prompts eingeben, kann nicht ausgeschlossen werden, dass auch deren Daten mit Microsoft Copilot verarbeitet werden. Das Land Berlin beschäftigt etwa 35.000 Lehrkräfte und unterrichtet mehr als 400.000 Schüler:innen, die somit durch eine Verarbeitung ihrer personenbezogenen Daten mithilfe von Microsoft Copilot betroffen sein können.

144 Siehe JB 2024, B.VII.1.

Wir gehen davon aus, dass der Einsatz von Microsoft Copilot ein hohes Risiko für die Rechte und Freiheiten der davon betroffenen Lehrkräfte oder Schüler:innen darstellt, da mit dem KI-Assistenten einer großen Anzahl von Personen eine neue Technologie bereitgestellt wird, die zu einer Vielzahl von Datenverarbeitungsvorgängen führt. Zudem ist nicht ausgeschlossen, dass je nach Prompt auch sensible personenbezogene Daten von Lehrkräften und Schüler:innen betroffen sein können.

Ist ein voraussichtlich hohes Risiko für die Rechte und Freiheiten von betroffenen Personen anzunehmen, so sieht die Datenschutz-Grundverordnung (DSGVO) die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung vor der Verarbeitung vor.[145] Zudem sind Vorgaben in Bezug auf Datenschutz durch Technikgestaltung sowie durch datenschutzfreundliche Voreinstellungen umzusetzen[146] und es sind ausreichende technische und organisatorische Maßnahmen für den Einsatz zu treffen.[147]

Diese gesetzlichen Vorgaben wurden von der Bildungsverwaltung bei der Einführung des Systems nicht eingehalten. Wir haben die Bildungsverwaltung daher mehrfach aufgefordert, zumindest nachträglich Maßnahmen zu treffen, um das mit dem Einsatz von Microsoft Copilot verbundene Datenschutzrisiko zu minimieren. Schließlich haben wir gegenüber der Bildungsverwaltung eine Verwarnung ausgesprochen und sie aufgefordert, bestimmte Maßnahmen zur Herbeiführung einer annehmbaren Risikominimierung nachzuholen. Dazu gehört z. B. eine Sensibilisierung der Lehrkräfte im Hinblick auf den Umgang mit personenbezogenen Daten bei der Nutzung des KI-Assistenten.

Im Auftrag aller Bildungsministerien der Bundesländer wird derzeit ein KI-Tool für Schulen entwickelt, das als Open-Source-Lösung im Rahmen des Förderprogramms DigitalPakt Schule von der gemeinnützigen Mediengesellschaft FWU[148] eigens für den Einsatz durch Lehrkräfte im Unterricht und für die Unterrichtsvorbereitung entwickelt wurde. Lehrkräfte können ihren Schüler:innen den KI-Chatbot zeitlich begrenzt und in einer geschützten Umgebung ebenfalls zur Nutzung freigeben. Zum Einsatz kommen

145 Siehe Art. 35 DSGVO.
146 Siehe Art. 25 DSGVO.
147 Siehe Art. 32 DSGVO.
148 Institut für Film und Bild in Wissenschaft und Unterricht (FWU) gGmbH, das als Medieninstitut aller Bundesländer in deren Auftrag handelt.

verschiedene große Sprachmodelle, auf die über den KI-Chatbot zugegriffen werden kann.

Die Bildungsverwaltung hat uns frühzeitig in die Planungen zum Einsatz des KI-Chatbots eingebunden. Da es sich um eine KI-Anwendung handelt, die in allen Bundesländern eingesetzt werden kann, befasst sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mit den zentral zu klärenden Datenschutzfragen in ihrem Arbeitskreis Schulen und Bildungseinrichtungen. Wir bringen uns in diesen Prozess ein und beraten gleichzeitig die Bildungsverwaltung im Hinblick auf die für Berlin spezifisch für den Einsatz des KI-Chatbots zu klärenden Fragen. Ein besonderes Augenmerk richten wir darauf, dass die notwendigen rechtlichen Grundlagen für den Einsatz von KI-Anwendungen im SchulG geschaffen werden.

Unser Ziel ist es, die Bildungsverwaltung darin zu unterstützen, einen datenschutzkonformen Einsatz von KI-Systemen für die Schulen zu ermöglichen. Dabei soll den Lehrkräften die Gelegenheit gegeben sein, die neue Technologie für die Optimierung der Unterrichtsgestaltung zu nutzen. Gleichzeitig sollen Lehrkräfte und Schüler:innen Kompetenzen im Umgang mit KI erwerben. Dies sollte aber im Kontext Schule geschehen können, ohne dass Lehrkräfte und Schüler:innen Datenschutzrisiken eingehen müssen. Wir erwarten, dass die Bildungsverwaltung den Schulen nur KI-Lösungen anbietet, die ohne Risiken für die Datenschutzrechte genutzt werden können.

3. Novellierung schulgesetzlicher Normen (Fortsetzung)

In diesem Jahr waren wir mit einer weiteren Anpassung des SchulG befasst, über die nun im parlamentarischen Gesetzgebungsverfahren das Abgeordnetenhaus von Berlin entscheiden wird.[149] Wir haben die Bildungsverwaltung zum Referentenentwurf des geplanten Änderungsgesetzes beraten; dennoch besteht eine Reihe von Punkten, in denen keine Einigkeit erzielt werden konnte. Schwerpunkte waren auch diesmal in erster Linie Änderungen sowie Ergänzungen der die Fortentwicklung der Schuldigitalisierung regelnden Vorschriften. Die Bildungsverwaltung hat unseren Vorschlag aufgegriffen und eine Regelung zum Einsatz von KI-Systemen in Schulen erarbeitet. Ein besonderes Anliegen der Bildungsverwaltung war es auch, Regelungen zu schaffen, die standardisierte Erhebungen zum individuellen Lernstand und zur Lernentwicklung der Schüler:innen ermöglichen. Diese Erhebungen haben erhebliche Auswirkungen auf die Datenschutzrechte der Schüler:innen.

In konstruktiven Beratungsgesprächen haben wir – gemeinsam mit den für die Umsetzung der Schuldigitalisierung in der Bildungsverwaltung Zuständigen – viele Aspekte der Erweiterung von Funktionalitäten der LUSD und des Schulportals behandelt. Bei unserem regelmäßigen Austausch hat es sich bewährt, anhand der Planungen zur technischen Umsetzung von Digitalisierungslösungen in den jeweiligen Fachverfahren den rechtlichen Anpassungsbedarf zu ermitteln und so das notwendige Ineinandergreifen von Recht und Technik zu erreichen.

Zum Beispiel war mit der letzten Anpassung des SchulG bereits die Möglichkeit eröffnet worden, zusätzliche Ausfertigungen und Zweitschriften von Zeugnissen elektronisch auszustellen. Nun soll der rechtliche Weg geebnet werden, auch die Ausstellung von digitalen Zeugnissen zu ermöglichen, die die gleichen Funktionen erfüllen wie die gedruckten Exemplare. Die hierfür notwendigen Regelungen konnten frühzeitig abgestimmt werden und wir erwarten, dass die technische Realisierung ebenfalls datenschutzkonform erfolgt.

Wir unterstützen den Ansatz der Bildungsverwaltung, den Schulen Funktionalitäten für die Organisation des Schulalltags über die eigens von der Bildungsverwaltung

149 Siehe zur letzten Novellierung des SchulG JB 2024, A.VII.2.

betriebenen Fachverfahren (LUSD und Schulportal) zur Verfügung zu stellen. Sie sind Alternativen zu Tools und Anwendungen, die die Schulen selbst beschaffen und auf deren Datenschutzkonformität sie sich gerade nicht ohne weiteres verlassen können. Auch erscheint es sinnvoll, die im schulischen Alltag und auch in der Schulorganisation zwischen Bildungsverwaltung und Schulen notwendige Verarbeitung personenbezogener Daten möglichst über die bestehenden Fachverfahren abzubilden. Dabei wird die Nutzung unnötiger und datenschutzrechtlich vielfach auch bedenklicher Kommunikationskanäle z. B. im Wege unverschlüsselter E-Mails vermieden. Auch die Doppelhaltung von personenbezogenen Daten und deren Pflege lässt sich durch die ausschließliche Nutzung der bestehenden Fachverfahren durch Schulen, Schulbehörden und der Bildungsverwaltung als Schulaufsichtsbehörde ersparen.

An vielen Stellen des Referentenentwurfs zeigte sich allerdings auch: Die Regelungen, die teilweise weitreichende Zugriffsmöglichkeiten der Schulaufsicht oder auch der Schulbehörden auf von den Schulen in der LUSD verarbeitete personenbezogene Daten vorsehen, korrespondieren nicht immer mit den ihnen durch das SchulG zugewiesenen gesetzlichen Aufgaben. Vielmehr sind Befugnisse vorgesehen, die einen Zugriff auf personenbezogene Daten erlauben, obwohl nicht ersichtlich ist, für welche konkrete gesetzliche Aufgabe ein solcher erforderlich ist. An dieser Stelle besteht Nachbesserungsbedarf: Verarbeitungsbefugnisse können gesetzliche Aufgabenzuweisungen nicht entbehrlich machen. Wenn die Aufgaben notwendig sind, dann sind diese gesetzlich zu formulieren und zuzuweisen. Erst dann stellt sich die Frage einer entsprechenden Befugnis zur Verarbeitung personenbezogener Daten, sofern diese für die normierte Aufgabe erforderlich ist. Dies gilt besonders bei Datenverarbeitungen, die zu dem für uns sehr nachvollziehbaren Zweck der gesamtstädtischen Steuerung und Koordination wichtig sind. Nach unserer Einschätzung lassen sich viele der inhaltlich für uns nachvollziehbaren Ziele jedoch auch mit aggregierten Daten erreichen. Die für die Aggregierung in einem ersten Schritt notwendige Verarbeitung von personenbezogenen Daten bedarf ebenfalls einer ausdrücklichen Rechtsgrundlage.

Deutliche Kritik haben wir an der vorgesehenen Regelung zur Erhebung individueller Lernstände und Lernentwicklungen der Schüler:innen geäußert. Die Bildungsverwaltung plant, dass Schulen einmal im Schuljahr standardisierte Erhebungen zum individuellen Lernstand und zur individuellen Lernentwicklung der Kompetenzen der Schüler:innen mittels eines Tests in Deutsch und Mathematik durchführen sollen. Dies soll für die

Jahrgangsstufen 1 bis 10 gelten und der adaptiven Unterrichtsgestaltung und der individuellen Förderung der Schüler:innen dienen.

Zunächst hatte die Bildungsverwaltung diese Datenerhebungen rechtlich den Maßnahmen der Qualitätssicherung und der Evaluation[150] zugeordnet. Die Qualitätssicherung und die Evaluation beziehen sich aber auf die Schule als Ganzes und gerade nicht auf die individuellen Schüler:innen. Die Erhebung individueller Lernstände und Lernverläufe dient insoweit einem gänzlich anderen Zweck.

Die Erhebung individueller Lernverläufe greift erheblich in das Recht auf informationelle Selbstbestimmung ein, da personenbezogene Daten der einzelnen Schüler:innen über einen langen Zeitraum und schulartenübergreifend miteinander verknüpft werden sollen. In der Folge werden Stärken und Schwächen in der Lernentwicklung deutlich und die Leistungs-, aber auch Persönlichkeitsentwicklung der einzelnen Schüler:innen abgebildet. Insoweit birgt die Erfassung von Lernverläufen in dieser Intensität für die Individuen ein erhebliches Stigmatisierungsrisiko. Eine Verarbeitung dieser Daten bedarf einer verfassungsgemäßen gesetzlichen Grundlage, die dem Gebot der Normenklarheit entspricht und den Grundsatz der Verhältnismäßigkeit wahren muss. Personenbezogene Daten dürfen nur verarbeitet werden, wenn aus der Norm ersichtlich ist, für welche konkreten Zwecke welche personenbezogenen Daten durch wen verarbeitet werden sollen. Zudem hat der Gesetzgeber organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, um den Schutz der betroffenen Personen und die Datensicherheit zu gewährleisten. Im Rahmen der Prüfung der Verhältnismäßigkeit ist zu bewerten, ob die Datenverarbeitung die Anforderungen der Geeignetheit und Erforderlichkeit erfüllt sowie angemessen ist. Zur Wahrung der Persönlichkeitsrechte der Schüler:innen muss Sorge dafür getragen werden, dass den Schüler:innen eine optimierte individuelle Lernförderung angeboten werden kann. Gleichzeitig muss aber auch gewährleistet werden, dass der Bildungsverlauf keine negativen Auswirkungen auf ihre Bildungs- und Berufschancen haben darf, die die Schüler:innen in ihren Möglichkeiten einschränken.

Wir haben der Bildungsverwaltung deutlich gemacht, dass eine entsprechende Regelung nur dann als datenschutzkonform angesehen werden kann, wenn diese Anforderungen umgesetzt werden. Wir konnten erreichen, dass nunmehr eine eigene Regelung

150 § 9 SchulG.

geschaffen werden soll. Der uns vorgelegte Entwurf erfüllt jedoch noch immer nicht alle von uns dargelegten Anforderungen. Insbesondere lässt sich weder dem Regelungsentwurf noch der dazugehörigen Begründung entnehmen, wie dem Stigmatisierungsrisiko konkret begegnet werden soll. Zudem fehlt es nach wie vor an einer Beschreibung der gesetzlichen Aufgabe sowie Rechtsgrundlage für die Nutzung der Daten durch die Schulaufsichtsbehörde. Auch ist die vorgesehene Aufbewahrungsfrist von sieben Jahren aus unserer Sicht zu lang.

Wir begrüßen die Bestrebungen der Bildungsverwaltung, mit der Schuldigitalisierung und ihrer technischen Umsetzung zügig voranzuschreiten und hierfür vorausschauend auch die notwendigen rechtlichen Anpassungen vorzunehmen. Dabei muss jedoch berücksichtigt werden, dass die Regelungen des SchulG teilweise die technischen Entwicklungen noch gar nicht abbilden und einige Regelungen die Bedürfnisse der Praxis nicht widerspiegeln. Darüber hinaus müssen in Teilen zunächst die Aufgaben gesetzlich normiert und zugewiesen werden, bevor dafür Datenverarbeitungsbefugnisse geschaffen werden. Die datenschutzrechtlichen Regelungen sowohl des SchulG als auch der Schuldatenverordnung (SchuldatenV) und der Digitalen Lehr- und Lernmittelverordnung (DigLLV) sollten vollständig auf den Prüfstand gestellt und ggf. überarbeitet werden, um eine notwendige Harmonisierung herzustellen. Dabei ist das Hauptaugenmerk darauf zu richten, die Rechtsgrundlagen anhand der jeweiligen gesetzlichen Aufgaben und Zwecke der Datenverarbeitung für die unterschiedlichen Akteure auszugestalten.

VII. Inneres, Justiz, Rechtsanwaltschaft und Parteien

1. Datenschutzrechtliche Begleitung der Reform des Allgemeinen Sicherheits- und Ordnungsgesetzes

Das Abgeordnetenhaus hat im Dezember ein Gesetz zur Reform des Polizei- und Ordnungsrechts beschlossen. Mit der Novelle des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) wurden diverse neue Eingriffsbefugnisse für die Polizei mit zum Teil erheblichen Auswirkungen auf die davon Betroffenen, auch unbeteiligte Dritte, geschaffen. Dazu gehören u. a. neue Rechtsgrundlagen für die automatisierte Datenanalyse, den Einsatz selbstlernender Systeme und die biometrische Fernidentifizierung. Die neuen Regelungen sind stellenweise unverhältnismäßig und werfen erhebliche verfassungsrechtliche Fragen auf. Wir haben das Gesetzgebungsverfahren auf Fachebene und im Rahmen der parlamentarischen Sachverständigenanhörung begleitet.

Die Reform des ASOG stellt eines der umfangreichsten Gesetzgebungsvorhaben der laufenden Legislaturperiode dar. Das ASOG wurde zuletzt im Jahr 2023 punktuell angepasst, u. a. hinsichtlich des Einsatzes von Bodycams.[151] Die Regierungsfraktionen hatten nun einen über siebenhundertseitigen Gesetzentwurf vorgelegt, der neue polizeiliche Befugnisse schaffen sollte (im Folgenden: Gesetzentwurf).[152] Wir wurden im Vorfeld auf Fachebene frühzeitig einbezogen und konnten dort Anmerkungen einbringen. Allerdings war der parlamentarische Prozess für dieses weitreichende Vorhaben teilweise knapp bemessen, sodass wir zu dem späteren Änderungsantrag der Regierungsfraktionen zum Gesetzentwurf (im Folgenden: Änderungsantrag)[153] in der Sachverständigenanhörung im Ausschuss für Inneres, Sicherheit und Ordnung nur zu ausgewählten Punkten Stellung nehmen konnten.

151 Siehe JB 2023, A.V.3.
152 Abghs.-Drs. 19/2553 vom 2. Juli 2025.
153 Siehe im Ergebnis Abghs.-Drs. 19/2786 vom 26. November 2025.

Ein zentrales Thema in der Sachverständigenanhörung war die in § 47a ASOG vorgesehene automatisierte Datenanalyse. Die Vorschrift ermöglicht die Zusammenführung umfangreicher polizeilicher Datenbestände auf einer Analyseplattform und deren automatisierte Auswertung. Bereits die Zusammenführung der Daten stellt eine zweckändernde Verarbeitung dar, die unter den Vorbehalt von Eingriffsschwellen zu stellen ist. Das Gesetz lässt diese Datenzusammenführung jedoch voraussetzungslos zu. Der Änderungsantrag hatte zwar klargestellt, dass die Zusammenführung ausschließlich der Vorbereitung der Datenanalyse dienen darf, und beschränkt die Nutzung von Verkehrsdaten auf Fälle konkreter Gefahr. Diese Änderungen gehen in die richtige Richtung. Entscheidende Fragen zum Umfang der einbezogenen Datenarten und zum Umfang der Zweckänderung bleiben jedoch offen. Zu den weiteren verfassungsrechtlichen Anforderungen an automatisierte Datenanalyseverfahren hat sich auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) geäußert.[154]

Der Änderungsantrag öffnete zudem die automatisierte Datenanalyse für selbstlernende Systeme, obwohl der ursprüngliche Gesetzentwurf dies mit Verweis auf noch ungeklärte verfassungsrechtliche Anforderungen ausgeschlossen hatte. Von dieser Einschätzung gehen wir auch weiterhin aus. Zwar sah der Änderungsantrag nunmehr teils abgestufte Eingriffsschwellen vor, die Regelungen bleiben jedoch unzureichend: Die Vorgabe, durch geeignete Maßnahmen sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden, ist zu unbestimmt. Wir haben konkretere Vorgaben empfohlen, etwa regelmäßige Tests auf Prüfung von mit Verzerrungen einhergehenden Diskriminierungen (sog. Bias), die Dokumentation der Trainingsdaten sowie eine fortlaufende, engmaschige Überwachung.

Eine weitere eingriffsintensive neue Befugnis betrifft den biometrischen Abgleich nach § 28a ASOG. Die Vorschrift ermöglicht erstmals die biometrische Fernidentifizierung durch automatisierten Abgleich von Gesichts- und Stimmdaten mit öffentlich zugänglichen Internetdaten; eine Maßnahme mit sehr hoher Reichweite, durch die vor allem körpereigene, unveränderliche Merkmale Unbeteiligter erhoben und abgeglichen werden. Die Zweckbestimmung der Regelung einer solchen Maßnahme bleibt im Kontext der Gefahrenabwehr unklar, selbst wenn der Änderungsantrag sie auf die Identifizierung

154 Siehe auch C.V.2.

oder Feststellung des Aufenthaltsortes beschränkt. Gleichzeitig wurde aber entgegen unserer Empfehlung der Anwendungsbereich noch ausgeweitet, indem er neben den gefahrverantwortlichen Personen auch deren Kontakt- und Begleitpersonen erfasst. Damit werden Personen einbezogen, bei denen die Verbindung zur Gefahr regelmäßig weniger eng ist als bei den Gefahrverantwortlichen selbst. Zu den Bedenken gegen biometrische Überwachungsmaßnahmen verweisen wir auch auf die Entschließung der DSK zum Verhältnis von Datenschutz und Innerer Sicherheit.[155]

Die sehr weitreichende Regelung zur zweckändernden Verwendung personenbezogener Daten zum Training von KI-Systemen in § 42d ASOG halten wir auch nach der Überarbeitung für nicht verfassungskonform, da weder die Anforderungen der hypothetischen Datenneuerhebung[156] ausreichend berücksichtigt werden, noch hinreichend bestimmt wird, zu welchen Zwecken die KI-Systeme trainiert werden dürfen.

Die ASOG-Reform zeigt exemplarisch das Verhältnis von Freiheit und Sicherheit. Es wird dort zum Spannungsfeld, wo aufgrund von polizeilichen Befugnissen anlasslos und mit hoher Streubreite in das Grundrecht auf informationelle Selbstbestimmung (auch) vieler unbeteiligter Personen eingegriffen wird. Ein Ausschöpfen dessen, was technisch an Überwachung möglich ist, wird es nicht geben können, wenn die Grundrechte von Unbeteiligten nicht ausgehöhlt werden sollen. Insofern muss immer wieder im Einzelnen und auch in der Gesamtschau von Maßnahmen austariert werden, was in den Grenzen des Rechtsstaats zum Erhalt der öffentlichen Sicherheit geeignet, erforderlich und angemessen ist. Unsere frühzeitige Einbeziehung auf Fachebene hat insoweit konstruktive Diskussionen ermöglicht, wenngleich zentrale Kritikpunkte im parlamentarischen Verfahren nicht aufgegriffen wurden. Insbesondere der Einsatz von Künstlicher Intelligenz in der Polizeiarbeit erfordert klare gesetzliche Regelungen, die die Abwägung verfassungsrechtlicher Anforderungen nicht allein der Verwaltung überlassen.

155 Siehe auch C.V.1.

156 Siehe BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 288 ff.

2. Änderung des Verfassungsschutzgesetzes

Der Senat von Berlin hat dem Abgeordnetenhaus ein Gesetz zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzrechts[157] vorgelegt. Mit dieser Gesetzesvorlage soll insbesondere das Gesetz über den Verfassungsschutz in Berlin (VSG) grundlegend geändert werden. Vorgesehen ist dabei sowohl eine neue Normierung bereits bestehender Befugnisse des Verfassungsschutzes als auch eine massive Ausweitung von Überwachungsbefugnissen, die zum Teil mit tiefen Eingriffen in das Recht auf informationelle Selbstbestimmung der Betroffenen verbunden sind. So sollen u. a. Befugnisse des Verfassungsschutzes zum Zugriff auf Videoüberwachung öffentlich zugänglicher Räume, zur Wohnraumüberwachung – auch bei Dritten – sowie zur Onlinedurchsuchung geschaffen werden.

Das im Wesentlichen aus dem Jahr 2001 stammende VSG muss seit längerem aufgrund verschiedener Entscheidungen des Bundesverfassungsgerichts (BVerfG) dringend geändert werden. Insofern begrüßen wir eine Novellierung im Grundsatz sehr. Allerdings geht der Gesetzentwurf in Teilen zu weit und berücksichtigt nicht in ausreichendem Maße das allgemeine Persönlichkeitsrecht der von den geplanten Maßnahmen betroffenen Bürgerinnen und Bürger. Gerade vor dem Hintergrund der umfassenden Neuregelung eingriffsintensiver Befugnisse mit erheblichen datenschutzrechtlichen Bezügen wäre hier eine sehr frühzeitige Einbindung der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) hilfreich gewesen.[158]

In einer parlamentarischen Anhörung am 15. September 2025 haben wir unsere Kritik an dem Gesetzentwurf dann vorgebracht und eine schriftliche Stellungnahme abgegeben.[159] Im Nachgang zu der Anhörung, in der sich auch weitere Expert:innen kritisch

157 Abghs.-Drs. 19/2466, abrufbar unter https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/DruckSachen/d19-2466.pdf.

158 Nach § 38 Satz 1 VSG i. V. m. § 11 Abs. 2 Satz 2 BlnDSG besteht eine gesetzliche Pflicht zur Anhörung der BlnBDI vor dem Erlass von Gesetzen, Rechtsverordnungen oder Verwaltungsvorschriften, wenn sie die Verarbeitung personenbezogener Daten betreffen.

159 Siehe Stellungnahme der BlnBDI vom 12. September 2025, abrufbar unter https://www.parlament-berlin.de/ados/19/VerfSch/vorgang/vfs19-0097-Stellungnahme%20zur%20Drs.2466-1.pdf sowie das Wortprotokoll der 35. Sitzung des Ausschusses für Verfassungsschutz am 15. September 2025, abrufbar unter https://www.parlament-berlin.de/ados/19/VerfSch/protokoll/vfs19-035-wp.pdf.

zum Gesetzentwurf äußerten, teilten die Koalitionsfraktionen mit, dass der Entwurf nochmals überarbeitet wird, und vertagten die Beschlussfassung.[160]

Wir haben festgestellt, dass einige gesetzliche Regelungen des Entwurfs gegen den Verhältnismäßigkeitsgrundsatz verstoßen, wobei wir folgende zentrale Punkte identifiziert haben:

- Es fehlt vollständig an der **Festlegung von Evaluations- und Befristungsklauseln**, die grundsätzlich dazu dienen, die Folgen des gesetzgeberischen Handelns und die Wirkungen der verabschiedeten Gesetze nach ihrem Inkrafttreten zu beobachten und im Hinblick auf notwendige Korrekturen oder Nachbesserungen zu überprüfen.[161]

- Es sind **zu wenige Kompensationsmaßnahmen** für die fehlende Transparenz bei heimlichen Überwachungsmaßnahmen und der Speicherung und Nutzung der dabei erhobenen personenbezogenen Daten geregelt worden. Als Instrumente zur Herstellung einer (nachträglichen) Transparenz der Datenverarbeitung gegenüber betroffenen Personen kommen insbesondere möglichst umfassende Auskunftsrechte, die Pflicht zur Benachrichtigung nach Beendigung einer Überwachungsmaßnahme sowie eine effektive Aufsicht und Kontrolle durch die Datenschutzbehörden in Betracht.[162]

- Das **Recht auf Auskunft** betroffener Personen gegenüber dem Verfassungsschutz soll künftig unverhältnismäßig eingeschränkt werden, indem es an eine über die allgemeine Antragstellung hinausgehende Mitwirkungspflicht geknüpft wird. Bei Antragstellung müssen Betroffene auf einen konkreten Sachverhalt hinweisen und ein berechtigtes Interesse darlegen. Gerade die erste Hürde dürfte faktisch kaum zu überwinden sein, wenn die Betroffenen keine Kenntnis davon haben, dass ihre Daten im Zusammenhang mit einem konkreten Sachverhalt verarbeitet wurden bzw. noch werden.

160 Siehe Beschlussprotokoll zur 37. Sitzung des Ausschusses für Verfassungsschutz am 10. November 2025, abrufbar unter https://www.parlament-berlin.de/ados/19/VerfSch/protokoll/vfs19-037-bp.pdf.

161 Siehe BVerfG, Urteil vom 3. März 2004, 1 BvR 2378/98 u. a., Rn. 213; BVerfG, Urteil vom 12. April 2005, 2 BvR 581/01, Rn. 64.

162 Siehe u. a. BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 134 ff.; BVerfG, Urteil vom 19. Mai 2020, 1 BvR 2835/17, Rn. 267.

- **Benachrichtigungspflichten** sind nur unzureichend im Gesetzentwurf vorgesehen. Statt dies nur bei einzelnen Überwachungsmaßnahmen wie der Wohnraumüberwachung und Onlinedurchsuchung zu regeln, wie momentan geplant, sollte eine zentrale Norm zur Benachrichtigung der Betroffenen in das VSG aufgenommen werden.[163] Zumindest sollte jedoch auch bei anderen besonders eingriffsintensiven Überwachungsbefugnissen eine Benachrichtigungspflicht gesetzlich normiert werden, wie z. B. für die Bestandsdatenauskunft, den verdeckten Einsatz von Dienstkräften und Vertrauensleuten sowie langfristige Observationen.

- Schließlich wurde in dem Gesetzentwurf auch das **Erfordernis einer richterlichen Kontrolle** vor der Durchführung einer Überwachungsmaßnahme des Verfassungsschutzes nur teilweise umgesetzt. Regelmäßig erforderlich ist eine solche vorherige Kontrolle bei längerfristigen Observationen (insbesondere mit Bildaufzeichnungen), der Erfassung nicht-öffentlicher Gespräche und dem Einsatz von Vertrauenspersonen.[164]

Ein weiterer zu berücksichtigender Aspekt der Verhältnismäßigkeit bei der Sicherheitsgesetzgebung ist die gesetzliche Formulierung von Eingriffsschwellen sowie Anforderungen an den Rechtsgüterschutz, was abhängig vom Eingriffsgewicht und dem jeweils betroffenen Grundrecht erfolgen muss. Das BVerfG misst der verhältnismäßigen Ausgestaltung der Eingriffsschwellen große Bedeutung zu, geht jedoch auch davon aus, dass das Eingriffsgewicht der Überwachungsmaßnahme einer Verfassungsschutzbehörde im Vergleich zu Polizeibehörden grundsätzlich geringer ist. Der Verfassungsschutzbehörde fehlen operative Anschlussbefugnisse, die mit Zwang durchgesetzt werden könnten.[165] Nachrichtendienste sind zur Erfüllung ihres Beobachtungsauftrags grundsätzlich nicht an polizeiliche Eingriffsschwellen wie die konkrete Gefahr oder den Anfangsverdacht gebunden. Sie können und sollen Aufklärung schon im Vorfeld von Gefährdungslagen betreiben, um die politischen Entscheidungsträger frühzeitig und angemessen zu informieren, sodass grundsätzlich eine „den Beobachtungsbedarf auslösende Bedrohungslage“ bzw. eine „beobachtungsbedürftige Bedrohung von Verfassungsgrundsätzen“ genügt.[166] Für nachrichtendienstliche Befugnisse von erheblicher Eingriffsintensität sind

163 Siehe BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 134.
164 Siehe BVerfG, Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, Rn. 149 ff.
165 Siehe u. a. BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 156.
166 Siehe BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 163.

jedoch höhere Anforderungen vorzusehen. Der Gesetzgeber muss daher Befugnisnormen, die Grundrechtseingriffe von erheblichem Gewicht erlauben, an eine qualifizierte Eingriffsschwelle knüpfen, die eine Schutzgutgefährdung von vergleichbarem Gewicht voraussetzt, d. h. eine hinreichend erhebliche Beobachtungsbedürftigkeit oder auch „gesteigerte Beobachtungsbedürftigkeit".[167] Zu den eingriffsintensiven Maßnahmen gehören etwa langfristige Observationen, die Erfassung nicht-öffentlicher Gespräche, der Einsatz von Vertrauenspersonen und verdeckt agierenden Mitarbeiter:innen des Verfassungsschutzes und die Onlinedurchsuchung sowie auch der Zugriff auf Videoüberwachungen des öffentlich zugänglichen Raums. Die Eingriffsschwellen sind in dem Entwurf des VSG nicht bei allen Maßnahmen ausreichend spezifisch berücksichtigt.

Im Zusammenhang mit den modifizierten Anforderungen aufgrund der verschiedenen Eingriffsschwellen ist auch zu beachten, dass die aus der jeweiligen Überwachung gewonnenen Informationen nicht ohne Weiteres an andere Behörden mit operativen Anschlussbefugnissen übermittelt werden dürfen.[168] Übermittlungen der aus nachrichtendienstlichen Maßnahmen erlangten Informationen an andere Stellen sind an Bedingungen zu binden, die den verfassungsrechtlichen Anforderungen genügen. Diese sind an entsprechende eigene Grundrechtseingriffe der empfangenden Stellen zu richten.[169] In den im zunächst vorgelegten Gesetzentwurf geregelten Vorschriften zu den Datenübermittlungen wurden diese verfassungsrechtlichen Vorgaben nur teilweise berücksichtigt.

Der Gesetzgeber hat bei der Ausgestaltung von eingriffsintensiven Überwachungsbefugnissen des Verfassungsschutzes grundgesetzliche Vorgaben und insbesondere die hierzu ergangene Rechtsprechung des BVerfG zu beachten. Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit ist bei einigen Vorschriften des Entwurfs des neuen VSG derzeit nicht gewahrt. Es bleibt abzuwarten, ob und inwieweit das Abgeordnetenhaus im laufenden Gesetzgebungsverfahren noch nachbessert und für einen verhältnismäßigen Ausgleich zwischen den staatlichen Sicherheitsinteressen und den Datenschutzrechten Betroffener sorgt.

167 Siehe BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 97, 136, 142, 149 und 187; BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 119; BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 193 f., 197, 213, 222, 328 und 359 f.

168 Zum „informationellen Trennungsprinzip" siehe BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 123.

169 „Kriterium der hypothetischen Datenneuerhebung"; siehe u. a. BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 287 ff.

3. Nicht erforderliche Informationen auf dem elektronischen Aufenthaltstitel

Der elektronische Aufenthaltstitel (eAT) wird in Deutschland seit dem Jahr 2011 für in Deutschland lebende Personen aus Nicht-EU-Staaten ausgestellt, die sich damit in Deutschland und der übrigen Europäischen Union (EU) im Alltag ausweisen und ihr Aufenthaltsrecht nachweisen können. Er wird als Plastikkarte im Scheckkartenformat ausgestellt und ähnelt in Form und Aussehen dem deutschen Personalausweis. Neben sichtbar aufgedruckten Daten enthält der eAT auch ein elektronisches Speichermedium (Chip), auf das zusätzlich biometrische Merkmale sowie Nebenbestimmungen zum Aufenthaltstitel (Bedingungen und Auflagen) gespeichert sind.

Der eAT wird in Berlin durch das zuständige Landesamt für Einwanderung (LEA) ausgestellt und von der Bundesdruckerei hergestellt. Auf der Vorderseite des eAT ist ein Lichtbild der Ausweisinhaber:in aufgebracht. Ferner sind dort sowohl Familienname und Vorname(n), Angaben zum Geschlecht, Staatsangehörigkeit und Geburtsdatum, aber auch die Art des Aufenthaltstitels, die Gültigkeitsdauer der Karte mit Datum und eventuelle Anmerkungen zu den Nebenbestimmungen zum Aufenthaltstitel vermerkt.[170]

Eine betroffene Person wandte sich an uns, da auf ihrem eAT seit einer Neuausstellung durch das LEA in dem Feld „Anmerkungen“ die Zusatzinformation „ASYL/GFK nach 5 Jahren“ hinzugefügt war. Zuvor war an gleicher Stelle nur die Rechtsgrundlage ihres Aufenthaltstitels aufgeführt. Im Ergebnis unseres daraufhin durchgeführten Verfahrens wird das LEA künftig – nach der notwendigen Umstellung des Fachverfahrens – auf diese Angabe auf dem eAT verzichten. Das LEA teilte jedoch auch mit, dass es dadurch von der Praxis anderer Bundesländer abweiche und im Ergebnis in der Aufnahme des Zusatzes keinen Datenschutzverstoß sehe.

Wir haben dem LEA mitgeteilt, dass die zusätzliche Information „ASYL/GFK nach x Jahren“ auf dem eAT gegen den Grundsatz der Datenminimierung[171] verstößt.

170 Siehe hierzu die veröffentlichten Informationen des Bundesamts für Flüchtlinge, abrufbar unter https://www.bamf.de/DE/Themen/MigrationAufenthalt/ZuwandererDrittstaaten/Migrathek/eAufenthaltstitel/eaufenthaltstitel-node.html.

171 Art. 5 Abs. 1 lit. c DSGVO.

Zu beachten ist vorliegend, dass im Aufenthaltsgesetz (AufenthG) abschließend geregelt wird, welche Angaben auf einem eAT sichtbar aufgebracht sein müssen.[172] Weitere Angaben unter „Anmerkungen" sind nur dann zu machen, wenn diese aufenthaltsrechtliche Relevanz haben oder als zusätzliche Hinweise gestattet sind. Erlaubt sind demnach bspw. Hinweise zur Erwerbstätigkeit, die Angaben „Ausweisersatz" oder „Personalien laut eigener Angabe" und die Angabe der technischen Kartennutzungsdauer.[173]

Im Ergebnis hat die Angabe „ASYL/GFK nach x Jahren" auf dem eAT keine gesonderte aufenthaltsrechtliche Relevanz. Die sichtbar aufgebrachte Angabe der Rechtsgrundlage (z. B. die Angabe „26 Abs. 3 S. 1" unter dem Feld „Anmerkungen") ist ausreichend, weil sich daraus der Grund für die jeweilige Erteilung des Aufenthaltstitels oder -rechts ergibt. Ein Mehrwert aus der Angabe „ASYL/GFK nach x Jahren" für den Zweck des Nachweises des konkreten Aufenthaltsrechts ist insoweit nicht erkennbar. Demgegenüber kann die Ausschreibung des Regelungsinhalts auf dem eAT für betroffene Personen aber stigmatisierend sein. Dritte Personen, die den eAT (kurzzeitig) in Augenschein nehmen, können aus der bloßen aufenthaltsrechtlichen Vorschrift nicht ohne Weiteres Rückschlüsse auf das jeweilige Aufenthaltsrecht ziehen, wohl aber aus der Angabe „ASYL/GFK nach x Jahren". Letztere Angaben lassen sofort erkennen, dass die betroffene Person seit fünf Jahren eine Aufenthaltserlaubnis hat, welche sie entweder aufgrund einer Asylberechtigung (ASYL) oder einer Flüchtlingsstellung nach der Genfer Flüchtlingskonvention (GFK) erhalten hat. Damit werden auch auf direktem Weg Informationen transportiert, die einen Rückschluss darauf zulassen, dass die Person nach Deutschland gekommen ist, da sie in ihrem Herkunftsstaat politisch oder anderweitig verfolgt wurde. Hierbei ist zu berücksichtigen, dass der eAT den Ausweisinhaber:innen auch als Identitätsnachweis dient und als solcher bei vielen nicht-öffentlichen und öffentlichen Stellen (z. B. dem Arbeitgeber, in der Universität oder in einer Bibliothek) vorgezeigt werden muss.

Bei der Ausstellung eines eAT dürfen nur Daten aufgenommen und verarbeitet werden, für die es eine gesetzliche Grundlage gibt und die zur Erreichung des Zwecks erforderlich sind. Hierbei ist zu berücksichtigen, dass der eAT von den Betroffenen in vielen alltäglichen Situationen als Identitätsnachweis genutzt wird (z. B. in der Universität, in der Bibliothek und im Beruf). Durch die sichtbar aufgedruckten Angaben

172 Siehe § 78 Abs. 1 AufenthG.
173 Siehe BT-Drs. 17/3354, zu Nr. 4 (§ 78), S. 15.

sollten keine Informationen zu einer persönlichen Geschichte als politisch verfolgte oder geflüchtete Person deutlicher offengelegt werden, als dies bei der bloßen Angabe einer Rechtsvorschrift der Fall ist.

4. Automatisierte Abfragen im Fahreignungsregister in Verkehrsordnungswidrigkeitenverfahren

Im Rahmen von Ordnungswidrigkeitenverfahren bei Verkehrsverstößen führte die Bußgeldstelle der Polizei auch automatisierte Abfragen im Fahreignungsregister (FAER) durch. In einem konkreten Fall wandte sich eine betroffene Person an uns, deren Daten aus dem FAER abgerufen worden waren, obwohl sie zum Zeitpunkt der Abfrage noch nicht als fahrende Person feststand.

Die Bußgeldstelle hatte bei einer fotografisch dokumentierten Geschwindigkeitsüberschreitung automatisiert sowohl die Anhörung des Halters als auch die FAER-Abfrage zu seiner Person veranlasst. In dieser Konstellation ist in der Regel lediglich das Kennzeichen des Fahrzeugs bekannt, aber noch nicht die Identität der tatsächlich fahrenden Person.

Nach § 28 Straßenverkehrsgesetz (StVG) wird das FAER zur Speicherung von Daten geführt, die u. a. für die Prüfung der Berechtigung, die Beurteilung der Eignung und der Befähigung von Personen zum Führen von Kraftfahrzeugen erforderlich sind. Die gespeicherten Daten dürfen für die Verfolgung von Ordnungswidrigkeiten an die zuständigen Stellen übermittelt werden, soweit dies zur Erfüllung der diesen Stellen obliegenden Aufgaben erforderlich ist.[174]

Im vorliegenden Fall wurde eine Abfrage zum Fahrzeughalter durchgeführt, obwohl der Fahrzeughalter noch nicht als fahrende Person feststand. Eine solche Abfrage darf erst dann zweck- und zielgerichtet erfolgen, wenn bereits die Identität der fahrenden Person geklärt ist. Zum maßgeblichen Zeitpunkt der Abfrage bestand damit kein hinreichender Tatverdacht gegen Person des Fahrzeughalters, sodass die Abfrage (noch) nicht zur Aufgabenerfüllung der Bußgeldstelle erforderlich war. Es lag damit ein Verstoß gegen

174 § 30 Abs. 1 Nr. 2 StVG.

§ 47 Nr. 1 Bundesdatenschutzgesetz (BDSG)[175] vor, da für die automatisierte Abfrage vor Feststellung der Fahrereigenschaft keine Rechtsgrundlage bestand.

Bereits 2021 hatte uns die Polizei in einem vergleichbaren Verfahren mitgeteilt, dass sie die automatisierten FAER-Abfragen selbst für nicht rechtskonform halte, und Maßnahmen zur Änderung angekündigt. Dennoch wurde die Praxis offenbar fortgesetzt. Wir haben aufgrund des wiederholten Verstoßes gegen die gesetzlichen Vorgaben daher eine Beanstandung ausgesprochen.[176] Da die angekündigten Abhilfemaßnahmen trotz Kenntnis der fehlerhaften technischen Konfiguration nicht erfolgten und so fortlaufend rechtswidrige Datenabfragen stattfanden, kam eine mildere Mangelfeststellung[177] nicht mehr in Betracht. Die Polizei teilte uns daraufhin mit, dass ab Februar dieses Jahres bei sog. Kennzeichenanzeigen keine automatisierte FAER-Anfrage mehr erfolgt.

Der Fall verdeutlicht die Bedeutung einer strikten Zweckbindung und Erforderlichkeit bei automatisierten Datenabfragen zur Verfolgung von Verkehrsordnungswidrigkeiten. Die Möglichkeit technisch einfacher Abfragen darf nicht dazu führen, dass Daten ohne hinreichenden Anlass abgerufen werden. Technische Abfragesysteme müssen kontinuierlich auf ihre Rechtskonformität überprüft und ggf. unverzüglich angepasst werden.

5. Nachweisbarkeit der Zulässigkeit von erweiterten Melderegisterauskünften

Wir haben festgestellt, dass die Aufbewahrungsfristen für die elektronische Protokollierung einer erweiterten Melderegisterauskunft und für die Unterlagen zum Nachweis eines berechtigten Interesses für eine solche Auskunft in den Meldebehörden auseinanderfallen. Betroffene Personen hatten Anträge auf Auskunft nach Art. 15 Datenschutz-Grundverordnung (DSGVO) gestellt, da sie zum Teil Zweifel an der Rechtmäßigkeit der Übermittlung aus dem Melderegister hatten. Zwar konnte ihnen die Tatsache der erweiterten Melderegisterauskunft mitgeteilt werden, nicht aber, aus

175 Für das Ordnungswidrigkeitenverfahren gilt gem. § 46 Abs. 1 Gesetz über Ordnungswidrigkeiten (OWiG) über § 500 Abs. 1 StPO der 3. Teil des BDSG.
176 Siehe § 13 Abs. 2 Satz 1 Berliner Datenschutzgesetz (BlnDSG).
177 Siehe § 13 Abs. 2 Satz 2 BlnDSG.

welchem Grund ihre Daten an andere Personen oder Stellen übermittelt wurden, weil diesbezügliche Unterlagen in den Meldebehörden bereits vernichtet waren.

Das Bundesmeldegesetz (BMG) sieht vor, dass Privatpersonen oder private Stellen auf Antrag unter bestimmten Voraussetzungen eine Auskunft aus dem Melderegister über eine andere Person erhalten können.[178] Bei Vorliegen eines berechtigten Interesses werden der antragstellenden Person oder Stelle neben einer Grundauskunft über Familienname, Vornamen, Doktorgrad, derzeitige Adresse und – soweit die Person verstorben ist, über diese Tatsache – auch weitere Daten, wie bspw. Tag und Ort der Geburt, frühere Namen sowie die derzeitige Staatsangehörigkeit mitgeteilt.[179] Der Antragsteller bzw. die Antragstellerin muss hierfür gegenüber der Meldebehörde ein berechtigtes Interesse „glaubhaft machen", d. h. er bzw. sie muss in dem schriftlichen Antrag auf Erteilung der erweiterten Melderegisterauskunft Tatsachen vorbringen und so substanziiert darlegen, dass die Meldebehörde vom Vorliegen der Tatsachen mit überwiegender Wahrscheinlichkeit ausgehen kann. Zur Glaubhaftmachung können zudem alle üblicherweise im Verwaltungsverfahren zulässigen Beweismittel herangezogen werden.[180]

Die bei den Meldebehörden durch die Antragsteller:innen zum Nachweis des berechtigten Interesses eingereichten Dokumente (Anträge sowie beigefügte Unterlagen) wurden in den Meldebehörden bislang nur ein Jahr als Papiervorgang aufbewahrt. Gleichzeitig waren im entsprechenden IT-Fachverfahren VOIS die erteilten Melderegisterauskünfte für zwei Jahre elektronisch protokolliert, wobei hier aus technischen Gründen nur ein Schlagwort für die Begründung des berechtigten Interesses hinterlegt werden kann. Sofern betroffene Personen bei der Meldebehörde daher einen Antrag auf Auskunft nach Art. 15 DSGVO stellten, wurden sie zwar über sämtliche erteilte erweiterte Melderegisterauskünfte der letzten zwei Jahre informiert. Bei Streitfällen oder Unklarheiten, ob tatsächlich ein berechtigtes Interesse vorgebracht wurde, konnte die Meldebehörde jedoch nur noch die innerhalb der letzten zwölf Monate eingegangenen Unterlagen prüfen. Bei älteren Auskünften konnte eine Prüfung der Rechtmäßigkeit der Erteilung weder durch die Meldebehörde noch durch uns als zuständige Aufsichtsbehörde erfolgen. Dies stellt einen Verstoß gegen die aus Art. 15 DSGVO für den

178 §§ 44, 45 BMG.
179 § 45 Abs. 1 BMG.
180 Siehe die nicht abschließende Aufzählung in § 26 Verwaltungsverfahrensgesetz (VwVfG).

Verantwortlichen folgende Dokumentationspflicht sowie gegen die gegenüber uns als Aufsichtsbehörde bestehende Rechenschafts- und Nachweispflicht der Meldebehörde dar.[181]

Sämtliche Unterlagen, die im Rahmen eines Antrags auf Erteilung einer erweiterten Melderegisterauskunft bei der Meldebehörde eingehen, müssen so lange aufbewahrt werden, dass eine angemessene Zeit für die Prüfung der Rechtmäßigkeit der Datenübermittlung zur Verfügung steht. Jedenfalls dürfen die Dauer der elektronischen Protokollierung und die Dauer der Aufbewahrung von Papierunterlagen nicht auseinanderfallen. Wir befinden uns hierzu derzeit in einem Abstimmungsverfahren mit dem Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) als für das IT-Fachverfahren zuständige Behörde, um eine sachgerechte Lösung zu finden.

6. Beschränktes Auskunftsrecht gegenüber Rechtsanwält:innen

Regelmäßig erhalten wir Beschwerden zu Anträgen auf Auskunft gegenüber Kanzleien oder Einzelrechtsanwält:innen, die nicht oder nicht vollständig beantwortet werden. Rechtsanwält:innen unterliegen als Verantwortliche grundsätzlich den Regelungen der DSGVO und müssen daher auch geeignete Maßnahmen ergreifen, um der betroffenen Person die jeweiligen Informationen und Mitteilungen zu übermitteln.[182] Das Recht der betroffenen Personen auf Auskunft kann gegenüber Rechtsanwält:innen jedoch u. U. beschränkt sein. Dies hängt mit deren Stellung als sog. Berufsgeheimnisträger:innen bzw. mit der anwaltlichen Verschwiegenheitsverpflichtung zusammen.[183]

Besteht ein Mandatsverhältnis mit einem Rechtsanwalt oder einer Rechtsanwältin, so können Mandant:innen ihre Betroffenenrechte aus der DSGVO grundsätzlich geltend machen. Sofern allerdings kein Mandatsverhältnis besteht, kann die Auskunftserteilung durch den Verantwortlichen aufgrund einer bereichsspezifischen Regelung in § 29 Abs. 1 Satz 2 BDSG gegenüber der betroffenen Person u. U. verweigert werden.

181 Siehe Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO.
182 Siehe Art. 12 DSGVO.
183 Siehe § 203 Abs. 1 Nr. 3 Strafgesetzbuch (StGB), § 43a Abs. 2 Satz 1 Bundesrechtsanwaltsordnung (BRAO) i. V. m. § 2 Abs. 1 Satz 1 Berufsordnung für Rechtsanwälte (BORA).

Demnach besteht das Recht auf Auskunft der betroffenen Person nach Art. 15 DSGVO nicht, „soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen." Eine solche Geheimhaltungsvorschrift stellt z. B. § 43a Abs. 2 Bundesrechtsanwaltsordnung (BRAO) dar.

Bereits aus dem Wortlaut der Vorschrift des § 29 Abs. 1 Satz 2 BDSG („soweit") folgt aber, dass das Auskunftsrecht einer betroffenen Person gegenüber einem Rechtsanwalt bzw. einer Rechtsanwältin nicht generell ausgeschlossen ist. Vielmehr müssen Rechtsanwält:innen in jedem Einzelfall prüfen, ob und inwieweit durch die Auskunftserteilung an eine Person Informationen herausgegeben würden, die geheimhaltungsbedürftig sind bzw. unter die anwaltliche Verschwiegenheitspflicht fallen. Es besteht bspw. keine Pflicht, über offenkundige Tatsachen zu schweigen, sowie in Fällen, in denen kein Geheimhaltungsbedürfnis besteht. Der Auskunftsanspruch nach Art. 15 DSGVO entfällt somit nur, wenn dessen Erfüllung Tatsachen berühren würde, die nicht offenkundig sind und dem anwaltlichen Geheimnisschutz unterfallen.[184]

Rechtsanwält:innen sollten auf ein Auskunftsersuchen nach Art. 15 DSGVO daher stets binnen Monatsfrist reagieren.[185] Soweit eine Auskunft (teilweise) verweigert wird, ist dies ohne Verzögerung, spätestens aber innerhalb eines Monats der antragstellenden Person mitzuteilen und zu begründen. Hierbei sollte man sich ggf. auf die einschlägigen Rechtsvorschriften beziehen. Zudem ist die betroffene Person über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen, zu informieren.[186]

184 Siehe auch Oberlandesgericht (OLG) Brandenburg, Beschluss vom 5. November 2025, 1 U 16/25.
185 Siehe Art. 12 Abs. 3 DSGVO.
186 Siehe insgesamt Art. 12 Abs. 4 DSGVO.

Art. 15 DSGVO ist grundsätzlich gegenüber Rechtsanwält:innen anwendbar, jedoch besteht das Recht auf Auskunft nicht, soweit Geheimhaltungspflichten bestehen. Rechtsanwält:innen dürfen Auskunftsanträge nach Art. 15 DSGVO jedoch nicht pauschal ablehnen, sondern müssen im Einzelfall prüfen, ob und inwieweit das Auskunftsrecht der antragstellenden Person aufgrund des Mandatsgeheimnisses bzw. der anwaltlichen Verschwiegenheitspflicht ausgeschlossen ist. Gegebenenfalls muss eine Teilauskunft erteilt werden.

7. Datenschutzkonforme Durchführung einer politischen Onlineabstimmung

Der Bundesverband einer politischen Partei richtete auf seiner Website eine öffentliche Onlineabstimmung ein, über die sich Nutzer:innen zu geplanten politischen Maßnahmen positionieren konnten. Aufgrund der Befürchtung, die Umfrage könne durch Teilnehmende manipuliert worden sein, wurde sie später eingestellt. Daraufhin wandten sich mehrere Personen in Sorge an uns, dass ihre Daten abgeflossen oder unbefugt verknüpft worden sein könnten.

Die Partei reagierte zeitnah und umfassend auf unsere Stellungnahmeersuchen: Die Abstimmungsergebnisse wurden nicht mit personenbeziehbaren Daten verknüpft, sondern lediglich gezählt. Zur Verhinderung von Mehrfachabstimmungen kamen u. a. Zugriffsbeschränkungen (sog. Rate-Limiter) und Sitzungs-Cookies (sog. Session-ID-Cookies) mit zufällig erzeugter Kennung zum Einsatz. Es ergaben sich keine Anhaltspunkte dafür, dass personenbezogene Daten unbefugt an Dritte weitergegeben wurden oder abgeflossen waren.

Die Verarbeitung personenbeziehbarer Daten wie IP-Adressen ist bei Website-Besuchen technisch erforderlich, um den Abruf zu ermöglichen. Die darüber hinausgehende Datenverarbeitung diente hier dem legitimen Zweck, Manipulationen zu verhindern. Entscheidend war, dass eine Verknüpfung mit dem konkreten Abstimmungsergebnis nicht stattfand. Das verhinderte mögliche Rückschlüsse darauf, wer wie abgestimmt hatte. Die beschriebene Form der Verarbeitung personenbezogener Daten zur Verhinderung von Mehrfachabstimmungen ist zulässig. Sie dient auch dann dem berechtigten Interesse, die Integrität einer Abstimmung zu gewährleisten, wenn die Abstimmung

lediglich ein Meinungsbild wiedergeben soll und keine direkten Rechtsfolgen zeitigt.[187] Gleichzeitig ermöglicht die gewählte Form der Datenverarbeitung eine niedrigschwellige und datenschutzfreundliche Teilnahme an einer Onlineabstimmung, da keine Registrierung oder weitergehende Identifizierungspflichten bestehen.

Im Zuge des öffentlich gewordenen Manipulationsverdachts wandten sich zahlreiche Personen mit Auskunftsersuchen an die Verantwortliche. Die Partei teilte uns mit, dass sie trotz der hohen Anzahl von Anfragen in der Lage war, alle Auskunftsansprüche fristgemäß zu erfüllen. Beschwerden über die Bearbeitung dieser Auskunftsersuchen erreichten uns nicht.

Der Fall zeigt, wie wichtig eine transparente Aufklärung ist, wenn Verantwortliche selbst Zweifel an der Integrität ihrer digitalen Instrumente äußern und damit Unsicherheit bei den Teilnehmenden auslösen: Die Partei hatte die Abstimmung mit der öffentlichen Begründung eingestellt, das Ergebnis könne manipuliert worden sein. Die konstruktive Zusammenarbeit mit uns ermöglichte eine zeitnahe Prüfung, wodurch besorgten Teilnehmenden Entwarnung gegeben werden konnte. Der Fall unterstreicht, dass politische Akteure bei digitalen Beteiligungsformaten von Beginn an proaktiv über die technische Umsetzung und entsprechende Datenschutzmaßnahmen informieren sollten.

187 Siehe Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

VIII. Gesundheit

1. Umgang mit Behandlungsakten nach Abschluss einer Behandlung

Nach Abschluss einer Behandlung in einer Arztpraxis haben Patient:innen mitunter den Wunsch, dass ihre Daten entweder umgehend gelöscht oder deren Verarbeitung eingeschränkt wird. Behandlungsakten sind jedoch in der Regel für die Dauer von zehn Jahren nach Abschluss einer Behandlung aufzubewahren und dürfen in diesem Zeitraum nicht gelöscht werden. Ein Recht auf Einschränkung der Verarbeitung nach Art. 18 Datenschutz-Grundverordnung (DSGVO) gegenüber der Arztpraxis besteht in diesem Zusammenhang ebenfalls nicht. Davon unberührt bleibt, dass Ärzt:innen durch technisch-organisatorische Maßnahmen[188] eine rechtmäßige Verarbeitung sicherstellen müssen.

Regelmäßig erreichen uns Beschwerden und Anfragen rund um den Umgang mit Behandlungsakten in Arztpraxen. Dabei geht es etwa darum, wer Zugriff auf die Daten hat und wie lange sie gespeichert werden. Die Behandlungsakte ist in der Regel für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren.[189] In dieser Zeit können ehemalige Patient:innen die Löschung ihrer Daten nicht verlangen.

Teilweise wenden sich ehemalige Patient:innen stattdessen mit dem Anliegen an uns, dass die Verarbeitung ihrer personenbezogenen Daten nach Art. 18 DSGVO eingeschränkt werden soll. Eine Einschränkung der Verarbeitung nach Art. 18 DSGVO kann z. B. umfassen, dass ausgewählte personenbezogene Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden.[190] Außerdem sollte die Einschränkung der Verarbeitung durch technische Mittel so erfolgen, dass die personenbezogenen Daten in keiner Weise weiterverarbeitet werden können.[191] Im Fall einer Einschränkung der Verarbeitung nach Art. 18 DSGVO dürfen die entsprechenden personenbezogenen

188 Siehe u. a. Art. 32 DSGVO.
189 § 10 Abs. 3 der Berufsordnung der Ärztekammer Berlin, § 630f Abs. 3 Bürgerliches Gesetzbuch (BGB), sofern nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen.
190 Erwägungsgrund (ErwGr.) 67 DSGVO.
191 Ebd.

Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden. Diese spezifischen Anforderungen unterscheiden sich von den generellen Anforderungen an die technisch-organisatorischen Maßnahmen, die Ärzt:innen bei der Verarbeitung personenbezogener Daten erfüllen müssen.

Ein Recht auf Einschränkung der Verarbeitung ergibt sich in den beschriebenen Fällen weder aus der DSGVO noch aus dem Bundesdatenschutzgesetz (BDSG). Nach Art. 18 Abs. 1 lit. c DSGVO bestünde bspw. ein Recht auf Einschränkung der Verarbeitung, wenn der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person auf sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen angewiesen ist. In diesem Fall läge die Löschung der personenbezogenen Daten nicht im Interesse der betroffenen Person, sondern hätte ggf. negative Auswirkungen zur Folge. In den hier in Frage stehenden Sachverhalten im Hinblick auf die Behandlungsakten darf eine Löschung aufgrund der gesetzlichen Aufbewahrungsfristen aber gerade noch nicht erfolgen. Nach dem BDSG tritt an die Stelle des Rechts auf Löschung die Einschränkung der Verarbeitung, wenn einer Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen.[192] Jedenfalls § 630f Abs. 3 BGB, in dem eine grundsätzliche zehnjährige Aufbewahrungsfrist für Behandlungsakten normiert ist, stellt indes eine gesetzliche, und keine satzungsgemäße oder vertragliche Aufbewahrungsfrist dar. Sinn und Zweck der Regelung im BDSG ist der Schutz des Verantwortlichen vor einer Pflichtenkollision, wenn sich das Recht auf Löschung und satzungsgemäße oder vertragliche Aufbewahrungspflichten gegenüberstehen.[193] Dieser Konflikt ist für den Fall gesetzlicher Aufbewahrungsfristen bereits durch Art. 17 Abs. 3 lit. b DSGVO gelöst.

Behandlungsakten in Arztpraxen sind in der Regel für zehn Jahre aufzubewahren. In dieser Zeit können Betroffene nicht verlangen, dass die Daten gelöscht werden oder die Verarbeitung dieser Daten nach den speziellen Anforderungen der DSGVO hierfür eingeschränkt wird. Unbeschadet dessen müssen Arztpraxen durch geeignete technisch-organisatorische Maßnahmen eine rechtmäßige Verarbeitung sicherstellen.

192 § 35 Abs. 3 i. V. m. Abs. 1 Satz 2 BDSG i. V. m. Art. 18 DSGVO.
193 BT-Drs. 18/11325, S. 106.

2. Aufsichtszuständigkeit und Durchsetzung von Betroffenenrechten beim Einsatz von Terminverwaltungsdienstleistern

In den vergangenen beiden Jahren berichteten wir über die Aufsichtszuständigkeit für die deutsche Niederlassung eines Terminverwaltungsunternehmens zur Onlinebuchung von Arztterminen mit Sitz in Berlin. Mittlerweile ist geklärt, dass die zuständige federführende Aufsichtsbehörde die für die Hauptniederlassung des Unternehmens zuständige Aufsichtsbehörde in einem anderen europäischen Mitgliedstaat ist. Betroffene Personen können sich trotzdem direkt an uns wenden. Im Rahmen einer behördlichen Voruntersuchung können auch wir darauf hinwirken, dass dem Begehren von Beschwerdeführenden entsprochen wird.

Immer wieder erreichen uns Beschwerden betreffs Internetplattformen zur Onlinebuchung von Arztterminen.[194] Teilweise richten sich diese Beschwerden direkt gegen die jeweilige Arztpraxis, die für die Datenverarbeitung auch bei Inanspruchnahme eines Dienstleisters für die Terminbuchung verantwortlich bleibt. Sie ist in der Pflicht, einen rechtmäßigen und datenschutzkonformen Einsatz in ihrer Praxis sicherzustellen.[195] Für Berliner Arztpraxen und weitere Leistungserbringer:innen in Berlin sind wir die zuständige Aufsichtsbehörde.

In anderen Fällen erhalten wir Beschwerden und Hinweise gegen die Terminverwaltungsunternehmen selbst. Nachdem wir im Jahr 2024 gemeinsam mit der zuständigen Aufsichtsbehörde eines anderen europäischen Mitgliedstaates geklärt haben, dass die Konzernmutter eines dieser Terminverwaltungsunternehmen Verantwortliche für die Datenverarbeitungen im Zusammenhang mit der Internetplattform ist, übermitteln wir Beschwerden nunmehr grundsätzlich zur federführenden Bearbeitung an diese Aufsichtsbehörde.[196] Soweit sich Beschwerdeführende allerdings bezüglich der Durchsetzung ihrer Betroffenenrechte an uns wenden, hat der Europäische Datenschutzausschuss (EDSA) interne Leitlinien entwickelt, die die Möglichkeit der Durchführung einer

194 Siehe dazu auch C.VI.2.
195 Siehe ebd.
196 Siehe JB 2024, A.IX.2.

sog. Vorprüfung vor der Übermittlung an die zuständige Aufsichtsbehörde in einem anderen europäischen Mitgliedstaat eröffnet.[197]

Auch im Falle der Berliner Niederlassung des Terminverwaltungsdienstleisters wenden wir dieses Verfahren an. Ist der Mutterkonzern verantwortlich für die Datenverarbeitung und fordert die beschwerdeführende Person Betroffenenrechte ein, treten wir an die in Berlin ansässige Tochtergesellschaft als lokale Niederlassung heran, stellen den Sachverhalt aus Sicht der beschwerdeführenden Person dar und geben allgemeine rechtliche Hinweise sowie eine vorläufige Einschätzung der Rechtslage. Damit erhält das Unternehmen direkt die Gelegenheit, den Sachverhalt zu überprüfen und dem Begehren der betroffenen Person ggf. nachzukommen. Ist dieses Verfahren nicht erfolgreich, übermitteln wir die Beschwerde im Rahmen des europäischen Kooperationsmechanismus an die zuständige federführende Aufsichtsbehörde. Diese hat dann die Möglichkeit, aufsichtsrechtliche Maßnahmen zu ergreifen, falls datenschutzrechtliche Pflichten verletzt wurden. In diesen Fällen bleiben wir Kontaktstelle für die betroffenen Personen und haben die Möglichkeit, einen maßgeblichen und begründeten Einspruch gegen Beschlussentwürfe der federführenden Aufsichtsbehörde einzulegen, falls wir das für erforderlich halten. Zusätzlich informieren wir die zuständige Aufsichtsbehörde des anderen europäischen Mitgliedstaates regelmäßig über die von uns im Rahmen der Vorprüfungen gelösten Beschwerden. Daneben stehen wir zu übergreifenden Themen mit ihr in einem regelmäßigen Austausch.

In Fällen grenzüberschreitender Verarbeitung kann im Rahmen einer Vorprüfung oft eine rasche Abhilfe für Betroffene mit effizientem Ressourceneinsatz erreicht werden. Sollte sich ein Fall durch dieses Verfahren nicht lösen lassen, erfolgt eine Übermittlung an die zuständige federführende Aufsichtsbehörde, die die weiteren Ermittlungen im Kooperationsverfahren führt.

197 EDSA, Internal EDPB Document 6/2020 on preliminary steps to handle a complaint: admissibility and vetting of complaints, abrufbar unter https://www.edpb.europa.eu/system/files/2022-07/internal_edpb_document_062020_on_admissibility_and_preliminary_vetting_of_complaints_en.pdf.

IX. Familie und Soziales

1. Multiinstitutionelle Fallkonferenzen in Hochrisikofällen (Fortsetzung)

Die Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung (SenASGIVA) und die Senatsverwaltung für Inneres und Sport (SenInnSport) haben ein Rahmenkonzept zum Gefährdungsmanagement und zur Durchführung multiinstitutioneller Fallkonferenzen in Hochrisikofällen bei häuslicher Gewalt und Stalking veröffentlicht, auf dessen Grundlage nunmehr Fallkonferenzen zum Schutz betroffener Frauen durchgeführt werden sollen.

Wir standen mit SenASGIVA schon im vergangenen Jahr zur Entwicklung des Konzepts zur Durchführung multiinstitutioneller Fallkonferenzen zwischen den mit dem Schutz vor Gewalt gegen Frauen befassten Institutionen im Kontakt.[198] Da ein behörden- und institutionsübergreifender Austausch zu konkreten Einzelfällen datenschutzrechtliche Grundpositionen berührt, ist dieser genau zu betrachten. Für jede einzelne Datenübermittlung im Rahmen einer Fallkonferenz bedarf es einer Erlaubnis für die übermittelnde Institution an alle weiteren Beteiligten. Um hier für die Praxis praktikable Hilfestellungen zu entwickeln, haben wir vorgeschlagen, gemeinsam mit der Senatsverwaltung praxisbezogene Handlungsleitfäden für die einzelnen Institutionen zu erarbeiten. Damit wollten wir den Fachkräften die notwendige Sicherheit in Bezug auf die bestehenden Befugnisse geben und herausfinden, an welcher Stelle ggf. Defizite bestehen könnten. Auf dieses Angebot ist SenASGIVA nicht eingegangen.

Der Presseberichterstattung konnten wir nun entnehmen, dass SenASGIVA die Erstellung eines Gutachtens beauftragt hat, um die bestehenden datenschutzrechtliche Möglichkeiten und Schwierigkeiten bei der Durchführung der Fallkonferenzen zu beleuchten.

Auch das Gutachten kommt zu dem Ergebnis, dass insbesondere die Erarbeitung von detaillierten und praxisnahen Handlungsleitfäden für die beteiligten Personen und

198 JB 2024, A.VIII.3.

deren Schulung von besonderer Relevanz ist. Zudem werden im Gutachten verschiedene Vorschläge zur Ausgestaltung der Fallkonferenzen aufgezählt, neben Schulungen und Leitfäden etwa ein verbindlicher Ablaufplan, Standards für die Protokollierung, die Pseudonymisierung von Daten und sichere Speicher- und Übermittlungswege.

Wir gehen davon aus, dass SenASGIVA und die weiteren teilnehmenden Stellen solche Handlungsleitfäden bereits erstellt haben oder erstellen werden, um Rechtssicherheit für ihre Fachkräfte sowie ausreichende Datenschutzkonformität in diesem sensiblen Bereich herzustellen. Diese Erwartung haben wir der SenASGIVA in einem Schreiben mitgeteilt und darüber hinaus darauf hingewiesen, dass die bislang im Rahmenkonzept fehlenden technisch-organisatorischen Maßnahmen umzusetzen sind, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten.

Insbesondere praxisbezogene Handlungsleitfäden sind aus unserer Sicht aufgrund der äußerst sensiblen Thematik besonders wichtig, um den beteiligten Fachkräften Rechtssicherheit zu geben, die Gefahr von Verwertungsverboten in Strafverfahren zu minimieren und Verstöße gegen gesetzliche Verschwiegenheitspflichten mit strafrechtlicher Relevanz auszuschließen. Wir werden die Umsetzung der Vorgaben bei der Durchführung von Fallkonferenzen weiterhin beobachten.

2. Datenschutzrechtliche Stellung von Verfahrensbeiständen und gerichtlich bestellten Sachverständigen im Familienverfahren

Immer wieder erreichen uns Beschwerden, die die Verletzung von Betroffenenrechten durch Verfahrensbeistände und gerichtlich bestellte Sachverständige im Familienverfahren zum Gegenstand haben. Beide Einrichtungen sind datenschutzrechtlich als eigene Verantwortliche mit entsprechenden Pflichten anzusehen.

In familiengerichtlichen Verfahren ist in verschiedenen Situationen die Einholung eines Sachverständigengutachtens durch das Gericht gesetzlich vorgesehen. So regelt bspw. § 163 Abs. 1 Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG), dass in bestimmten Kindschaftssachen, die etwa die elterliche Sorge oder das Umgangsrecht betreffen, das insoweit erforderliche

Gutachten durch geeignete Sachverständige zu erstatten ist. Dies gilt auch für die Unterbringung Minderjähriger sowie bei freiheitsentziehenden Maßnahmen bei Minderjährigen[199] und bei Verfahren in Betreuungs-[200] oder in Unterbringungssachen[201].

Für die Verarbeitung von personenbezogenen Daten in diesem Zusammenhang stellt sich die Frage der Verantwortlichkeit: Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[202] Beim Einsatz Sachverständiger trifft regelmäßig das Gericht die maßgebliche Entscheidung über den Zweck der Datenverarbeitung: die Erstellung eines Sachverständigengutachtens. Die Aufgabenstellung hierfür ergibt sich aus einer gerichtlichen Beweisanordnung. Hingegen legen primär die Sachverständigen die Mittel der Datenverarbeitung fest, denn sie entscheiden, welche Daten sie erheben und welche sie für die Ausarbeitung des Gutachtens benötigen. Zwar ist grundsätzlich vorgesehen, dass das Gericht die Tätigkeit von Sachverständigen zu leiten hat und befugt ist, den Sachverständigen Weisungen zu erteilen.[203] Sachverständige tragen jedoch grundsätzlich Eigenverantwortung und haben die Aufgabe, unvoreingenommen und unparteiisch eine fundierte Einschätzung zu treffen.

Auch wenn Sachverständigen somit durch die gerichtlichen Vorgaben bei der Ausübung ihrer Tätigkeit Grenzen gesetzt werden können, sind sie im Rahmen dieser Grenzen in der Wahl der Mittel bei der Verarbeitung personenbezogener Daten frei und entscheiden eigenverantwortlich über diese. So legen sie bspw. fest, wie sie den Verfahrensgegenstand untersuchen möchten, und damit auch, wie und welche personenbezogenen Daten sie verarbeiten, um das Gutachten anzufertigen. Auch legen sie fest, welche Schlüsse sie aus den erhobenen personenbezogenen Daten ziehen.

Nur im Ausnahmefall, etwa dann, wenn der gerichtliche Auftrag so eng begrenzt ist, dass Sachverständige keinerlei eigene Entscheidungen hinsichtlich der Mittel und Zwecke der Datenverarbeitung treffen können (etwa bei der spezifischen Untersuchung

199 § 167 FamFG.
200 § 280 FamFG.
201 § 321 FamFG.
202 Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO).
203 Siehe § 404a Zivilprozessordnung (ZPO).

einer Blutprobe), kann die eigene Verantwortlichkeit der Sachverständigen fraglich sein. Diese Fälle dürften in der Praxis allerdings nur eine untergeordnete Rolle spielen.

Auch Verfahrensbeistände nach § 158 FamFG sind datenschutzrechtlich Verantwortliche. Verfahrensbeistände haben das Interesse des Kindes festzustellen und sowohl das objektive Kindeswohl als auch die subjektiven Interessen des Kindes im gerichtlichen Verfahren zur Geltung zu bringen. Hierzu können sie bspw. Einsicht in Gerichtsakten nehmen, Gespräche mit dem Kind führen, mit dem Kind den gerichtlichen Beschluss erörtern oder im Interesse des Kindes Rechtsmittel einlegen und zurücknehmen. Die Art und Weise, wie Verfahrensbeistände ihre Aufgaben erfüllen, steht in ihrem freien Ermessen. Verfahrensbeistände haben eigenständig und weisungsfrei die Rechte des Kindes wahrzunehmen und unterliegen auch nicht der Aufsicht des Gerichts.[204] Damit sind sie zumindest bei der Wahl der Mittel der Verarbeitung personenbezogener Daten frei und entscheiden eigenverantwortlich über diese.

Sowohl gerichtlich bestellte Sachverständige als auch Verfahrensbeistände müssen bei der Ausübung ihrer Tätigkeit als datenschutzrechtlich Verantwortliche die Vorgaben der DSGVO einhalten. Insbesondere obliegt es ihnen damit, die Betroffenenrechte nach Art. 12 ff. DSGVO zu gewährleisten. So sind u. a. gem. Art. 13, 14 DSGVO die betroffenen Personen zu informieren und auch Auskunftsansprüche nach Art. 15 DSGVO zu erfüllen. Eine Auskunft kann, insbesondere wenn dadurch Rechte und Freiheiten anderer Personen beeinträchtigt werden, allerdings beschränkt werden.

204 Siehe OLG Karlsruhe, Beschluss vom 4. Juli 2019, 18 UF 62/19, Rn. 20.

X. Videoüberwachung

1. Videoüberwachung durch die Kultureinrichtung eines Drittstaats

Wir haben in diesem Jahr mehrere Beschwerden zu Videokameras an der Fassade des sog. Russischen Hauses in Berlin erhalten. Wir haben zunächst geprüft, ob und inwieweit das Russische Haus überhaupt unserer Aufsicht untersteht. Sodann haben wir geprüft, ob die Videoüberwachung an sich rechtmäßig ist und inwieweit das Russische Haus die Informationspflichten gegenüber den Betroffenen einhält.

Das Russische Haus ist ein Kultur- und Informationszentrum. Es wird von der Rossotrudnitschestwo betrieben, einer Regierungsagentur, die dem russischen Außenministerium angeschlossen ist. Das Russische Haus stellt aber keine diplomatische Vertretung dar und genießt daher keine Unverletzlichkeit nach dem Wiener Übereinkommen über diplomatische Beziehungen (WÜD). Dies ist auch in dem völkerrechtlichen Abkommen, das die Tätigkeit des Russischen Hauses regelt, explizit festgelegt.[205]

Die Datenschutz-Grundverordnung (DSGVO) ist anwendbar, obwohl es sich bei der Rossotrudnitschestwo um eine öffentliche Stelle eines Drittstaates handelt. Denn die Videoüberwachung erfolgt im Rahmen der Tätigkeiten des Russischen Hauses in der Union und damit im räumlichen Geltungsbereich der DSGVO[206]. Wir sind insoweit die zuständige Datenschutzaufsichtsbehörde.

Hinsichtlich der Videoaufnahmen hat unsere Prüfung ergeben, dass das Russische Haus diese auf überwiegende berechtigte Interessen gem. Art. 6 Abs. 1 Satz 1 lit. f DSGVO stützen kann. Das Russische Haus hat mittels einer Dokumentation vergangener Vorfälle nachgewiesen, dass eine Gefährdungslage besteht, die Videoüberwachungsmaßnahmen

205 Art. 4 Abs. 3 des Abkommens zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Russischen Föderation über die Tätigkeit von Kultur- und Informationszentren vom 4. Februar 2011.

206 Siehe Art. 3 Abs. 1 DSGVO: Handlungen von Stellen aus Drittstaaten in der Union sind nicht vom Anwendungsbereich der DSGVO ausgenommen.

erforderlich macht. Die Kameras erfassen zwar Teile des öffentlichen Straßenlandes, aber lediglich die unmittelbare Umgebung des Russischen Hauses von bis zu ca. einem Meter von dessen Fassade bzw. Eingangsbereich entfernt. Dort kam es in der Vergangenheit zu Sachbeschädigungen und Gefährdungen. Das Russische Haus hat allerdings gegen seine Informationspflicht[207] verstoßen, da es zunächst keine Schilder mit Hinweisen auf die Videoüberwachung und weiteren datenschutzrechtlichen Informationen installiert hatte.

Zwar hat das Russische Haus im Laufe des Verfahrens Hinweisschilder beschafft. Auf diesen haben aber immer noch einige notwendige Informationen gefehlt. So konnten die betroffenen Personen allein aufgrund der Hinweisschilder nicht erkennen, dass die Aufnahmen für einen bestimmten Zeitraum gespeichert und ggf. weiterverwendet werden. Diese Informationen sollten unmittelbar aus den Hinweisschildern hervorgehen, mag es auch im Fall von Videoaufnahmen grundsätzlich zulässig sein, Datenschutzhinweise „stufenweise“ zu erteilen.[208] Dem Russischen Haus haben wir diese Bewertung mitgeteilt.

Auch wenn Einrichtungen von einer Stelle, Organisation, Behörde etc. aus einem Drittstaat betrieben werden, kann der räumliche Anwendungsbereich der DSGVO eröffnet sein, mit der Folge, dass auch die Zuständigkeit der Aufsichtsbehörde gegeben ist. Auf die Rechtsform der Einrichtung bzw. der Betreiberin der Einrichtung kommt es nicht an.

207 Siehe Art. 13 Abs. 1, 2 DSGVO.

208 Siehe auch Europäischer Datenschutzausschuss (EDSA), Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, Rn. 114 f., abrufbar unter https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_de.pdf.

2. Videoüberwachung eines ohne Personal betriebenen Selbstbedienungskiosks

Wir prüften anlässlich einer Beschwerde die Zulässigkeit der Videoüberwachung eines ohne Personal betriebenen Selbstbedienungskiosks. Die angebrachten Dome-Kameras erweckten den Eindruck, öffentliches Straßenland weiträumig zu erfassen. Tatsächlich hatte der Gewerbetreibende den Erfassungsbereich der Videoüberwachung allerdings mittels Verpixelung beschränkt. Wir empfahlen ihm, diesen Bereich für Außenstehende zusätzlich kenntlich zu machen.

Ein auf dem Fußweg frei stehender typischer Zeitungskioskwürfel wurde zu einem autonomen Selbstbedienungskiosk umfunktioniert. Dafür hat der Betreiber in die Außenwände des ehemaligen Zeitungskiosks verschiedene Warenautomaten integriert, die jederzeit von außen ohne Verkaufspersonal bedient und aus denen Waren erworben werden können. An zwei Ecken unter der Überdachung hat der Betreiber zum Schutz vor Vandalismus und zur Aufklärung etwaiger Sachbeschädigungen zwei sog. Dome-Kameras angebracht. Dadurch werden alle vier Seiten des Kiosks videoüberwacht. Da die Dome-Kameras 360-Grad-Rundumaufnahmen ermöglichen, ist für Außenstehende der konkrete Erfassungsbereich nicht ersichtlich. Es bestand die Befürchtung, alle Vorbeilaufenden und -fahrenden würden gefilmt. Auch reichten die von dem Gewerbetreibenden angebrachten Hinweisschilder nicht dafür aus, hinreichende Transparenz über die Videoüberwachung zu schaffen.

Im vorliegenden Fall standen gleich wirksame Alternativen zur Videoüberwachung nicht zur Verfügung. Insbesondere reichte etwa eine Ausleuchtung der Warenautomaten – ggf. über einen Bewegungsmelder – als Schutzmaßnahme nicht aus. Die Videoüberwachung öffentlichen Straßenlandes durch Private ist allerdings nur in sehr begrenztem Umfang zulässig. In der Rechtsprechung ist die Erfassung eines auf einen Meter von der Hausfassade entfernten Bereichs für zulässig erachtet worden, soweit dies für die Dokumentation von Sachbeschädigungen erforderlich ist.[209]

Der Erfassungsbereich der Kameras war mittels Verpixelung auf das zulässige Maß beschränkt. Gleichwohl sollten bei Dome-Kameras weitere Maßnahmen ergriffen

209 Siehe Amtsgericht (AG) Berlin-Mitte, Urteil vom 18. Dezember 2003, 16 C 427/02, Rn. 23.

werden, um den Eindruck der unzulässigen weiträumigen Videoüberwachung zu verhindern, etwa durch Sichtblenden an den Kameras und Markierungen, die visuell verdeutlichen, welcher Bereich von der Videoüberwachung betroffen ist. Wir haben dem Gewerbetreibenden aufgegeben, entsprechend nachzubessern und die Hinweisschilder anzupassen.

Auch beim Einsatz von Videokameras im Rahmen neuartiger Geschäftsmodelle gelten die allgemeinen Anforderungen an die Zulässigkeit einer Videoüberwachung. Grundsätzlich haben Verantwortliche vor der Installation einer Videokamera zunächst immer zu prüfen, ob es gleich geeignete, weniger einschneidende Maßnahmen zur Erreichung des Zwecks der Videoüberwachung gibt. Beim Einsatz von sog. Dome-Kameras ist zu berücksichtigen, dass für Außenstehende eine etwaige Beschränkung des Erfassungsbereichs der Videoüberwachung mittels Verpixelung nicht erkennbar ist und somit der Eindruck der Überwachung entstehen kann, obwohl diese tatsächlich nicht erfolgt. Um dem entgegenzuwirken, sollte der videoüberwachte Bereich bzw. die Beschränkung der Videoüberwachung kenntlich gemacht werden.

XI. Arbeit, Wirtschaft und Finanzen

1. E-Mail-Check bei Abwesenheit von Beschäftigten oder bei Beendigung des Beschäftigungsverhältnisses

E-Mail-Kommunikation spielt in sehr vielen Arbeitsbereichen eine große Rolle. Wir haben eine Reihe von Beratungsanfragen erhalten, die den Umgang mit personalisierten E-Mail-Konten von ausgeschiedenen oder länger abwesenden Mitarbeiter:innen betrafen. Dabei stand im Vordergrund, ob und – wenn ja – wie Arbeitgeber:innen auf das E-Mail-Postfach zugreifen dürfen.

Verantwortliche sollten von Beginn an Prozesse zur Nutzung von E-Mail-Postfächern festlegen, um datenschutzrechtlichen Problemen vorzubeugen. Zunächst kann überlegt werden, ob es tatsächlich personalisierter Postfächer bedarf oder Funktionsadressen ausreichend sind. Wichtige Informationen, auf die mehrere Personen Zugriff haben sollen, können von und an solche Funktionspostfächer (z. B. buchhaltung@verantwortlicher.de) adressiert werden. Sie können nach dem Ausscheiden einzelner Beschäftigter fortgeführt und durch mehrere Personen genutzt werden.

Sollen Postfächer personalisiert sein, müssten Beschäftigte angewiesen werden, grundsätzlich alle für die Zukunft relevanten Inhalte außerhalb ihres persönlichen Postfachs für die Personen, die sie vertreten oder mit denen sie zusammenarbeiten, abzulegen. Für Abwesenheiten sollte zudem ein Abwesenheitsassistent eingerichtet sein, der darüber informiert, dass eingehende E-Mails nicht zur Kenntnis genommen werden und daher ggf. an eine andere E-Mail-Adresse zu senden sind. Bei dauerhafter Abwesenheit sollte das Postfach abgeschaltet werden. Zumindest sollte die Annahme von E-Mails abgelehnt werden, sinnvollerweise ebenfalls in Verbindung mit einem Abwesenheitsassistenten. Ein Sammelpostfach für alle E-Mails, die nicht zugeordnet werden können (ein sog. Catch-all-Postfach), sollte nicht eingerichtet werden. Das könnte zu der Verarbeitung von personenbezogenen Daten führen, die Verantwortliche gar nicht erhalten möchten und für die es auch keine Rechtsgrundlage gibt.

Wenn Beschäftigte ihre Arbeitsstelle länger oder dauerhaft verlassen, sollten sie angewiesen werden, vorher die in ihrem E-Mail-Postfach vorhandenen persönlichen bzw. privaten E-Mails zu löschen. Die betrieblichen E-Mails sind entweder an die Vertretung bzw. Nachfolge weiterzuleiten oder ggf. ebenfalls zu löschen, wenn sie für betriebliche Zwecke nicht mehr benötigt werden.

Wenn dies nicht mehr möglich ist (bspw. bei einer fristlosen Kündigung), sollte eine verantwortliche Person bestimmt werden, die zur Wahrung der schutzwürdigen Interessen der oder des ehemaligen Beschäftigten nur Einsicht in das Postfach nimmt, um betriebliche Mails auszusortieren und offensichtlich private Mails unverzüglich zu löschen. Bei dieser Person kann es sich z. B. um ein Mitglied des Betriebsrats, die bzw. den betriebliche:n Datenschutzbeauftragte:n oder eine von den Betroffenen bestimmte Person handeln.

Die Weiterleitung bzw. Kenntnisnahme von E-Mails ausgeschiedener Mitarbeitender durch die Geschäftsführung ist darüber hinaus zulässig, soweit die E-Mail-Nutzung nur zu betrieblichen Zwecken erlaubt und die Nutzung zu privaten Zwecken ausdrücklich untersagt worden war. Aber auch dann ist zu prüfen, ob jeweils geschäftliche oder private E-Mails vorliegen. Der private Charakter einer E-Mail könnte etwa aus dem Header bzw. durch eine eindeutige Themenbezeichnung erkennbar sein. Erst wenn aufgrund des Headers kein privater Charakter zu erkennen ist, sollte die E-Mail geöffnet werden. Ergibt sich dann aus dem Inhalt doch ein privater Charakter, ist die E-Mail ohne weitere Kenntnisnahme sofort wieder zu schließen. In jedem Fall ist die betroffene Person von einer solchen Maßnahme zu unterrichten.

Soll die private Nutzung der betrieblichen E-Mail-Adresse erlaubt sein, empfiehlt es sich, eine entsprechende Betriebs- bzw. Dienstvereinbarung abzuschließen. In jedem Fall sollten Verantwortliche für ihre Beschäftigten schriftlich festlegen, ob und in welchem Umfang eine private Nutzung der E-Mail-Adressen zulässig ist.

Verantwortliche sollten vorab festlegen, ob eine private Nutzung von beruflichen E-Mail-Postfächern zulässig ist. Sie sollten auch Prozesse festlegen, wie ein personalisiertes Postfach nach dem Ausscheiden von Beschäftigten abgewickelt wird.

2. Datenverarbeitungen durch Personalräte

Personalräten steht das Recht zu, rechtzeitig und umfassend über alle für sie entscheidungsrelevanten Sachverhalte informiert zu werden. Auch müssen sie nicht alle Angelegenheiten hinter verschlossener Tür verhandeln, sondern dürfen – und sollen auch – in den Austausch mit der Belegschaft und der Dienststellenleitung treten. Anhand einiger aktueller Beispiele stellen wir dar, wo die Grenzen des Austauschs liegen können.

Wenn Personalräte Informationen von der Dienststellenleitung wünschen, die einen Personenbezug aufweisen, muss nach Ansicht des Bundesverwaltungsgerichts (BVerwG) geprüft werden, ob die Informationen zur Wahrnehmung der gesetzlichen Aufgaben des Personalrats im Sinne des Verhältnismäßigkeitsgrundsatzes erforderlich sind.[210] In dem konkreten Fall wollte der Personalrat monatlich eine Liste mit den Salden aller Gleitzeitkonten der Beschäftigten vom Dienststellenleiter erhalten, um zu überwachen, ob eine Dienstvereinbarung zur gleitenden Arbeitszeit eingehalten wird. Das BVerwG, das mit dem Beschluss seine ständige Rechtsprechung zu dieser Thematik bestätigt, hat die Erforderlichkeit im vorliegenden Fall verneint. Allerdings sind dem Personalrat von der Dienststellenleitung aussagekräftigte Informationen zur Verfügung zu stellen, mit denen er seiner Überwachungsaufgabe nachkommen kann. Dies können auf einer ersten Stufe anonymisierte oder pseudonymisierte Daten sein. Sollte ein konkreter Bedarf bestehen, bestimmte Informationen personenbezogen zu erhalten, kann der Personalrat dies unter Darlegung der Verhältnismäßigkeit ggf. auf einer zweiten Stufe im Einzelfall verlangen. Dies kommt nach dem Gericht allerdings nur als Ultima Ratio in Betracht.

Ebenso können und sollen Personalräte die Belegschaft zumindest einmal jährlich auf einer Personalversammlung über ihre Arbeit informieren. Schon aus allgemeiner Rücksichtnahme auf die einzelnen Betroffenen verbietet es sich in aller Regel, über Einzelfälle zu sprechen. Eine Ausnahme kann gemacht werden, wenn die betroffene Person hierin ausdrücklich einwilligt oder sich explizit wünscht, als Beispiel genannt zu werden. In einer bei uns eingereichten Beschwerde hat ein Personalrat in einer Personalversammlung personenbeziehbar über Stellenbesetzungsverfahren berichtet. Bei

210 BVerwG, Beschluss vom 29. April 2025, 5 P 7.23.

dem Kreis der Zuhörer:innen musste dabei im vorliegenden Fall davon ausgegangen werden, dass zumindest einigen bekannt war, wer sich auf die Stelle beworben hat. Dadurch bekam die Darstellung des Verfahrens einen Personenbezug.

Hier lag ein Verstoß gegen die gesetzliche Schweigepflicht des Personalrats.[211] Die gesetzliche Schweigepflicht gilt u. a. für Personaleinzelangelegenheiten, die Personalratsmitglieder im Rahmen ihrer Personalratstätigkeit erfahren. Auch wenn der Ablauf der Nichtbesetzung einer Stelle für die Beschäftigten von Interesse sein mag, geht die Schweigepflicht in Bezug auf personenbezogene Daten regelmäßig vor. Es muss in solchen Fällen zwischen allgemein bekannten sowie nicht personenbeziehbaren Informationen auf der einen Seite und geheimhaltungsbedürftigen Informationen auf der anderen Seite unterschieden werden. Dieses Verfahren haben wir mit einem entsprechenden Hinweis an den Personalrat abgeschlossen.

An dieser Stelle noch ein Hinweis: Das Verfahren zur Feststellung, dass ein Personalratsmitglied verhindert ist, wurde in § 28 Abs. 1 Personalvertretungsgesetz Berlin (PersVG Bln) neu gefasst. Dort heißt es jetzt: „Scheidet ein Mitglied aus dem Personalrat aus, so tritt ein Ersatzmitglied ein. Das gleiche gilt für die Zeit, in der ein Mitglied nach der Feststellung des Personalrats verhindert ist." Dies ist eine Änderung zu der vorangegangenen Fassung, in der diese Feststellung nur durch den Vorsitz des Personalrats getroffen wurde. Demnach ist es nun zulässig, dass der gesamte Personalrat von den Verhinderungen weiß und tatsächlich auch den Verhinderungsgrund kennt. Es darf und muss jetzt also ein größerer Personenkreis von dem Verhinderungsgrund Kenntnis erlangen. Trotzdem sollte umsichtig mit diesen Daten umgegangen werden. Insbesondere können die Personalratsmitglieder auf Folgendes hingewiesen werden: Über die Information, dass sie krank sind, und die Krankheitsdauer hinaus sollen keine genaueren Angaben an das Personalratspostfach gesandt werden.

Auch wenn der Personalrat umfassende Informationsrechte hat, muss immer geprüft werden, ob tatsächlich ein Aufgabenbezug besteht, bevor personenbezogene Daten durch den Personalrat verarbeitet werden. Ebenso muss er besonders in Personaleinzelangelegenheiten darauf achten, seine Schweigepflicht einzuhalten.

211 Siehe § 11 PersVG Bln.

3. Vertraulicher Kontakt zu betrieblichen Datenschutzbeauftragten

Verantwortliche und Auftragsverarbeiter müssen die direkten Kontaktdaten ihrer Datenschutzbeauftragten (DSB) veröffentlichen, damit Aufsichtsbehörden und betroffene Personen vertraulich Verbindung zu ihnen aufnehmen können. Wer als Kontaktdaten der betrieblichen DSB nur die des Unternehmens – bzw. eines Datenschutzteams, das für das Unternehmen und nicht lediglich als Hilfspersonal des DSB tätig ist[212] – angibt, verstößt gegen diese Verpflichtung und gegen die Vertraulichkeitspflichten der DSB.

Ein Unternehmen hatte als Kontaktdaten seines DSB neben der Postanschrift eine Telefonnummer und ein Kontaktformular angegeben. Bei Nutzung der Telefonnummer wurde man allerdings an den IT-Service weitergeleitet, der nicht an den DSB durchstellen konnte. Daten, die in das Kontaktformular eingegeben und abgeschickt wurden, gingen an ein Datenschutz-Team, in dem er lediglich Mitglied war. Wir haben das Unternehmen verwarnt, weil es gegen seine Verpflichtung zur Veröffentlichung der Kontaktdaten des DSB[213] und gegen die Vertraulichkeitspflichten des DSB[214] verstoßen hat.

Durch die gesetzlichen Pflichten soll sichergestellt werden, dass sich betroffene Personen und Aufsichtsbehörden ohne Weiteres auf direktem Wege und in vertraulicher Form an die DSB wenden können, ohne mit einem anderen Teil der Einrichtung in Kontakt treten zu müssen.[215] Nur so ist sichergestellt, dass die DSB ihren Kontrollfunktionen und ihrer Funktion als Anlaufstelle für betroffene Personen und Aufsichtsbehörden sowie ihren gesetzlichen Verschwiegenheitspflichten auch gegenüber dem sie benennenden Verantwortlichen nachkommen können. Bereits bei der (Festlegung und) Veröffentlichung der Kontaktdaten der bzw. des DSB muss also gewährleistet sein, dass die Kontaktaufnahme ausschließlich zu ihr bzw. zu ihm führt. Die in der Poststelle für sie oder ihn eingehenden Schreiben dürfen nicht geöffnet werden. Auch auf das Telefon

212 Siehe Art. 38 Abs. 2 Datenschutz-Grundverordnung (DSGVO).
213 Siehe Art. 37 Abs. 7 Var. 1, Art. 13 Abs. 1 lit. b und Art. 14 Abs. 1 lit. b DSGVO.
214 Siehe Art. 38 Abs. 5 DSGVO i. V. m. § 38 Abs. 2 i. V. m. § 6 Abs. 5 Satz 2 Bundesdatenschutzgesetz (BDSG).
215 Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), WP 243 rev.01, Kap. 2.6., abrufbar unter https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html, bestätigt durch den Europäischen Datenschutzausschuss (EDSA).

der bzw. des DSB dürfen ausschließlich sie bzw. er persönlich oder deren bzw. dessen Mitarbeiter:innen gem. der Weisung Zugriff haben.

Es genügte hier also nicht, dass auch der DSB des Unternehmens Zugriff auf die übersandten Kontaktformulare hatte, da dieser Zugriff nicht ausschließlich war. Für betroffene Personen, die vielleicht gerade die oder den DSB kontaktieren wollen, weil sie Probleme mit dem Unternehmen haben, kann eine fehlende Vertraulichkeit ein unüberwindbares Hindernis für die Ausübung ihrer Rechte aus der DSGVO darstellen.

Verantwortliche und Auftragsverarbeiter müssen darauf achten, dass sie tatsächlich die direkten Kontaktdaten ihrer DSB veröffentlichen und bspw. nicht die Kontaktdaten ihres Datenschutz-Teams als Kontaktdaten ihrer DSB bezeichnen. Auf eingehende Nachrichten wie auch auf das Telefon der DSB dürfen nur diese selbst oder ihre ihnen gegenüber weisungsgebundenen Mitarbeiter:innen Zugriff haben. Post an sie darf in der Poststelle nicht geöffnet werden. Eine „Vorfilterung" durch die sie benennende Stelle ist unzulässig – der Gesetzgeber hat den betroffenen Personen das Recht eingeräumt, sich unmittelbar und vertraulich an die DSB zu wenden. Diese Vorgaben korrekt umzusetzen, ist auch im Interesse der benennenden Stellen: Denn wenn die oder der DSB sich eines Problems annimmt, verzichten betroffene Personen ggf. auf eine Beschwerde bei einer Aufsichtsbehörde, die ein entsprechendes behördliches Verfahren nach sich ziehen kann.

4. Klarnamen bei Google-Rezensionen

In eine sprichwörtlich haarige Angelegenheit hat sich ein Friseursalon verwickelt. Ein unzufriedener Kunde hatte nach einem Termin unter Verwendung seines Klarnamens eine negative Google-Bewertung über den Salon veröffentlicht. Als Reaktion darauf veröffentlichte der Friseursalon auf dem Google-Profil des Arbeitgebers des betreffenden Kunden eine negative Bewertung über ihn mit vollständigem Namen und negativen Charakterisierungen.

Hier lag ein Datenschutzverstoß vor, weil die Veröffentlichung der Daten ohne Rechtsgrundlage erfolgte.[216] Zwar kann die Antwort auf eine negative Bewertung einer Friseur-

216 Siehe Art. 6 Abs. 1 Satz 1 DSGVO.

leistung berechtigte Interessen (die Reputation) wahren. Die dargestellte Offenlegung der personenbezogenen Daten war hierfür objektiv jedoch nicht erforderlich. Denn auch ohne die Veröffentlichung der Daten des Rezensenten hätte eine Gegendarstellung zur Wahrung der Reputation erfolgen können.

Zum gleichen Ergebnis kam das Bundesverwaltungsgericht der Republik Österreich (BVwG) in einem ähnlichen Fall:[217] Nach einer missglückten Stornierung veröffentlichte die betroffene Kundin eine kritische Google-Rezension. Der Unternehmer antwortete öffentlich – und nannte dabei den vollständigen Vor- und Nachnamen der Kundin. Einige Wochen später änderte der Unternehmer seine Antwort, beließ es aber bei der vollen Namensnennung. Die Österreichische Datenschutzbehörde verhängte deshalb eine Geldbuße gegen den Unternehmer. Eine Beschwerde des Unternehmers dagegen wies das BVwG ab. Das Gericht hielt in seiner Entscheidung fest, dass die Verarbeitung der betreffenden Daten der Kundin ohne Rechtsgrundlage erfolgte. Eine Antwort auf die Google-Rezension der Kundin sei genauso gut ohne Nennung des Klarnamens möglich gewesen, die Nennung war daher nicht erforderlich und somit rechtswidrig.

Zwar kann die Antwort eines Unternehmens auf eine negative Google-Rezension seiner Reputation dienen und damit berechtigte Interessen wahren. Die Offenlegung des Namens oder anderer personenbezogener Daten von z. B. Kund:innen ist hierfür in aller Regel jedoch nicht erforderlich.

217 Siehe BVwG, Entscheidung vom 2. Juni 2025, BVwG W292 2298457-1. ECLI:AT:BVWG:2025:W292.2298457.1.00, abrufbar unter https://rdb.manz.at/document/ris.bvwg.BVWGT_20250602_W292_2298457_1_00.

5. Empfängerprüfung durch SEPA-Verordnung

Seit Oktober ist im Zahlungsverkehr der Europäischen Union (EU) die sog. Empfängerprüfung[218] durchzuführen. Dabei haben Zahlungsdienstleister die Zahlenden vor Ausführung einer Überweisung darüber zu informieren, ob der von den Zahlenden angegebene Name der Empfänger:innen mit dem beim Zahlungsdienstleister der Empfänger:innen zu der angegebenen IBAN hinterlegten Namen übereinstimmt. Uns haben Anfragen zu der Konstellation erreicht, wenn lediglich eine nahezu vollständige Übereinstimmung zwischen dem angegebenen und dem hinterlegten Namen vorliegt.

Die Pflicht zur Durchführung der Empfängerprüfung folgt aus Artikel 5c der Verordnung (EU) 2024/886[219] (im Folgenden: Verordnung zur Echtzeitüberweisung). Ziel der Regelung ist es, den Schutz vor betrügerischen und fehlgeleiteten Zahlungen im Euro-Zahlungsverkehrsraum zu erhöhen. Unmittelbar nach Eingabe der Überweisungsdaten (Name, IBAN, Betrag) überprüft auf Anfrage des Zahlungsdienstleisters der Zahlenden der Zahlungsdienstleister der Empfänger:innen, ob der zur IBAN hinterlegte Name mit dem angegebenen Namen übereinstimmt. Sofern die Prüfung technisch durchgeführt werden konnte, sind drei Ergebnisse möglich: vollständige Übereinstimmung, keine Übereinstimmung oder nahezu Übereinstimmung. Bei vollständiger Übereinstimmung schließt sich unmittelbar die Autorisierung der Zahlung durch die Zahlenden an. Bei fehlender Übereinstimmung informiert der Zahlungsdienstleister die überweisende Person über das erhöhte Risiko, dass die Überweisung an falsche Zahlungsempfänger:innen gehen könnte. Werden lediglich geringe Abweichungen festgestellt, legt der Zahlungsdienstleister der überweisenden Person den Namen des bzw. der durch die IBAN gekennzeichneten Zahlungsempfängers bzw. -empfängerin offen. Die Zahlenden entscheiden anschließend, ob die Abweichung für sie erheblich ist, und können die Zahlungsdaten korrigieren oder mit den ursprünglich eingegebenen Daten autorisieren. Erteilen sie die Autorisierung trotz des Hinweises, ist der Zahlungsdienstleister bei weisungsgemäßer Ausführung von seiner Haftung befreit.[220]

218 Auf Englisch: Verification of Payee (VoP).

219 Verordnung (EU) 2024/886 des Europäischen Parlaments und des Rates vom 13. März 2024 zur Änderung der Verordnungen (EU) Nr. 260/2012 und (EU) 2021/1230 und der Richtlinien 98/26/EG und (EU) 2015/2366 im Hinblick auf Echtzeitüberweisungen in Euro.

220 Art. 5c Abs. 8 Satz 1 der o. g. Verordnung.

Was relativ einfach klingt, wirft in der Praxis Fragen auf. Die Verordnung zur Echtzeitüberweisung sieht vor: Wenn die Daten nahezu übereinstimmen, ist der „Name des Zahlungsempfängers" anzugeben. Sie lässt jedoch offen, ab welchem Grad eine Übereinstimmung als nahezu zu qualifizieren ist. Damit verlagert sich ein Teil der eigentlich den Zahlenden zugewiesenen Entscheidungskompetenz faktisch auf die Zahlungsdienstleister. Verfügen Zahlungsempfänger:innen über mehrere Vornamen, kann dies dazu führen, dass sämtliche hinterlegten Vornamen als Abweichungsinformation angezeigt werden. Dies birgt die Gefahr, dass personenbezogene Daten offengelegt werden, die für die konkrete Zahlungsentscheidung nicht erforderlich sind. Auch gezielte Ausspähungsversuche könnten dadurch begünstigt werden.

Die technische Umsetzung der Empfängerprüfung erfolgt europaweit auf Grundlage des „Verification of Payee Scheme Rulebook" des European Payments Council (EPC)[221]. Maßgeblich ist dabei, dass bei nahezu übereinstimmenden Daten ergänzende Informationen angezeigt werden dürfen, um eine bewusste Zahlungsentscheidung zu ermöglichen. Zwar hat der EPC unverbindliche Empfehlungen zur Datenminimierung beim Namensabgleich erlassen, nach denen der antwortende Zahlungsdienstleister nur diejenigen Namensbestandteile übermitteln soll, die bereits Gegenstand der Anfrage waren.[222] In der Praxis wird diese Empfehlung jedoch scheinbar nicht von allen Zahlungsdienstleistern umgesetzt. Aus Datenschutzsicht sollten zusätzliche Vornamen jedenfalls nur dann angezeigt werden, wenn sie für die Risikoentscheidung der Zahlenden relevant sind und keine mildere, datenminimierende Variante zum selben Ergebnis führt. So könnte bspw. der Hinweis, dass weitere Vornamen zum Zahlungsempfänger vorhanden sind, bereits ausreichend sein.

Bei der Empfängerprüfung für Überweisungen ist es maßgeblich, welche Informationen für eine sichere Zahlungsentscheidung tatsächlich erforderlich sind. Im Rahmen der Empfängerprüfung sollten die Zahlenden lediglich zur Korrektur der

221 EPC 218-23/2024, Version 1.0, abrufbar unter https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-10/EPC218-23%20v1.0%202024%20Verification%20Of%20Payee%20Scheme%20Rulebook_0.pdf.

222 EPC, Recommendations for the Matching Process under the VOP Scheme Rulebook, EPC 218-23/2024, Version 1.0, abrufbar unter https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-10/EPC288-23%20v1.0%20EPC%20Recommendations%20for%20the%20Matching%20Processes%20under%20the%20VOP%20Scheme%20Rulebook_0.pdf.

eingegebenen Daten angehalten werden, ohne dass zusätzliche personenbezogene Daten des Zahlungsempfängers offengelegt werden. Datenschutzfreundliche Alternativen wie die Anzeige von Hinweistexten („weitere Vornamen vorhanden“) sind zu bevorzugen, solange sie den Zweck gleichermaßen erfüllen. Für Zahlungsdienstleister ergibt sich daraus die Aufgabe, ihre Prüfmechanismen so auszugestalten, dass Fehlüberweisungen wirksam verhindert und zugleich unnötige Offenlegungen personenbezogener Daten vermieden werden.

6. Seriennummern bei Banknoten

Bargeld gilt weithin als Inbegriff des anonymen Zahlens. Zugleich zeigt es sich, dass technische Infrastrukturen Seriennummern von Banknoten erfassen können. Das Ergebnis ist ein differenziertes Bild: Bargeld ist in der Regel ein datensparsames Zahlungsmittel; gleichwohl können auch Bargeldzahlungen nachverfolgt werden.

Bargeld ermöglicht Zahlungen ohne Nutzerkonten, ohne dauerhafte Identifikatoren und ohne zentrale Protokollierung einzelner Zahlungsvorgänge. Für alltägliche Transaktionen bedeutet dies ein hohes Maß an informationeller Selbstbestimmung: Wer bar zahlt, hinterlässt in der Regel keine personenbezogenen Datenspuren bei Zahlungsdienstleistern oder Plattformen. Diese Eigenschaften tragen dazu bei, dass Bargeld häufig als Instrument zum Schutz von Freiheit und Privatsphäre betrachtet wird.

Technische Entwicklungen relativieren dieses Bild jedoch: Moderne Geldbearbeitungsmaschinen, Ein- und Auszahlungsautomaten sowie Sicherheitssysteme können die individuellen Seriennummern[223] von Banknoten erfassen, etwa zur Falschgeldprävention, Logistiksteuerung oder Diebstahlsaufklärung. Dabei werden die Banknoten mit Kameras oder Bildsensoren erfasst, der Bereich der Seriennummer wird automatisiert ausgelesen und mittels optischer Zeichenerkennung (OCR) in maschinenlesbaren Text überführt. Werden diese Informationen systematisch gespeichert und mit

223 Die Banknoten der zweiten Euro-Serie tragen auf der Rückseite eine Seriennummer als waagerechte Nummer. Diese besteht aus zwei Buchstaben, gefolgt von zehn Ziffern. Der erste Buchstabe gibt Auskunft über die Druckerei. Der zweite Buchstabe hat keine besondere Bedeutung, ermöglicht aber eine größere Anzahl von Seriennummern; abrufbar unter https://www.bundesbank.de/action/de/642688/bbksearch?pageNumString=0.

Orts-, Zeit- oder weiteren Kontextdaten verknüpft, kann im Einzelfall eine nachträgliche Rekonstruktion von Umlaufwegen einzelner Banknoten möglich werden. Dies betrifft vor allem Situationen, in denen Bargeld in automatisierte Prozesse eingebunden ist.

Banknoten als solche enthalten keine personenbezogenen Daten der das Bargeld nutzenden Personen. Werden jedoch die auf Banknoten verzeichneten Seriennummern mit den genannten Zusatzinformationen kombiniert, die eine Identifizierung von Personen ermöglichen, kommt das Datenschutzrecht zur Anwendung. Eine solche Verarbeitung ist nur im Rahmen der datenschutzrechtlichen Erlaubnistatbestände zulässig, etwa zur Erfüllung gesetzlicher Pflichten oder auf Grundlage einer Einwilligung. Dabei sind insbesondere die Grundsätze der Zweckbindung und Datenminimierung zu beachten. Kreditinstitute, Betreiber:innen von Geldautomaten und Dienstleister:innen sind gehalten, nur erforderliche Daten zu verarbeiten und diese nicht zur Erstellung von Bewegungs- oder Verhaltensprofilen zu verdichten. Dafür konnten wir im Rahmen eines von uns durchgeführten Verfahrens bisher keine Anhaltspunkte finden.

Bei alledem zeigt sich eine konzeptionelle Parallele zum geplanten digitalen Euro.[224] Dessen Offlinevariante soll ausdrücklich „bargeldähnliche“ Eigenschaften bieten, insbesondere eine hohe Privatsphäre und fehlende Transaktionsverfolgungsmöglichkeiten. Fachliche Gutachten weisen jedoch darauf hin, dass die technische Realisierung einer vollständig anonymen, zugleich fälschungssicheren und massentauglichen Offlinelösung mit erheblichen Herausforderungen verbunden ist. Die Diskussion um Seriennummern bei Banknoten verdeutlicht, dass es anspruchsvoll sein kann, Anonymität unter realen Betriebsbedingungen dauerhaft zu gewährleisten.

Bargeld bleibt ein datensparsames Zahlungsinstrument, gerade im Vergleich zu konten- und datengetriebenen digitalen Zahlungsverfahren. Zugleich zeigt der Blick auf Seriennummern, dass auch analoges Geld in digitalen Infrastrukturen neue Formen der Beobachtbarkeit erfahren könnte. Für die Diskussionen um die Gestaltung des digitalen Euro lässt sich daraus lernen, dass seine mögliche „Bargeldähnlichkeit“ nicht nur programmatisch behauptet, sondern auch technisch und rechtlich belastbar umgesetzt werden muss.

224 Siehe dazu D.II.1.

XII. Datenschutzvorfälle und Technischer Datenschutz

1. Datenschutzvorfall bei den Berliner Verkehrsbetrieben

Im Frühjahr dieses Jahres kam es zu einem Angriff auf die IT-Systeme eines Dienstleisters der Berliner Verkehrsbetriebe (BVG), von dem ca. 180.000 Datensätze von Kund:innen der BVG betroffen waren. Die BVG hat uns den Vorfall gemeldet und die betroffenen Personen darüber informiert. In der Folge haben uns zahlreiche Anfragen erreicht. Wir haben die Betroffenen zu ihren Rechten beraten und geprüft, inwieweit die BVG ihrerseits ihre Pflichten im Umgang mit dem Vorfall und ihre Kontrollpflichten gegenüber ihrem Dienstleister eingehalten hat.

Die BVG hatte den Dienstleister mit einer Versandaktion beauftragt. Von dem Datenschutzvorfall waren potenziell alle Personen betroffen, die im Januar dieses Jahres von der BVG im Zusammenhang mit dem Tarifprodukt „Berlin Abo“ kontaktiert wurden. Die betroffenen Daten waren Namen, Anschriften, Vertrags- und Kundennummern sowie ggf. E-Mail-Adressen, nicht aber etwa Bankdaten oder Passwörter.

Nach der Prüfung des Vorgangs kamen wir zu dem Ergebnis, dass die BVG ihre Kontrollpflichten gegenüber dem Dienstleister nicht ausreichend ausgeübt hat: Verantwortliche Stellen müssen sicherstellen, dass Dienstleister, die, wie hier, für sie Daten im Auftrag verarbeiten (sog. Auftragsverarbeiter), die Daten nach Ende des Auftrags löschen. Sie dürfen sich dabei nicht allein darauf verlassen, dass der jeweilige Auftragsverarbeiter sich an zuvor vertraglich vereinbarte Löschpflichten hält. Die BVG hatte sich im vorliegenden Fall nicht bei ihrem Dienstleister vergewissert, ob dieser die Daten nach Abschluss der Versandaktion gelöscht hat. Hätte die BVG ihre Kontrollrechte ausgeübt, wäre der Datenschutzvorfall mit hoher Wahrscheinlichkeit verhindert worden.

Zudem hat die BVG ihre Meldepflicht gegenüber uns nicht rechtzeitig erfüllt. Verantwortliche Stellen müssen Datenschutzvorfälle, sofern diese meldepflichtig sind, unverzüglich – innerhalb von 72 Stunden, nachdem sie ihnen bekannt geworden sind – an

die zuständige Aufsichtsbehörde melden.[225] Dies gilt auch für den Fall, dass sich der Datenschutzvorfall, wie vorliegend, nicht unmittelbar bei der verantwortlichen Stelle, sondern bei einem Auftragsverarbeiter ereignet hat. Die Frist beginnt in einem solchen Fall regelmäßig, sobald die verantwortliche Stelle von ihrem Auftragsverarbeiter über den Datenschutzvorfall informiert wurde. Die BVG hätte hier mit ihren Untersuchungen zur Aufklärung früher beginnen und diese zügiger abschließen müssen.

Verantwortliche Stellen haben auch dann Meldepflichten zu erfüllen, wenn sich Datenschutzvorfälle bei ihrem Auftragsverarbeiter ereignen. Damit es hier keine Verzögerungen gibt, sollten sowohl zwischen Auftragsverarbeiter und verantwortlicher Stelle als auch innerhalb der verantwortlichen Stelle die Abläufe im Fall eines Datenschutzvorfalls im Vorfeld klar festgelegt sein. Zudem muss sichergestellt werden, dass es dabei nicht deshalb zu Verzögerungen kommt, weil der Verantwortliche die Datenverarbeitung auf einen Auftragsverarbeiter ausgelagert hat. Nach Abschluss des Auftrags muss sich die verantwortliche Stelle zudem vergewissern, dass die betroffenen Daten gelöscht worden sind. Wo keine Daten sind, können Dritte auch nicht unberechtigt auf diese zugreifen. Den von einem Datenschutzvorfall betroffenen Personen raten wir, auf eventuell auftretende ungewöhnliche Kontaktaufnahmen zu achten, die sie etwa dazu verleiten sollen, weitere Informationen preiszugeben.

2. Dienstleister für Rechtsanwält:innen informiert unzureichend über Sicherheitslücke

Aufgrund einer Sicherheitslücke in einer Software für Rechtsanwält:innen zur Verwaltung ihrer Mandate konnte auf die Backup-Daten der Kanzleien zugegriffen werden. Das Unternehmen, das diese Software für die Rechtsanwält:innen als Auftragsverarbeiter betrieben hat, kam seiner Verpflichtung zur Meldung des Datenlecks gegenüber den Verantwortlichen nicht nach.

Durch einen Hinweis von Sicherheitsforschenden stellte sich heraus, dass bei der Umsetzung der Software als Cloud-Version eine Reihe von Fehlern gemacht wurde. Die

225 Art. 33 Abs. 1 Satz 1 Datenschutz-Grundverordnung (DSGVO).

Software generierte regelmäßig Backup-Daten, die in eindeutig benannten Dateien in einem festen Unterverzeichnis der Instanz abgelegt wurden. Der Pfad zu diesen Backup-Daten war ohne Zugriffsbeschränkung aus dem Internet abrufbar. Das Unternehmen argumentierte, dass dies kein Sicherheitsrisiko darstelle, da die Domainnamen der produktiven Instanzen nicht bekannt seien. Diese Einschätzung teilten wir nicht: Die virtuellen Server besaßen zusätzliche, fortlaufend durchnummerierte Domainnamen, die sich systematisch durchsuchen ließen und zudem in einer einschlägigen Suchmaschine auffindbar waren. Die Backup-Daten waren zudem unzureichend mit einem veralteten Standardverfahren verschlüsselt, bei dem es Angriffsmöglichkeiten gibt, insbesondere wenn man von Teilen der verschlüsselten Daten die Klartexte kennt. Hier ergab sich aus der frei nutzbaren Demoversion der Software, dass es identische Beispiel-Dateien in jeder Instanz und damit in jedem Backup gab.

Die so abrufbaren Backup-Daten enthielten umfangreichen Schriftverkehr der Rechtsanwält:innen mit Mandanten, gegnerischen Anwält:innen sowie anderen Gegenparteien und den Gerichten. Zusätzlich enthielten die Backup-Daten Zugangsdaten zu E-Mail-Accounts und zum besonderen elektronischen Anwaltspostfach (beA), womit man potenziell diese Postfächer hätte übernehmen können.

Innerhalb kurzer Zeit nach Kenntnis des Datenschutzvorfalls wurden vom Unternehmen Maßnahmen ergriffen, um die Sicherheitslücke zu schließen. Später fanden die Sicherheitsforschenden jedoch noch weitere Angriffsmöglichkeiten, die dann ebenfalls geschlossen werden mussten. Zudem wurde endlich eine Sicherheitsüberprüfung der Software durch ein spezialisiertes Unternehmen durchgeführt.

Ausreichend informiert wurden die Kund:innen trotz mehrfacher Aufforderung durch uns allerdings bis Ende dieses Jahres nicht.[226] Dadurch war es den betroffenen Rechtsanwält:innen nicht möglich, ihren Benachrichtigungspflichten nachzukommen.[227] Das Unternehmen erklärte: Es habe die Sicherheitslücke untersucht und festgestellt, dass diese nicht kritisch sei, weil niemand außer den Sicherheitsforschenden auf Daten zugegriffen habe. Allerdings konnte für einen Großteil des Zeitraums wegen nicht mehr vorhandener Protokolldaten gar nicht mehr nachvollzogen werden, ob Zugriffe stattgefunden haben. Unabhängig davon bestand über lange Zeit ein hohes Risiko,

226 Siehe Art. 33 Abs. 2 DSGVO.
227 Siehe Art. 33, 34 DSGVO.

dass – potenziell – umfangreiche sensible und der anwaltlichen Schweigepflicht unterliegende Daten in falsche Hände gelangen, selbst wenn niemand auf diese Daten zugegriffen haben sollte. Eine Abgabe an die Sanktionsstelle wird geprüft.

Auftragsverarbeiter haben in der Praxis meistens die vollständige technische Kontrolle über die Datenverarbeitungsprozesse. Die Verantwortlichen für die Datenverarbeitung müssen dennoch über eingetretene Datenschutzvorfälle informiert werden, um die Risiken selbst einschätzen und angemessen reagieren zu können.

3. Technische Aspekte von Datenschutzvorfällen

Seit Jahren erreichen uns immer wieder Hinweise auf Sicherheitslücken, die auf relativ simple und wiederkehrende Fehler in Webanwendungen zurückzuführen sind. So auch dieses Jahr: Das Buchungssystem einer Hotelgruppe ermöglichte durch eine unzureichende Zugriffskontrolle den Abruf fremder Buchungsdaten einschließlich sensibler Reisepassdaten.

Das Buchungssystem einer Hotelgruppe ermöglichte den Kund:innen den Download der Rechnung zu einer Hotelbuchung über einen Link, der als wesentlichen Bestandteil eine Buchungsnummer enthielt. Mit diesem Link war einerseits der Abruf der jeweiligen Rechnung mit den darin enthaltenen personenbezogenen Daten möglich, andererseits wurde – ohne dass dies notwendig gewesen wäre – auch ein unternehmensinterner Datensatz ausgeliefert, der die kompletten Buchungsdaten wie die E-Mail-Adresse der buchenden Person, den Reisezweck (geschäftlich, privat) sowie Namen, Geschlecht, Nationalität, Geburtsdatum und Passdaten (Passnummer und Ausstellungsdatum) auch sämtlicher angegebenen Mitreisenden enthielt. Die Buchungsnummer wurde dabei fortlaufend vergeben und das Buchungssystem überprüfte vor Ausgabe der Daten zwar, ob die abrufende Person über eine gültige Sitzungskennung verfügte, aber nicht, ob die eingeloggte Person auch tatsächlich eigene Buchungen abrief. So war es durch einfache Veränderung der Buchungsnummer in der URL möglich, jeden beliebigen anderen Buchungsdatensatz abzurufen.

Potenziell gefährdet waren bis zu 500.000 Buchungsdatensätze. Im Laufe der Bearbeitung konnte die Hotelgruppe jedoch nachweisen, dass nur eine niedrige zweistellige

Zahl von unberechtigten Zugriffen auf Rechnungen bzw. Buchungsdatensätze erfolgt war. Zudem konnten alle diese Zugriffe den Sicherheitsforschenden zugeordnet werden, die die Sicherheitslücke gemeldet hatten.

Eine systematische Berücksichtigung von IT-Sicherheitsprinzipien bereits in der Entwicklungsphase sowie regelmäßige Sicherheitsaudits können Schwachstellen bei technischen Zugriffskontrollmechanismen verhindern und damit sowohl die Betroffenen als auch die Unternehmen vor erheblichen Schäden schützen. Hierzu gehört die Umsetzung von grundlegenden Aspekten wie dem Least-Privilege-Prinzip[228] und der Validierung[229] von Benutzerberechtigungen.

4. Unbemerkte Aufzeichnung von Telefongesprächen durch fehlerhafte Testkonfiguration

Ein IT-Dienstleister und seine Kund:innen meldeten uns dieses Jahr einen ungewöhnlichen Vorfall: Über mehr als ein Jahr wurden unbemerkt alle Telefonate aufgezeichnet, die über eine für mehrere Kund:innen betriebene Telefonanlage geführt wurden. Ein automatisches Löschskript beseitigte diese Aufzeichnungen täglich, sodass der Vorfall nicht auffiel. Erst als eine Systemänderung das Skript unwirksam machte und Speicherüberläufe auftraten, wurden die Aufzeichnungen entdeckt.

Die Telefonanlage wurde im Rahmen eines Projekts zwischen 2022 und 2023 eingeführt. Bestandteil des Projekts war zunächst auch eine Aufzeichnungsfunktion für Telefonate, die jedoch während der Projektumsetzung verworfen wurde. Eine automatische Löschfunktion für eventuelle Aufzeichnungen wurde dennoch, wie ursprünglich vorgesehen, implementiert und funktionierte bis zum Zeitpunkt der Entdeckung des Vorfalls zuverlässig. Die Aufzeichnungsfunktion wurde dann im November 2023 bei abschließenden Qualitäts- und Lasttests der Anlage aktiviert, bei denen auf dem Produktivsystem Telefonate zu Testzwecken aufgezeichnet wurden. Nach Abschluss der Tests wurde jedoch vergessen, diese Funktion wieder zu deaktivieren. Da die aufgezeichneten Daten ohnehin täglich automatisch gelöscht wurden, fiel dieser Konfigurationsfehler

228 Prinzip der geringsten Berechtigung.
229 Bestätigung der Gültigkeit.

nicht auf. Eine Protokollierung der Aufzeichnungen und Funktionalitäten zur systematischen Auswertung der Audiodaten wurde nicht vorgenommen.

Besonders problematisch war, dass der Dienstleister die Telefonanlage als Dienstleistung zur Vermittlung von Telefongesprächen unterschiedlichen Kund:innen anbot, die alle von dem Vorfall betroffen waren. Im Rahmen unserer Analyse des Vorfalls untersuchten wir mit dem Dienstleister, wer während der Tests, im darauffolgenden Produktivbetrieb und zum Zeitpunkt der Unwirksamkeit der Löschroutine Zugriff auf die aufgezeichneten Daten hatte. Dabei handelte es sich ausschließlich um sicherheitsüberprüfte und vertraulichkeitsverpflichtete Administrator:innen, die auch sonst Möglichkeiten zum Zugriff auf die Systeme gehabt hätten. Weiterhin wurden keine Metadaten aufgezeichnet, die ohne inhaltliche Auswertung der eigentlichen Audiodaten hätten genutzt werden können. Aufgrund der Nutzungszeiten und Löschzeitpunkte waren die Gesprächsdaten bis zur Kenntnisnahme des Vorfalls jeweils nur 18 Stunden im System verfügbar, in denen ein Zugriff durch Unbefugte hätte möglich sein können. Es existierten keine systematischen Zugriffsmöglichkeiten, außer denen der Administrator:innen. Letztere unterliegen einem Rollen- und Rechtekonzept und werden regelmäßig automatisch protokolliert und überwacht, sodass unberechtigte Zugriffe ausgeschlossen werden konnten.

Die meldenden Kund:innen teilten mit, dass kein hohes Risiko für die Betroffenen aus der ungewollten Aufzeichnung der Gespräche abgeleitet wurde und folglich keine Pflicht zur Benachrichtigung gesehen werde. Wir hatten keine Anhaltspunkte, die gegen diese Risikoanalyse sprachen. Wir wiesen jedoch die Verantwortlichen darauf hin, dass es hinsichtlich des mutmaßlichen Vertrauensverlusts bei Bekanntwerden des Vorfalls hilfreich sein könnte, diesen selbst proaktiv zu kommunizieren.

Der Fall offenbarte Mängel im Umgang mit Anforderungen, Testprozessen und dem Betriebsmonitoring durch den Dienstleister. Die Durchführung der Tests auf dem Produktivsystem im November 2023 entspricht nicht den etablierten IT-Sicherheitspraktiken. Tests sollten nach Möglichkeit stets in separaten Testumgebungen durchgeführt werden, die von produktiven Systemen getrennt sind. Die fehlende Deaktivierung der Aufzeichnungsfunktion nach Abschluss der Tests zeigt zudem, dass in der Testplanung keine vollständig definierten Rückbauschritte existierten. Ein ordnungsgemäßes Testkonzept muss nicht nur die Durchführung der Tests, sondern auch die vollständige Rücknahme aller zu Testzwecken vorgenommenen Konfigurationsänderungen vorsehen.

Offenbar war auch das Betriebsmonitoring nicht geeignet, alle Konfigurationszustände kontinuierlich zu überwachen. Dadurch hätte die aktivierte Aufzeichnungsfunktion unmittelbar nach den Tests erkannt und gemeldet werden können. Moderne Konfigurationsmanagement-Systeme ermöglichen es, Soll-Konfigurationen zu definieren und Abweichungen automatisch aufzuspüren. Eine Überwachung der Speichernutzung und Protokollierung war zwar vorhanden, aber im Hinblick auf die Erkennung dieses Vorfalls nicht geeignet konfiguriert. Wenn nicht vermieden werden kann, dass Testszenarien sensible Funktionen – wie hier die Aufzeichnung von Gesprächen auf Produktivsystemen – aktivieren, müssen besondere Sicherungsmaßnahmen wie zeitlich befristete Aktivierungen mit automatischer Deaktivierung oder Vier-Augen-Prinzipien bei der Konfigurationsänderung vorgesehen werden.

Besonders bemerkenswert ist im beschriebenen Fall, dass trotz der lang andauernden unbeabsichtigten Aufzeichnung der Telefongespräche aufgrund der vorhandenen Zugangskontrollen, der automatischen Löschung und der fehlenden Metadaten kein hohes Risiko für Betroffene entstand. Dies zeigt, dass technische und organisatorische Maßnahmen nach Art. 32 DSGVO auch dann wirken können, wenn andere Kontrollen versagen.

Die Trennung von Test- und Produktivumgebungen ist eine fundamentale Voraussetzung für sichere und datenschutzkonforme IT-Systeme. Kontinuierliches Betriebsmonitoring darf sich nicht auf die Verfügbarkeit von Diensten beschränken, sondern muss auch Konfigurationszustände, Speichernutzung und Logging-Aktivitäten umfassen. Die Definition und Dokumentation von Testszenarien müssen explizit auch die Rücknahme von Testkonfigurationen vorsehen.

XIII. Datenhandel

Obwohl hier umfassende Informationen über viele Millionen Menschen gehandelt werden, sind die konkreten Verarbeitungsvorgänge und Unternehmen aus dem Bereich Datenhandel der Öffentlichkeit meist nicht bekannt. Bereits im letzten Jahr[230] wiesen wir auf Risiken für den Datenschutz im Bereich der Onlinewerbung und unsere diesbezügliche Tätigkeit hin. Seither haben wir uns insbesondere mit dem Bereich Datenhandel vertiefend beschäftigt. Am Beispiel der personalisierten Onlinewerbung geben wir einen genaueren Einblick in das Geschäftsmodell und die Wege, auf denen personenbezogene Daten in enormem Umfang erhoben, zusammengeführt und verkauft werden.

Durch vermehrte Medienberichterstattung rückte das Thema Datenhandel in den vergangenen zwei Jahren in den Fokus der Öffentlichkeit.[231] Datenhandel kann als die gewerbliche Verarbeitung personenbezogener Daten verstanden werden, insbesondere die Sammlung, die Zusammenführung und die Weitergabe zum Zwecke der Anreicherung, der Profilbildung oder zum Ausspielen personalisierter Werbung. Die Verarbeitung erfolgt dabei meist ohne konkretes Wissen der Betroffenen und ist mit erheblichen Risiken verbunden. Datenhandel kann zu intransparenter Profilbildung sowie zum Kontrollverlust im Hinblick auf die Anzahl und die Identität der datenverarbeitenden Stellen führen bzw. im Hinblick auf die Zusammenhänge, in denen diese mit Wirkung für die betroffenen Personen verwendet werden können. So wird die Vielzahl von zum Teil sensiblen Daten im Rahmen des Ökosystems von Werbenetzwerken zum Verkauf von personalisierten Bannerwerbeplätzen oder sonstiger Internetwerbung verwendet, aber auch umfassende Datensets über Datenhandelsplätze an einen offenen Interessentenkreis verkauft.

Datenhandel bringt auch gesellschaftliche Herausforderungen mit sich. So ermöglicht eine umfassende Profilbildung die zielgerichtete Ansprache einzelner Bevölkerungsgruppen sowie die Ausspielung gezielter – ggf. auch manipulativer – Botschaften. Wenn die freie Meinungsbildung gefährdet ist, gerade auch im politischen Bereich und im Vorfeld von Wahlen, dann hat das negative Auswirkungen auf demokratische Prozesse.

230 JB 2024, A.XII.1.
231 Siehe bspw. https://netzpolitik.org/tag/datenhandel/#netzpolitik-pw.

Beim Datenhandel sind eine Vielzahl an Unternehmen beteiligt. Die wichtigsten Funktionen am Beispiel von Onlinewerbenetzwerken sind die Folgenden:

- **Publisher** (meist: Websitebetreiber oder Plattform): Stellt Werbeflächen auf seiner eigenen Website oder in seiner eigenen App zur Verfügung und versteigert diese zur Anzeige personalisierter Werbung. Oft agiert ein Publisher auch als Datenlieferant, da er über wertvolle verhaltens- oder kontextbasierte Nutzerdaten (z. B. Seitenaufrufe, Interessen, Standort) seiner Besucher:innen verfügt.

- **Supply Side Plattform:** Hilft dabei, Werbeflächen automatisiert und effizient in Millisekunden an Werbetreibende bzw. Demand Side Plattforms zu verkaufen.

- **Werbenetzwerk** (auch: Intermediary): Versammelt mehrere Unternehmen und vermittelt diesen die vom Publisher etc. erhaltenen Daten und Angebote für Werbeflächen.

- **Datenhandelsplattform**: Vermittelt interessierte Unternehmen und stellt Vertriebskanäle sowie standardisierte Schnittstellen zum Erwerb und Austausch von Daten bereit.

- **Data Management Plattform:** Strukturiert und analysiert Daten, um Segmente und Zielgruppen (sog. Audiences) zu erstellen. Erlaubt es, Daten aus eigenem Bestand (z. B. aus dem firmeneigenem Kundenverwaltungssystem) oder fremden Quellen anzureichern. Data Management Plattforms erlauben es also, Daten aus verschiedenen Quellen zusammenzuführen und damit neue Informationen abzuleiten.

- **Demand Side Plattform:** Nimmt für werbetreibende Unternehmen oder Werbeagenturen an Versteigerungen von Werbeplätzen teil und verkauf diese dann an ihre Auftraggeber weiter.

Werbeplätze im Internet werden meist innerhalb von wenigen Millisekunden nach dem Öffnen einer Website versteigert (sog. Real Time Bidding). Die Versteigerung und ggf. der Weiterverkauf des Werbeplatzes an Agenturen oder andere Unternehmen erfolgt automatisiert anhand von Angebot und Nachfrage.

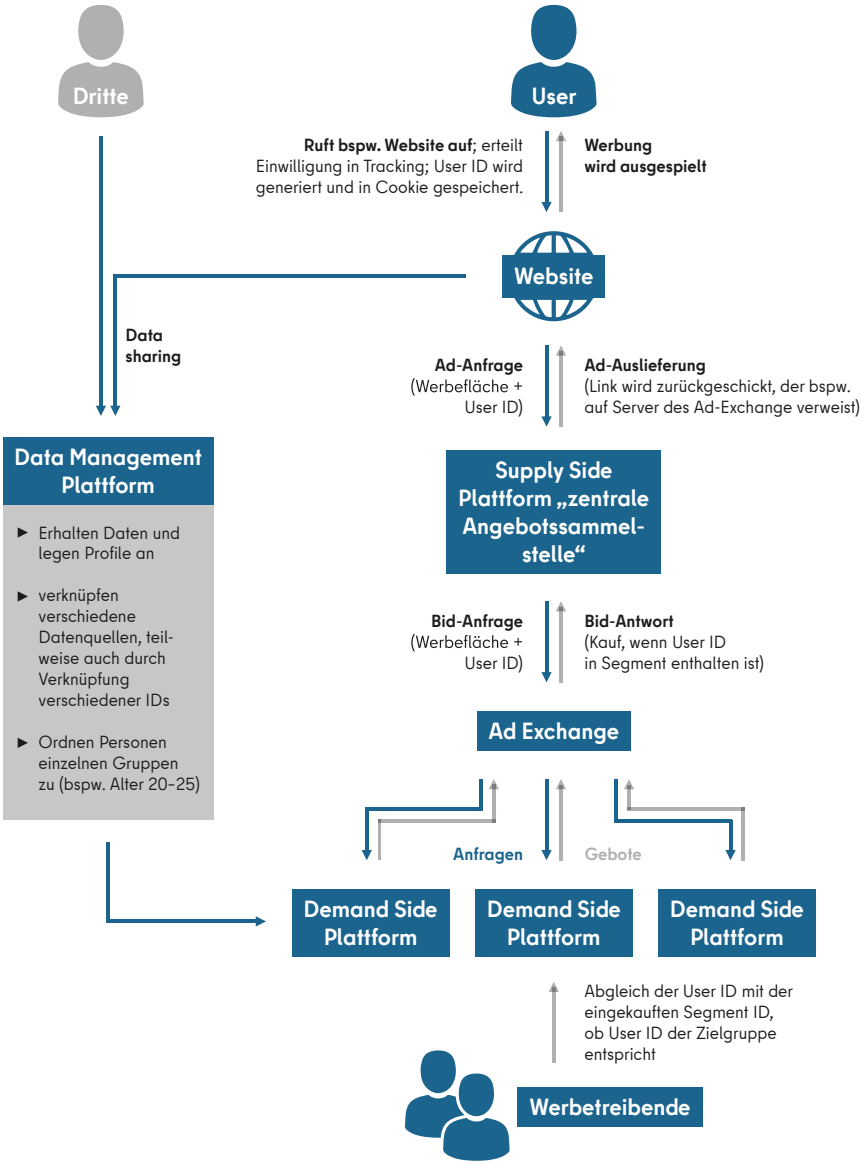
Versteigert werden dabei nicht nur die Werbeplätze: Nach Erhalt einer Einwilligung unterbreitet ein Publisher über eine Supply Side Plattform einer Vielzahl an

Unternehmen, die über eine Demand Side Plattform auf die Werbefläche bieten, das Angebot, einen Werbeplatz im Rahmen einer Versteigerung zu mieten und einer bestimmten Besucherin oder einem Besucher einer Website auf diesem Wege Werbung auszuspielen. Dieser sog. Bid Request enthält u. a. eine Werbe-ID, die die Seitenbesucher:innen unter bestimmten Umständen eindeutig identifizierbar und damit auch quer über verschiedene Websites und Dienste verfolgbar machen. Daneben können auch Angaben über potenzielle Interessen der jeweiligen Person für eine möglichst gezielte Werbeausspielung weitergegeben werden. Regelmäßig spielen hierbei auch Standortdaten eine große Rolle. Der ebenfalls mit übersandte Datensatz zeigt üblicherweise an, für welche Daten die Seitenbesucherin bzw. der Seitenbesucher eine Einwilligung abgegeben hat.

Zudem: Mit der Offenlegung dieser Informationen gegenüber allen beteiligten Akteur:innen eines Werbenetzwerks gelangen die Daten der Besucherin oder des Besuchers einer Website zu diesen Unternehmen. An diesem Punkt entsteht ein großes Missbrauchsrisiko. Möglich sind dann u. a. die Verarbeitung der erhaltenen Daten zu ganz anderen als den angedachten Zwecken, eine Verarbeitung von Daten über das von der Einwilligung abgedeckte Maß hinaus oder sogar die Weitergabe der Daten an Unternehmen außerhalb des Werbenetzwerks (z. B. durch einen Verkauf an Datenhändler:innen, ggf. auch über Datenhandelsplattformen). Beschränkt werden diese Verarbeitungen bislang in erster Linie über vertragliche Absicherungen der Werbeindustrie. Hier kommt es in der Praxis teilweise zu sog. Unterlizenzierungen, also der Datenweitergabe an Dritte im Rahmen eines zivilrechtlichen Vertrags. Eine derartige Verarbeitung ist jedoch in den meisten Fällen unzulässig, da regelmäßig keine (wirksame) Einwilligung zu diesem Datenverkauf vorliegt und die Verantwortlichen derartige Weitergaben auch nicht auf ein berechtigtes Interesse stützen können.

Datenschutzrechtlich stellen sich außerdem besonders die Frage nach der Verantwortlichkeit, also welches Unternehmen über die Zwecke und Mittel der Datenverarbeitung entscheidet, sowie die Frage nach der Zulässigkeit der Offenlegung personenbezogener Daten an andere Unternehmen.

Wir empfehlen daher, im Bereich von Onlinewerbung auf personalisierte Werbung möglichst zu verzichten und auf weniger verarbeitungsintensive Möglichkeiten auszuweichen. Denkbar ist hier der Einsatz von kontextbasierter Werbung, um intensive



Übersicht über ein typisches Werbenetzwerk

Verarbeitungen personenbezogener Daten unter Beteiligung einer Vielzahl an unterschiedlichen Akteur:innen zu vermeiden.

Betroffene Personen sollten im Internet und insbesondere im Rahmen von Websites und Apps Folgendes beachten, um das Risiko des Handels mit ihren eigenen Daten zu reduzieren:

- Machen Sie sich mit der Datenschutzerklärung der genutzten Dienste vertraut. Prüfen Sie, welche Daten eine Website oder App von Ihnen erhebt.

- Willigen Sie nur in die Verarbeitungen ein, über die Sie sich ausreichend informiert fühlen. Widerrufen Sie ggf. andere Einwilligungen. Prüfen Sie, ob Sie einzelnen Verarbeitungen, die Sie nicht möchten, widersprechen können.

- Überprüfen Sie die Datenschutzeinstellungen: Welchen Zugriff hat der Dienst auf Ihr Gerät, Ihre Kontakte oder Ihren Standort?

- Entscheiden Sie, ob Sie den Dienst unter diesen Umständen weiterhin nutzen möchten. Wenn nicht, können Sie jede App (vorübergehend) löschen oder Ihr Konto deaktivieren. Seien Sie zurückhaltend mit dem, was Sie teilen. Geben Sie keine sensiblen Informationen weiter.

- Berücksichtigen Sie etwaige Prüfungen oder Entscheidungen der Aufsichtsbehörden in Bezug auf dieses Unternehmen oder eine bestimmte App.

Beim Datenhandel wirken eine Vielzahl von Unternehmen darauf hin, Daten natürlicher Personen anzureichern und mit weiteren Unternehmen zu teilen. Dabei entstehen aussagekräftige Profile, die u. a. zur gezielten Beeinflussung ganzer Bevölkerungsgruppen missbraucht werden können. Verantwortliche sollten bei der Nutzung eines komplexen Systems in besonderem Maße prüfen, ob sie den Transparenzanforderungen der Datenschutz-Grundverordnung (DSGVO) entsprechen können. Obwohl die Ermittlung der beteiligten Akteur:innen und das Nachvollziehen der Datenströme eine große Herausforderung für die Aufsichtsbehörden darstellen, arbeiten wir weiter an der Durchsetzung der bestehenden gesetzlichen Vorgaben in Berlin, Deutschland und Europa.

XIV. Beschwerdeverfahren zu Betroffenenrechten

Die Bearbeitung von Beschwerden von Bürgerinnen und Bürgern zählt zu einer der Hauptaufgaben der Aufsichtsbehörden. In diesem Jahr konnten wir einen besonders starken Anstieg der Eingaben verzeichnen, insbesondere im Banken- und Finanzbereich. Außerdem beschäftigten (un)berechtigte Datenübermittlungen an Inkassounternehmen, die zwangsweise Nutzung von mobilen Apps und die Folgen von Identitätsdiebstählen die Bürger:innen sehr.

Die eigenen Rechte im Zusammenhang mit der Verarbeitung von persönlichen Daten spielen für viele eine immer größer werdende Rolle in ihrem Alltag. Dass sich im Zuge der fortschreitenden Digitalisierung viele ehemals analog abgewickelte Vorgänge ins Internet oder das eigene Mobiltelefon verlagern, verstärkt diese Sensibilisierung. Dies zeigt sich auch an dem Anstieg von Eingaben und Beschwerden, die wir erhalten haben.[232]

Viele Unternehmen nutzen mittlerweile mobile Applikationen („Apps"), um ihre Dienstleistung oder ihren Service anzubieten. Dies darf indes nicht dazu führen, dass bspw. Betroffenenrechte ausschließlich über die Verwendung einer solchen App ausgeübt werden können. Die Nutzung derartiger Selbstbedienungstools (auch Self-Service-Tools genannt) ersetzt die Ausübung von Betroffenenrechten nicht und darf diese auch nicht einschränken.[233] Unternehmen müssen stets eine Kontaktvariante anbieten, die es auch ohne die (meist datenintensiveren) Apps auf dem eigenen Mobiltelefon ermöglicht, bspw. ein Nutzungskonto zu löschen oder Auskunft über die eigenen Daten zu erhalten. Wenn die betroffenen Personen statt der Nutzung der Selbstbedienungstools bspw. per E-Mail um eine Datenlöschung bitten, ist es für Unternehmen grundsätzlich unzulässig,

232 Siehe E.I.

233 Siehe Europäischer Datenschutzausschuss (EDSA), Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.0, Rn. 138, abrufbar unter https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202201_data_subject_rights_access_v2_de.pdf.

die Bearbeitung des Löschersuchens unter Verweis auf ein über ein Kundenkonto erreichbares Selbstbedienungstool zu verweigern.

Gerade bei der Nutzung von Finanzdienstleistungen scheint die Verwendung von Apps stark auf dem Vormarsch. Gefördert wird dies auch durch niedrigschwellige Angebote zur Teilnahme am Aktienhandel oder dem Zeichnen von börsengehandelten Fonds. Hier sollten Bürger:innen jedoch besonders vorsichtig sein, da meist sehr sensible Daten benötigt werden, um diese Dienstleistungen zu nutzen. Das erhöhte Eingabeaufkommen in diesem Bereich spricht zudem dafür, dass einige Unternehmen Schwierigkeiten haben, Betroffenenrechte zu wahren oder entsprechende Anfragen rechtskonform zu bearbeiten.

Eine von vielen unangenehmen Folgen, die sich aus dem unsachgemäßen Umgang mit personenbezogenen Daten ergeben können, ist der Diebstahl der eigenen Identität, die dann bspw. in Onlineshops für Bestellungen missbraucht werden kann. Hierzu erhalten wir seit Jahren viele Eingaben.[234] Im Falle eines Identitätsdiebstahls sind den hiervon betroffenen Personen auf Anfrage sämtliche auf ihre Person bezogenen Daten zu beauskunften, inklusive derjenigen Daten, die ggf. Aufschluss über die Betrüger:innen geben können.[235]

Bei Identitätsdiebstählen schließt sich oft weiterer Ärger an, wenn eine aufgrund des Betrugs widerrechtlich erhobene Forderung an ein Inkassounternehmen abgetreten wird, das dann an die Opfer herantritt, um den offenen Betrag beizutreiben. Vorbeugend sollten betroffene Personen umgehend der gegen sie erhobenen Forderung gegenüber dem geltend machenden Unternehmen widersprechen. Eine Datenübermittlung an ein Inkassounternehmen darf nach einem solchen Widerspruch nämlich erst dann erfolgen, wenn die Rechtmäßigkeit der Forderung nach dieser Einwendung nochmals genau überprüft und bejaht wurde.

234 Siehe auch JB 2020, 10.1.

235 Siehe Verwaltungsgericht (VG) Berlin, Urteil vom 9. Oktober 2025, 1 K 463/22, Rn. 18 ff.; EDSA, Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.0, Rn. 107, abrufbar unter https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202201_data_subject_rights_access_v2_de.pdf.

Bürger:innen sind sich ihrer von der Datenschutz-Grundverordnung (DSGVO) gewährten Betroffenenrechte mehr und mehr bewusst und üben diese auch in vielfältiger Weise aus. Verantwortliche sollten es den Bürger:innen durch technische und organisatorische Maßnahmen so leicht wie möglich machen, ihre Rechte auszuüben.

XV. Informations- und Beschwerdestelle

In unserer Informations- und Beschwerdestelle erfolgt die erste Bearbeitung der eingehenden Anfragen und Beschwerden von Bürger:innen. Viele Prozesse erfolgen dort nach standardisierten Verfahren, um den Bürger:innen möglichst zeitnah Antworten auf Fragen bzw. Rückmeldung zur weiteren Bearbeitung ihrer Eingaben geben zu können. Gerade in Zeiten stetig steigender Beschwerdezahlen, die aktuell sogar einen Höchststand erreicht haben, bewähren sich die Prozesse der vorgelagerten Erstbearbeitung.

Die Informations- und Beschwerdestelle sichtet sämtliche Eingaben und Beschwerden von Bürger:innen und nimmt eine erste Bearbeitung vor. Häufig können die Anliegen bereits beantwortet werden, ohne dass hierzu die Fachabteilungen einbezogen werden müssen. Dies hat den Vorteil, dass Bürger:innen zügig Antworten bzw. Hinweise auf Informationsmaterialien erhalten. Wenn Bürger:innen z. B. Auskünfte von Verantwortlichen zur Datenverarbeitung wünschen, klärt die Informations- und Beschwerdestelle sie über die Rechtslage bei der Geltendmachung von Betroffenenrechten auf und gibt Hinweise, wie dabei vorgegangen werden sollte. Zeigt sich bspw. aufgrund einer Beschwerde, dass ein möglicher Datenschutzverstoß im Raum steht, wird dort geprüft, ob die mit der Beschwerde übermittelten Informationen und Nachweise ausreichend sind, um ein verwaltungsrechtliches Verfahren einleiten zu können. Gegebenenfalls werden fehlende Unterlagen angefordert. Grundsätzlich erfolgt erst bei Vorliegen sämtlicher für die weitere Bearbeitung notwendiger Informationen die Weiterleitung an die zuständige Fachabteilung, die sich dann inhaltlich mit dem Fall befasst. In einem stetigen engen Austausch mit den Fachabteilungen erarbeitet die Informations- und Beschwerdestelle Muster, klärt wiederkehrende Fragen und bereitet diese auf, um die Anliegen von Bürger:innen möglichst zügig beantworten zu können. Auch die an unsere Behörde gerichteten Anträge zur Geltendmachung von Betroffenenrechten, wie bspw. das Recht auf Auskunft nach Art. 15 Datenschutz-Grundverordnung (DSGVO) oder das Recht auf Löschung nach Art. 17 DSGVO, werden hier in einem standardisierten Verfahren bearbeitet.

In diesem Jahr haben wir einen Höchststand an Eingaben verzeichnet. Noch nie zuvor haben sich so viele Menschen mit Anfragen und Beschwerden an uns gewandt.[236] Insgesamt haben uns 9.224 Eingaben von Bürger:innen in Form von Beschwerden und Beratungsanfragen erreicht.[237] Im Vergleich zum Vorjahr bedeutet dies eine Steigerung von rund 50 Prozent. Darunter fallen 2.856 förmliche Beschwerden und 6.368 Anfragen betroffener Personen nach einer Beratung, bspw. in Bezug darauf, wie eigene Rechte gegenüber verantwortlichen Stellen geltend gemacht werden können. Mehr Eingaben erhielten wir insbesondere im Banken- und Finanzbereich, zu Inkassounternehmen und wegen der zwangsweisen Nutzung von mobilen Apps. Auch die Videoüberwachung und die Folgen von Identitätsdiebstählen waren häufiger Gegenstand von Beschwerden.

Zu der signifikanten Steigerung tragen viele Gründe bei. Ein erheblicher Grund liegt in der Nutzung von KI-Anwendungen. Über solche wird auf die Frage, wer in Datenschutzfragen helfen kann, einerseits offensichtlich das Angebot unserer Behörde sichtbarer; und andererseits werden immer mehr Eingaben dann mittels KI-Chatbots wie ChatGPT sogar erstellt. Generell sollten die aus KI-Anwendungen gewonnenen Erkenntnisse stets auf ihre Richtigkeit überprüft und abgegebene Prognosen kritisch hinterfragt werden. Auch muss den Bürger:innen klar sein, dass sie sensible personenbezogene Daten über sich selbst weitergeben, wenn sie eine KI-Anwendung für ihr Anliegen nutzen. Häufig weckt die von einer KI-Anwendung getroffene Vorhersage über den Ausgang der eigenen Beschwerde zudem falsche Erwartungen bei den Bürger:innen. Aussagen und vor allem die Einschätzung der Rechtslage erfolgen oft unvollständig oder sind schlicht falsch. Teilweise wurden wir sogar mit von der KI-Anwendung frei erfundenen Gerichtsurteilen oder nicht existenter juristischer Literatur konfrontiert.

236 Siehe unsere Pressemitteilung vom 5. Januar 2026, abrufbar unter https://www.datenschutz-berlin.de/pressemitteilung/zahl-der-datenschutzeingaben-um-50-prozent-gestiegen/.

237 Siehe E.I.1.

Die bewährten Prozesse in der Informations- und Beschwerdestelle werden fortlaufend gepflegt und optimiert, um auch zukünftig trotz des signifikant erhöhten Eingabeaufkommens eine möglichst zügige Erstbearbeitung der Eingaben und Beratungsanfragen für die Bürger:innen zu ermöglichen. Das hohe Aufkommen stellt unsere Behörde jedoch vor erhebliche Herausforderungen. Längere Bearbeitungszeiten lassen sich daher kaum vermeiden. Wir arbeiten stets an der Optimierung von Prozessen. Dabei nehmen wir auch für unsere Behörde die sich durch KI-Anwendungen bietenden Möglichkeiten in den Blick. Grundvoraussetzung dafür ist natürlich, dass diese datenschutzkonform nutzbar sind.[238]

238 Siehe zum Einsatz von KI in der Verwaltung B.IV.1.

XVI. Medien- und Datenschutzkompetenz

1. Medienpädagogische Arbeit mit Kindern und Jugendlichen

Wir haben unsere medienpädagogische Arbeit in diesem Jahr deutlich ausgeweitet. Besonders an Grundschulen zeigt sich ein stark wachsender Bedarf an Präventionsangeboten, weil Smartphones und soziale Medien immer früher Teil des Alltags von Kindern werden. Mit erweiterten Workshops, neuen Formaten und weiterentwickelten Onlineangeboten stärken wir Kinder und Jugendliche darin, ihre Rechte im Zusammenhang mit der Verarbeitung von persönlichen Daten besser zu schützen.

In vielen Grundschulen ist zu beobachten, dass Kinder bereits in den unteren Klassenstufen ein eigenes Smartphone nutzen und damit früh Datenschutzrisiken ausgesetzt sind. Unsere Präventionsworkshops setzen genau an dieser Stelle an und unterstützen die Schulen dabei, einen reflektierten Umgang mit persönlichen Daten zu lernen.

Besonders deutlich wird dies an der Entwicklung unseres Angebots: Die Anzahl der durchgeführten Workshops für Grundschulklassen der Jahrgangsstufen 4 bis 6 ist von 39 Veranstaltungen im vergangenen Jahr auf 83 in diesem Jahr gestiegen. Damit haben wir mehr als doppelt so viele Klassen wie im Vorjahr erreicht und unser Angebot in allen Bezirken verankert, wobei die stärkste Nachfrage von Klassen der 5. Jahrgangsstufe kam. Ergänzend wurde ein Projekttag zum Thema Datenschutz für alle 2. Klassen einer Grundschule in Charlottenburg durchgeführt, nachdem unangemessene Fotos in einem Klassenchat geteilt worden waren. Im Mittelpunkt standen Privatsphäre, das Recht am eigenen Bild und die Frage, welche Informationen in Chats geschützt werden müssen.

Für Jugendliche der 9. Klassenstufe wurde mit dem Workshop „Likes, Fame – und deine Daten?“ ein neues Format entwickelt, das am Beispiel einer beliebten Social-Media-Plattform Datenerfassung, Online-Sichtbarkeit und ihre Folgen thematisiert und seit diesem Jahr von Schulen regulär bei uns gebucht werden kann. Darüber hinaus

diskutierten mehrere Schulklassen im Rahmen einer Filmvorführung in einem Kino gemeinsam mit uns, welche Konsequenzen umfassende digitale Überwachung für den Alltag junger Menschen haben kann. Parallel dazu wurde die Website data-kids.de in Bezug auf die Barrierefreiheit umfassend überarbeitet, damit noch mehr Kinder, Eltern und pädagogische Fachkräfte die Inhalte nutzen können. Wir setzten auch unsere Mitarbeit an der länderübergreifenden Jugendplattform youngdata.de fort.

Die beschriebenen Angebote zeigen, dass Medienbildung und Datenschutz nur gemeinsam gedacht werden können und dass Prävention dann besonders wirksam ist, wenn Schulen, Kitas und außerschulische Einrichtungen eng mit uns zusammenarbeiten. Für Kinder und Jugendliche bedeutet dies, dass sie frühzeitig erfahren, welche Folgen ein unbedachter Umgang mit Fotos, Videos und Profildaten haben kann und welche Handlungsmöglichkeiten ihnen zur Verfügung stehen. Lehr- und Fachkräfte gewinnen zugleich Sicherheit im Umgang mit datenschutzrelevanten Fragen im pädagogischen Alltag und erhalten erprobte Materialien, um das Thema strukturiert in Unterricht und Projekte integrieren zu können.

Einen wichtigen Beitrag dazu leistete auch der zweite medienpädagogische Fachtag „Datenschutz trifft Medienkompetenz“, den wir gemeinsam mit jugendnetz.berlin veranstalteten. Rund 100 Fachkräfte der Kinder- und Jugendarbeit nutzten Fachvorträge und Workshops, um zu diskutieren, wie zeitgemäße Medienarbeit unter Berücksichtigung des Datenschutzes gestaltet werden kann und welche Rahmenbedingungen es dafür braucht. Auch auf der Bildungsmesse didacta 2025 waren wir gemeinsam mit weiteren Aufsichtsbehörden mit einem Stand vertreten und konnten zahlreiche Lehrkräfte und Erzieher:innen zu unseren Bildungsangeboten beraten, insbesondere zu data-kids.de, youngdata.de und unterstützenden Angeboten für den Kitabereich.

Beim Fachtag „Kita digital stärken“ in Neukölln wurde der digitale „Berliner Datenschutzwegweiser für Kitas“ gemeinsam mit Kita-Trägern und Fachkräften praktisch erprobt und als Hilfsmittel für einen sicheren und datenschutzbewussten Umgang mit Informationen im Kitaalltag beworben. Die Rückmeldungen zeigen, dass praxisnahe und niedrigschwellige Materialien entscheidend sind, damit Datenschutz im pädagogischen Alltag nicht als zusätzliche Belastung wahrgenommen wird, sondern als Bestandteil guter Bildungsarbeit. Für die kommenden Jahre planen wir, diese Formate weiterzuentwickeln und zusätzliche Zielgruppen einzubeziehen.

Die Entwicklungen machen deutlich, dass der Bedarf an Prävention im Bereich Medien- und Datenschutzkompetenz weiter steigt, insbesondere dort, wo Kinder bereits im Grundschulalter mit digitalen Geräten und Plattformen in Kontakt kommen. Unser Ansatz, unterschiedliche Altersgruppen mit passgenauen Angeboten anzusprechen und gleichzeitig Fachkräfte systematisch einzubinden, hat sich bewährt. Die deutliche Ausweitung der Grundschul-Workshops, die Einführung eines neuen Angebots für 9. Klassen, Sonderformate wie Filmgespräche sowie die Weiterentwicklung unserer Onlineangebote und Fachtage zeigen, dass eine enge Verbindung von Datenschutz und Medienbildung möglich und fruchtbar ist. Für uns bleibt entscheidend, dass Kinder und Jugendliche nicht nur über Risiken informiert werden, sondern selbstbewusst lernen, ihre Rechte auf Privatsphäre und informationelle Selbstbestimmung wahrzunehmen. Die in diesem Jahr gesammelten Erfahrungen fließen in die Weiterentwicklung unserer Angebote ein und bilden die Grundlage dafür, Medien- und Datenschutzkompetenz in Berlin auch künftig strukturell zu stärken.

2. Schulungsreihe Starthilfe Datenschutz

Die Schulungsreihe Starthilfe Datenschutz entwickelte ihr Angebot für Berliner Existenzgründer:innen und Kleinstunternehmen in diesem Jahr stetig weiter. Insbesondere haben wir die Zielgruppe auf Vereine erweitert und zusätzliche Schulungsangebote zu aktuellen Fragestellungen konzipiert. Erstmalig konnten wir neben Online- und Präsenzschulungen in unserer Dienststelle auch externe Veranstaltungen bei Dachverbänden in unser Programm aufnehmen.

Unsere Schulungsreihe entwickelte sich aus der „Start-up-Sprechstunde“, die seit 2019 Berliner Start-ups bei der Umsetzung der Datenschutz-Grundverordnung (DSGVO) unterstützte. Seit 2023 nahmen neben den Existenzgründer:innen auch vermehrt Vertreter:innen von Vereinen und bereits bestehenden Klein- und Kleinstunternehmen an den Schulungen teil. Um diese Ausweitung der Zielgruppe auch im Namen des Schulungsangebots abzubilden, wurde ein neuer Titel gefunden: „Starthilfe Datenschutz“. Damit wird betont, dass wir mit den Schulungen vor allem einen Anschub geben (Hilfe zur Selbsthilfe). Ziel bleibt es, denjenigen Unternehmen und Vereinen praktische Tipps und Hilfestellungen zu geben, die sich keine u. U. teure

Datenschutzberatung leisten können oder wollen und die Umsetzung der DSGVO selbst in die Hand nehmen.

Die Schulungsreihe ist als Zyklus mit aufeinander aufbauenden Themen geplant. Vorteilhaft ist es, diese vom ersten bis zum letzten Schulungstermin chronologisch zu besuchen. Um auch Nachzügler:innen abzuholen, haben wir die Grundlagenschulung „Basisüberblick DSGVO“ in der Jahresmitte erneut angeboten. In diesem Jahr wurden mit den zusätzlichen Schwerpunktthemen „Effizienz mit Verantwortung: Einsatz von Künstlicher Intelligenz“ und „Technisch-organisatorische Maßnahmen I: Datenschutz managen“ insgesamt 15 Schulungstermine von April bis Dezember durchgeführt. Die Veranstaltungen fanden hauptsächlich als Präsenzschulungen in unserer Dienststelle statt, um den direkten Austausch unter den Teilnehmenden zu fördern. Rein informative Inhalte konnten als Onlineformat vermittelt werden. Im Schnitt haben sich je Termin 15 bis 20 Teilnehmende angemeldet. Im Mai fand zudem das erste externe Angebot der Starthilfe Datenschutz beim Landessportbund Berlin statt. Rund 40 Teilnehmende aus verschiedenen Sportvereinen konnten wir zu den Grundlagen der DSGVO und den Besonderheiten im Vereinswesen schulen.

Die kostenlose Schulungsreihe Starthilfe Datenschutz gibt praktische Tipps und Hilfestellungen zu relevanten Themen des Datenschutzes und wird im nächsten Jahr weitergeführt. Anmeldungen können über unsere Website erfolgen. Laut den zurückgegebenen Feedbackbögen würden sämtliche Teilnehmenden die Starthilfe Datenschutz weiterempfehlen.

C.

Wir in Deutschland

I. Operationalisierung der Leitlinien zur Anonymisierung und Pseudonymisierung

Anonymisierung und Pseudonymisierung stellen wichtige Maßnahmen für eine datenschutzkonforme und datensparsame Datenverarbeitung dar, insbesondere angesichts datenintensiver Technologien in Bereichen wie Künstliche Intelligenz (KI) oder medizinische Forschung, aber auch im Kontext der europäischen Digitalrechtsakte. Da die Anforderungen an Anonymisierungs- und Pseudonymisierungsverfahren stark vom Einzelfall abhängen, erarbeitet die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) seit Beginn dieses Jahres unter unserer Leitung hierzu praktische Hilfestellungen anhand konkreter Fallbeispiele. Das DSK-Papier wird auf den bereits vom Europäischen Datenschutzausschuss (EDSA) veröffentlichten Leitlinien zur Pseudonymisierung[239] sowie der finalen Fassung der derzeit in Arbeit befindlichen EDSA-Leitlinien zur Anonymisierung basieren und soll kurz nach deren Veröffentlichung erscheinen.

Der EDSA hatte der Technology Subgroup den Auftrag erteilt, Leitlinien zur Anonymisierung und Pseudonymisierung zu erarbeiten. Die Leitlinien zur Pseudonymisierung wurden vom EDSA-Plenum im Januar dieses Jahres verabschiedet, die öffentliche Konsultation ist bereits abgeschlossen. Die Annahme der Leitlinien zur Anonymisierung steht noch aus. Die Leitlinien werden wesentliche Grundlagen für die Beurteilung von Anonymisierungs- und Pseudonymisierungsverfahren sein.

Aufgrund des hohen Abstraktionsgrads der Leitlinien und der Bedeutung der jeweiligen Techniken für eine datenschutzkonforme und datensparsame Datenverarbeitung erarbeitet eine aufsichtsbehörden- und arbeitskreisübergreifende Projektgruppe unter

239 EDSA, Guidelines 01/2025 on Pseudonymisation, abrufbar unter https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_de.

unserer Leitung ein Papier mit Hilfestellungen zur Operationalisierung der Vorgaben der Leitlinien im Hinblick auf ihre Anwendung in konkreten Fällen.

Der derzeitige Entwurf umfasst neben einigen einfachen Beispielen Fallgruppen zur Anonymisierung von Standortdaten aus vernetzten Fahrzeugen, Skelett-Rigs[240] aus Videodaten, Daten aus dem Krebsregister, IP-Adressen und Kundendaten von Onlineshops. Außerdem werden konkrete Anforderungen an das Training eines anonymisierten KI-Modells für CT-Oberkörperaufnahmen sowie an deren Pseudonymisierung zu diesem Zweck dargestellt. In den beiden letzten Kapiteln des Entwurfs werden schließlich Verallgemeinerungen aus den beschriebenen Fallgestaltungen abgeleitet und ein Ausblick auf die Bedeutung von Anonymisierung und Pseudonymisierung bei der Umsetzung europäischer Digitalrechtsakte gegeben.

Die oben genannten Fallgruppen basieren im Wesentlichen auf Vorschlägen der thematisch zuständigen Arbeitskreise der DSK und wurden so ausgewählt und zusammengefasst, dass sie einerseits ein breites Spektrum relevanter Fallgestaltungen abdecken und die Fragestellungen andererseits hinreichend spezifisch sind. Die einzelnen Fallgestaltungen – einschließlich der getroffenen Annahmen – werden zunächst jeweils genau beschrieben und abgegrenzt und die Ziele der Pseudonymisierung oder Anonymisierung hervorgehoben. Anschließend werden grundlegende Eigenschaften der jeweiligen Fallgruppe beleuchtet, wie z. B. wer für die Verarbeitung verantwortlich ist oder welche Zusatzinformationen für die Bewertung der Verfahren relevant sind. Darauf aufbauend werden dann ein oder mehrere für den Anwendungsfall relevante Anonymisierungs- oder Pseudonymisierungsverfahren unter Einbeziehung wissenschaftlicher Ergebnisse diskutiert und bewertet. Bei der Bewertung wird gemäß den EDSA-Leitlinien vorgegangen und ein starker Bezug zu diesen hergestellt. Neben den originär datenschutzrechtlichen Fragen wird auch die Eignung der pseudonymisierten oder anonymisierten Daten für den beabsichtigten Zweck untersucht.

Im Kontext der Anonymisierung von Daten aus vernetzten Fahrzeugen spielen bspw. mit Zeitstempeln kombinierte Positionsdaten bei der Frage des Personenbezugs eine wichtige Rolle. Im Rahmen der entsprechenden Fallgestaltung wird die Anonymisierung solcher Daten für die an die Verkehrsdichte angepasste Navigation durch Dritte näher

240 Abstrahierte Strichfiguren, z. B. zur Erkennung von Gesten oder bestimmtem Verhalten.

betrachtet. Es wird dargelegt, wie die Kombination aus der Aggregation der Daten mehrerer Fahrzeuge und der Vergröberung der örtlichen und zeitlichen Auflösung zu anonymen Daten im Sinne der Leitlinien führen kann, ohne den beabsichtigten Zweck der Verarbeitung übermäßig zu beeinträchtigen.

Am Beispiel eines Onlineshops wird die Anonymisierung von Kundendaten zu eigenen Zwecken betrachtet. Da dem Verantwortlichen im Beispielsfall zahlreiche Zusatzinformationen vorliegen, die zur Re-Identifizierung der betroffenen Personen herangezogen werden können, ergeben sich entsprechend hohe Anforderungen an die technischen Verfahren. Es wird konkret dargestellt, wie man diese Anforderungen mithilfe von Differential Privacy[241] oder synthetischen Daten erfüllen könnte.

Die Beiträge zu den einzelnen Fallgestaltungen und zu den weiteren Kapiteln wurden in Kleingruppen mit Teilnehmenden aus den thematisch zuständigen Arbeitskreisen der DSK jeweils unter Federführung einer der beteiligten Aufsichtsbehörden erarbeitet. Für die kontextspezifischen, methodischen Fragestellungen gab es darüber hinaus einen intensiven Austausch mit Fachleuten aus der Wissenschaft. Um fallgruppenübergreifende Fragen zu klären und die einzelnen Beiträge zu vereinheitlichen, fanden in diesem Jahr insgesamt drei Vor-Ort-Treffen der gesamten Projektgruppe in Berlin statt. Neben der Konzeption und Führung des gesamten Projekts haben wir die Kleingruppe zu der oben beschriebenen Anonymisierung von Kundendaten von Onlineshops geleitet und uns auch in der Kleingruppe zur Anonymisierung von IP-Adressen eingebracht.

Die EDSA-Leitlinien zur Anonymisierung sind bisher noch nicht finalisiert und verabschiedet worden, nicht zuletzt infolge eines Urteils des Europäischen Gerichtshofs (EuGH) in diesem Jahr,[242] das weitreichende Ausführungen zum Personenbezug pseudonymisierter Daten enthält. Da Hilfestellungen zur Operationalisierung insbesondere auch diese Leitlinien betreffen, wurden sie von der Projektgruppe nicht, wie ursprünglich geplant, Ende dieses Jahres der DSK zur Verabschiedung vorgelegt. Stattdessen wird eine Verabschiedung und anschließende Veröffentlichung unmittelbar nach dem Erscheinen der Leitlinien zur Anonymisierung angestrebt.

241 Differential Privacy ist ein besonders sicheres Anonymisierungs-Framework mit mathematischen Garantien in Bezug auf den maximalen Grad der Re-Identifizierbarkeit einer Person.

242 EuGH, Urteil vom 4. September 2025, C-413/23 P.

Die Operationalisierung abstrakter Leitlinien anhand konkreter Fallgestaltungen ist ein wesentlicher Beitrag zur Rechtssicherheit und Praxistauglichkeit des Datenschutzes. Verantwortliche bekommen eine klare Orientierung, um datenintensive Technologien datenschutzkonform zu gestalten, ohne deren Funktionsfähigkeit unverhältnismäßig einzuschränken. Die aufsichtsbehördenübergreifende Erarbeitung solcher Hilfestellungen gewährleistet zudem eine einheitliche Rechtsauslegung in Deutschland und stärkt damit die Vorhersehbarkeit datenschutzrechtlicher Anforderungen in der Praxis. Dies ist gerade bei komplexen Verfahren wie der Anonymisierung und der Pseudonymisierung von Daten von zentraler Bedeutung, da hier die Grenze zwischen personenbezogenen und anonymen Daten im Einzelfall schwierig zu bestimmen sein kann.

II. Rechtsdurchsetzung

1. Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich auf Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden (MRiDaVG)[243] geeinigt. Die Musterrichtlinien geben leitende Vorgaben zum Verfahrensablauf, zur Ermessensausübung und zur Anwendung sowie Auslegung von deutschen Rechtsnormen im Rahmen von Verfahren über Geldbußen nach der Datenschutz-Grundverordnung (DSGVO).

Unter der Leitung unserer Behörde hat eine Arbeitsgruppe mit Beteiligung weiterer Aufsichtsbehörden die Musterrichtlinien erarbeitet. Nach dem Vorbild ergänzender Verwaltungsvorschriften anderer Behörden, wie etwa die Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV), haben wir Arbeitshinweise für typische Verfahrensschritte und -situationen in Verfahren über Geldbußen nach der DSGVO geschaffen. Die Musterrichtlinien ermöglichen in diesen Verfahren eine weitgehend bundeseinheitliche Behandlung grundlegender Fragen der Verfahrensführung.

Bei der Durchführung von Verfahren über Geldbußen nach der DSGVO sind auch nationale Verfahrensregelungen zu berücksichtigen. Die Musterrichtlinien unterstützen bei Anwendung und Auslegung der verfahrensrechtlichen Vorgaben, indem sie auslegungsbedürftige Rechtsbegriffe konkretisieren und ermessenslenkende Vorgaben geben. Das betrifft etwa Fragen zur Zuständigkeit, der Einleitung von Verfahren oder der Ermessensausübung sowie die Gestaltung von Bescheiden.

Im Einklang mit der Rechtsprechung des Europäischen Gerichtshofs (EuGH)[244] stellen die MRiDaVG klar, dass datenschutzrechtliche Verfahren über Geldbußen

243 DSK, Festlegung vom 16. Juni 2025, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2025/20250617-DSK-Festlegung_MRiDaVG.pdf.

244 EuGH, Urteil vom 5. Dezember 2023, C-807/21; siehe zuletzt auch JB 2024, A.II.3.

unmittelbar gegen die Verantwortlichen, Auftragsverarbeiter, Zertifizierungs- und Überwachungsstellen zu führen und entsprechende Bescheide an diese zu adressieren sind. Dies gilt unabhängig davon, in welcher Rechtsform diese organisiert sind und ob der Verstoß durch ihre Organe, Vertreter:innen, Leitungspersonen oder jede andere Person begangen wurde, die im Rahmen der unternehmerischen Tätigkeit und im Namen dieser Stelle gehandelt hat. Auch im Rahmen der Verwendung von Datenschutzvorfällen nach Art. 33 DSGVO oder einer Benachrichtigung nach Art. 34 DSGVO berücksichtigen die Musterrichtlinien EuGH-Rechtsprechung[245], wonach die Selbstbelastungsfreiheit für Unternehmen nicht uneingeschränkt gilt. Dementsprechend sieht die MRiDaVG vor, § 43 Abs. 4 Bundesdatenschutzgesetz (BDSG) unionsrechtskonform dahingehend auszulegen, dass ein Verwendungsverbot nur besteht, soweit die meldende Stelle durch die gemeldete Verletzung das Verschulden eines Datenschutzverstoßes zugesteht.

Die Musterrichtlinien sind in unserem Haus als Verwaltungsvorschrift erlassen worden und die Regelungen damit für alle bei uns geführten Verfahren über Geldbußen bindend.

Die Aufsichtsbehörden des Bundes und der Länder haben sich in enger und konstruktiver Zusammenarbeit auf ein einheitliches und transparentes Vorgehen bei Verfahren über Geldbußen nach der DSGVO geeinigt. Die MRiDaVG tragen als praktische Arbeitshilfe maßgeblich dazu bei, dass aufsichtsrechtliche Verfahren der deutschen Aufsichtsbehörden im nicht-öffentlichen Bereich weiter harmonisiert werden.

2. Merkblatt zu Verständigungen in datenschutzrechtlichen Verfahren über Geldbußen

Die DSK hat ein Merkblatt zu Verständigungen in datenschutzrechtlichen Verfahren über Geldbußen veröffentlicht.[246] Das Merkblatt skizziert die Voraussetzungen, den Ablauf und die Folgen einer einvernehmlichen Verfahrensbeendigung in Verfahren über Geldbußen nach der DSGVO.

245 EuGH, Urteil vom 18. Oktober 1989, Rs. 374/87, Orkem/Kommission.

246 Stand: Dezember 2025, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2025/2025-DSK-Merkblatt-Verstaendigung.pdf.

Unter der Leitung unserer Behörde hat eine Arbeitsgruppe mit Beteiligung weiterer Aufsichtsbehörden ein Merkblatt zu Verständigungen in datenschutzrechtlichen Verfahren über Geldbußen erarbeitet. Eine Verständigung (auch „Settlement“ genannt) ermöglicht, ein u. U. komplexes und ermittlungsintensives Verfahren abzukürzen und bspw. eine zu zahlende Geldbuße zu reduzieren. Dies kann sowohl für Betroffene als auch für die Aufsichtsbehörde eine effiziente und ressourcenschonende Lösung bieten. Das Instrument der Verständigung wird aus diesen verfahrensökonomischen Gründen auch von anderen Aufsichtsbehörden, wie der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) oder dem Bundeskartellamt (BKartA) regelmäßig angewendet. Mit dem Merkblatt machen nun auch die Datenschutzaufsichtsbehörden auf die grundsätzliche Möglichkeit einer Verständigung aufmerksam.

Eine Verständigung im Verfahren über Geldbußen nach der DSGVO kann sowohl durch Betroffene als auch von der Aufsichtsbehörde angeregt werden. Ein Anspruch auf die Beendigung eines Verfahrens mit einer Verständigung besteht jedoch nicht. Voraussetzung für eine Verständigung und eine damit ggf. verbundene Herabsetzung der Geldbuße ist die geständige Einlassung durch die oder den Betroffene:n. Der Schwerpunkt im Verständigungsgespräch zwischen den Beteiligten liegt somit auf der Rechtsfolgenseite. Das Verfahren endet auch bei der Verständigung mit einem entsprechenden Bescheid über Geldbußen, gegen den Einspruch eingelegt werden kann. Unsere Behörde hat bereits positive Erfahrungen mit der einvernehmlichen Beendigung von Verfahren mittels Verständigungen gemacht.

In Verfahren über Geldbußen nach der DSGVO ist grundsätzlich eine einvernehmliche Verfahrensbeendigung möglich. Mit der Veröffentlichung des Merkblatts zu Verständigungen in datenschutzrechtlichen Verfahren über Geldbußen können Ablauf und Voraussetzungen nunmehr öffentlich nachvollzogen werden.

III. Künstliche Intelligenz

1. Neuer DSK-Arbeitskreis zur Künstlichen Intelligenz

Die rasant fortschreitende Entwicklung verschiedenster Ausprägungen von Systemen der Künstlichen Intelligenz (KI) stellt auch die Aufsichtsbehörden vor komplexe Herausforderungen. Um die Entwicklung und den Einsatz dieser Technologien datenschutzrechtlich fundiert zu begleiten, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) einen neuen Arbeitskreis ins Leben gerufen.

Im Januar dieses Jahres fand die konstituierende Sitzung des Arbeitskreises Künstliche Intelligenz (AK KI) unter dem Vorsitz von Baden-Württemberg und Rheinland-Pfalz statt. Neben den in der DSK organisierten Aufsichtsbehörden nahmen auch Vertreter:innen der spezifischen Datenschutzinstitutionen der Kirchen und des Rundfunks teil. Der AK KI vereinigt technische und rechtliche Expertise und unterstützt die DSK darin, die Entwicklung und den Einsatz von Modellen und Systemen Künstlicher Intelligenz datenschutzrechtlich zu begleiten. Dabei wird ein konstruktiver und zielorientierter Ansatz verfolgt.

Im Mittelpunkt der Arbeit des AK KI steht der Grundrechtsschutz. Zur Betonung der grundrechtsschützenden Elemente wird ein menschenzentrierter Ansatz im Hinblick auf die Gestaltung vertrauenswürdiger KI verfolgt. Diese Elemente sollen möglichst auf ihre Vereinbarkeit mit den Interessen an der Entwicklung und dem Einsatz von KI geprüft und risikospezifisch fortentwickelt werden.

Da es sich bei KI um ein Querschnittsthema handelt, erfüllt der AK KI auch eine Koordinierungsfunktion. Er ist im Auftrag der DSK Ansprech- und Schnittstelle für die datenschutzrechtlichen Gremien auf deutscher und europäischer Ebene. Deshalb verständigte man sich auch frühzeitig über die Form von Kooperationen sowohl interner – mit anderen Arbeitskreisen der DSK – als auch externer Natur – etwa mit der französischen Datenschutzaufsicht (CNIL) und der britischen Datenschutzaufsicht (ICO).

Anhand eines Arbeitsplans einigte man sich bereits in der konstituierenden Sitzung auf die Erstellung zweier Papiere. Das eine soll sich an Verantwortliche richten. Darin sollen Anforderung bzgl. der Transparenz beim Einsatz von KI herausgearbeitet und erläutert werden. Das andere soll die Ende des vergangenen Jahres veröffentlichte Opinion des Europäischen Datenschutzausschusses (EDSA) bzgl. Datenschutz und KI-Modellen[247] operationalisieren. Dafür werden konkrete risikomindernde Maßnahmen für die in der Opinion skizzierten Szenarien identifiziert und beschrieben. Wir sind an beiden Arbeitsgruppen, die diese Papiere jeweils erstellen, beteiligt.

Darüber hinaus wurden zwei Unterarbeitskreise (UAK) des AK KI eingerichtet. Der UAK „Regulatorische Entwicklung in der EU und international“ wird Aktivitäten hinsichtlich der Regulierung von KI beobachten und relevante Entwicklungen zur Diskussion in den AK KI einbringen. Der UAK „Forschung und Entwicklung“ wird den Stand der Wissenschaft in ausgewählten Themenfeldern der KI-Forschung verfolgen, sich einen gemeinsamen Wissensstand erarbeiten und diese Expertise für alle Aktivitäten des AK KI vorhalten. Wir beteiligen uns an der Arbeit des letztgenannten UAK.

Die Institutionalisierung der Datenschutzaufsicht über KI-Systeme innerhalb der DSK durch die Einrichtung des AK KI markiert einen wichtigen Schritt hin zu einer einheitlichen Beratungs- und Prüfpraxis in Deutschland. Durch die Bündelung der Ressourcen begegnen die Aufsichtsbehörden der technologischen Komplexität mit hoher Fachkompetenz. Dabei verfolgen sie einen konstruktiven Ansatz. Damit wird gewährleistet, dass Grundrechtsschutz und Innovation bei der Entwicklung und dem Einsatz von KI Hand in Hand gehen.

247 Abrufbar unter https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_de.pdf.

2. Orientierungshilfe für technische und organisatorische Maßnahmen bei KI-Systemen

Die datenschutzkonforme Entwicklung von KI-Systemen stellt Verantwortliche vor große Herausforderungen. Die Aufsichtsbehörden möchten hierbei praktische Unterstützung leisten und haben ihre Arbeiten an einer gemeinsamen Publikation zu diesem Thema finalisiert. Das Ergebnis ist eine umfassende Orientierungshilfe, die konkrete Maßnahmen für den gesamten Lebenszyklus von KI-Modellen definiert.

Wie bereits im vergangenen Jahr berichtet,[248] haben wir zusammen mit anderen Aufsichtsbehörden an einer Publikation gearbeitet, die Hersteller:innen und Betreiber:innen von KI-Modellen und -Systemen einen Katalog von empfohlenen technischen und organisatorischen Maßnahmen an die Hand gibt. Die Maßnahmen betreffen die datenschutzfreundliche Entwicklung von KI-Modellen sowie den mit der Datenschutz-Grundverordnung (DSGVO) konformen Betrieb von KI-Systemen, die diese Modelle integrieren. Diese Publikation ist im Juni dieses Jahres als „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen“ von der DSK veröffentlicht worden.[249]

Der in der Orientierungshilfe abgebildete Maßnahmenkatalog orientiert sich an den Gewährleistungszielen des sog. Standard-Datenschutzmodells (SDM). Er verfolgt das Ziel, für jede Phase des Lebenszyklus eines KI-Systems geeignete technische und organisatorische Maßnahmen zu identifizieren, die die mit der jeweiligen Verarbeitung personenbezogener Daten verbundenen Risiken ausreichend mindern. Dies ermöglicht den Hersteller:innen und Betreiber:innen von KI-Systemen und -Modellen, durch den Einsatz spezifischer Maßnahmen die datenschutzrechtlichen Anforderungen zu erfüllen und so die Rechte und Freiheiten von natürlichen Personen bei der Entwicklung und dem Betrieb von KI-Systemen zu schützen. Verantwortliche können dadurch bei der Entwicklung und dem Betrieb von KI-Systemen den Anforderungen zum Datenschutz durch Technikgestaltung[250] von Anfang an nachkommen.

248 Siehe JB 2024, B.II.6.
249 Abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/DSK-OH_KI-Systeme.pdf.
250 Siehe Art. 25 DSGVO.

Die unter unserer Mitwirkung erstellte und veröffentlichte Orientierungshilfe schließt eine wichtige Lücke zwischen abstrakten rechtlichen Vorgaben und der technischen Praxis. Sie bietet Entwickler:innen, Hersteller:innen und Betreiber:innen von KI-Modellen und -Systemen einen Katalog von Maßnahmen, um datenschutzrechtliche Anforderungen in jeder Lebenszyklusphase adressieren zu können. Dabei verdeutlicht sie, dass Datenschutz durch Technikgestaltung (Privacy by Design) auch bei komplexen KI-Anwendungen umsetzbar ist und so Rechtssicherheit für Innovationen gewährleistet werden kann.

3. Orientierungshilfe für Systeme mit Retrieval-Augmented Generation

Die Verknüpfung von Sprachmodellen mit externem Wissen durch Retrieval-Augmented Generation (RAG) verspricht präzisere Antworten. Doch diese Technik birgt spezifische Risiken für den Datenschutz. Eine neue Orientierungshilfe der DSK zeigt Behörden und Unternehmen praxisnahe Wege für den rechtskonformen Einsatz auf.

Im Oktober dieses Jahres hat die DSK eine Orientierungshilfe für Behörden und Unternehmen veröffentlicht, die KI-Systeme mit sog. Retrieval-Augmented Generation (RAG) einsetzen möchten oder dies bereits tun.[251] Die Orientierungshilfe, an der wir mitgewirkt haben, enthält sowohl rechtliche als auch technische Hinweise, um die Potenziale solcher Systeme zu nutzen und gleichzeitig die Risiken für Betroffene zu verringern.

RAG ist eine KI-Technologie, die Sprachmodelle durch externe Wissensquellen erweitert. In einem solchen System ist ein Large Language Model (LLM) nur eine Komponente, die mit einem RAG-Subsystem ergänzt wird. Durch Anbindung interner Datenbanken oder behördenspezifischer Dokumente wird das Sprachmodell so in die Lage versetzt, Antworten zu generieren, die sich nur auf den spezifischen Kontext dieses Wissens beziehen.

251 Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_RAG.pdf.

Ein Vergleich der semantischen Nähe von Anfragen mit den Informationen in diesen Wissensquellen sowie die Anweisung, nur diese Quellen zur Antwortgenerierung zu nutzen, sorgt dafür, dass die von großen Sprachmodellen bekannten Halluzinationen und unrichtigen Ausgaben reduziert werden. Damit erhöht sich die Genauigkeit und Verlässlichkeit dieser Systeme im Vergleich zu reinen LLMs. Darüber hinaus lassen sich zumindest für die zusätzlich angebundenen Wissensquellen und externen Dokumente Betroffenenrechte wie Auskunft, Berichtigung oder Löschung gewährleisten.

Da die LLM-Komponenten in RAG-Systemen vorrangig zur Textgenerierung genutzt werden, spielt das in den Modellen selbst vorhandene Wissen eine untergeordnete Rolle. Daher können in diesen Systemen u. U. kleinere Modelle genutzt werden, die aufgrund der verringerten Komplexität eher für den lokalen Einsatz oder einen On-Premise-Betrieb (vor Ort im eigenen Unternehmen) geeignet sind. Damit kann die Übermittlung sensibler Daten an externe KI-Anbieter oder die Nutzung von Cloud-Ressourcen vermieden werden. Wird ein RAG-System lokal oder on-premise entwickelt und betrieben, kann damit nicht nur der Ansatz des Datenschutzes durch Technikgestaltung verfolgt werden. Ein solches Vorgehen kann darüber hinaus auch maßgeblich zur digitalen Souveränität beitragen.

RAG-Systeme bringen aber auch Herausforderungen mit sich. So wird das datenschutzrechtlich problematische rechtswidrige Training von am Markt befindlichen Modellen nicht beseitigt. Auch die Umsetzung von Anforderungen, wie Transparenz und Zweckbindung, oder die Gewährleistung von Betroffenenrechten innerhalb der LLM-Komponenten stellen bisher ungelöste Probleme dar. Daher müssen verantwortliche Stellen, die RAG-Systeme einsetzen oder betreiben wollen, dafür Sorge tragen, die datenschutzrechtlichen Bewertungen einzelner Verarbeitungen personenbezogener Daten fallspezifisch vorzunehmen und technisch-organisatorische Maßnahmen immer auf dem aktuellsten Stand zu halten.

Der Einsatz von RAG-Systemen verdeutlicht das Spannungsfeld zwischen technologischer Innovation und Datenschutz. Diese Technik kann die Richtigkeit von KI-Antworten verbessern; gleichzeitig müssen Verantwortliche die zugrunde liegenden Modelle kritisch prüfen. Die Orientierungshilfe setzt hier einen wichtigen Standard: Sie fordert eine ganzheitliche Betrachtung des Gesamtsystems und stärkt damit die Position der Betroffenen gegenüber komplexen KI-Architekturen.

IV. Verwaltungsdigitalisierung

1. Das „Einer für Alle“-Prinzip zur Digitalisierung von Verwaltungsleistungen nach dem Onlinezugangsgesetz

Die Verwaltungsdigitalisierung in Bund und Ländern erfolgt nach dem „Einer für Alle“-Prinzip (EfA-Prinzip).[252] In der Praxis werden dazu auf Grundlage des Onlinezugangsgesetzes (OZG) vor allem länderübergreifende Onlinedienste zentral durch ein Bundesland entwickelt und betrieben.[253] Wir haben in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die Entwicklung eines standardisierten Prüfprozesses für die Entwicklung dieser länderübergreifenden Onlinedienste initiiert, der die effektive OZG-Umsetzung fördert.

Mit der Novellierung des OZG im Jahr 2024 hat der Bundesgesetzgeber „länderübergreifende Onlinedienste“ als zentrales Nachnutzungsmodell im Gesetz verankert.[254] Diese werden nach dem EfA-Prinzip[255] zentral durch ein Bundesland entwickelt und betrieben und durch die anderen Bundesländer nachgenutzt. Dabei fehlte es bisher an einheitlichen und praxisorientierten Vorgaben zur Umsetzung des Datenschutzes.

Vor diesem Hintergrund haben wir in der von der DSK eingesetzten Kontaktgruppe OZG 2.0, deren Vorsitz wir innehaben, einen standardisierten Prozess zur Prüfung und Dokumentation der datenschutzrechtlichen Anforderungen im Rahmen der Entwicklung von länderübergreifenden Onlinediensten erarbeitet. Vorbild hierfür ist der von uns im letzten Jahr veröffentlichte Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben.[256] Die DSK hat den erarbeiteten Prüfprozess nun beschlossen[257]

252 Das EfA-Prinzip bedeutet, dass eines oder mehrere Länder eine länderübergreifend einsetzbare Lösung entwickeln, die durch eine zentrale Stelle fachlich und technisch betrieben wird, siehe https://www.digitale-verwaltung.de/SharedDocs/faqs/Webs/DV/DE/faq_nachnutzung/faq016.html; siehe auch JB 2021, 2.3.

253 Siehe JB 2024, B.II.3.

254 Siehe § 2 Abs. 8 und § 8a OZG; JB 2024, B.II.3.

255 Siehe dazu auch https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/efa/efa-node.html.

256 Siehe JB 2024, A.VI.2.

257 Abrufbar unter https://www.datenschutzkonferenz-online.de/beschluesse-dsk.html.

und empfiehlt diesen den nach § 8a OZG Verantwortlichen in Bund und Ländern als Standard im Hinblick auf die Datenschutzprüfung. Ziel der Entwicklung dieses Prozesses war, die datenschutzrechtlichen Anforderungen in konkrete Prüf- und Dokumentationsschritte zu übersetzen, die den Verantwortlichen nicht nur vorgeben, was umzusetzen ist, sondern auch zeigen, wie diese Vorgaben zu verwirklichen sind. Die Prüf- und Dokumentationsschritte sind dabei entsprechend den standardisierten Phasen des Projektmanagements[258] angeordnet, die auch für IT-Projekte der öffentlichen Verwaltung in Bund und Ländern etabliert sind.[259] Der standardisierte Prüfprozess bietet zudem auch eine Orientierung, wann die Datenschutzvorgaben im Verlauf der Projekte in den Blick zu nehmen und umzusetzen sind. Diesen methodischen Ansatz haben wir bereits bei dem für Berlin entwickelten Standardprozess Datenschutz bei öffentlichen Digitalisierungsvorhaben verfolgt.

Der standardisierte Prüfprozess berücksichtigt darüber hinaus auch die allgemeinen Standards der Verwaltungsdigitalisierung wie den Servicestandard für die digitale Verwaltung[260] und die DIN SPEC 66336[261]. Auch diese definieren Datenschutzanforderungen als Teil der allgemeinen Qualitätskriterien, geben jedoch keine Hinweise zur konkreten Umsetzung. Hier setzt der Prüfprozess an und zeigt jeweils in Form von einzelnen Prüf- und Dokumentationsschritten, wie auch die in den allgemeinen Standards enthaltenen Datenschutzvorgaben[262] erfüllt werden können.

Die DSK empfiehlt, den standardisierten Prüfprozess zur einheitlichen Umsetzung der datenschutzrechtlichen Anforderungen bei länderübergreifenden Onlinediensten für OZG-Verantwortliche zu nutzen. Gleichzeitig definieren die Aufsichtsbehörden mit dem Prüfprozess aber auch einheitliche Prüfungs- und Dokumentationsanforderungen für ihre Bewertung von länderübergreifenden Onlinediensten und machen diese transparent. Der Prüfprozess fördert damit eine effektive Umsetzung des OZG und leistet einen Beitrag, das EfA-Prinzip auch für die Datenschutzberatung und -prüfung der Aufsichtsbehörden nutzbar zu machen.

258 DIN 69901.
259 Siehe bspw. den Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung der Bundesregierung sowie die Projektmanagementhandbücher der einzelnen Bundesländer; siehe auch Anlage 8.2.1 des Prüfprozesses.
260 Siehe https://servicestandard.gov.de/.
261 Siehe https://servicestandard.gov.de/din-spec-66336/.
262 Siehe Servicestandard, Prinzip 5 und DIN SPEC 66336, Abschnitt 5.8.

Die DSK-Kontaktgruppe OZG 2.0 wird den standardisierten Prüfprozess auf der Grundlage der Erfahrungen in der Anwendungspraxis fortlaufend überarbeiten und weiterentwickeln. Bereits in dessen Entwicklungsphase stand die Kontaktgruppe dazu im Austausch mit der Föderalen IT-Kooperation (FITKO); sie wird diese Zusammenarbeit nun auch bei der Umsetzung in der Praxis fortführen.

Standardisierte Verwaltungsdigitalisierung nach dem EfA-Prinzip erfordert auch Standards für eine einheitliche Umsetzung des Datenschutzes. Der standardisierte Prüfprozess der DSK für länderübergreifende Onlinedienste bietet den OZG-Verantwortlichen eine klare Orientierung und definiert gleichzeitig einheitliche und transparente Prüfungs- und Dokumentationsanforderungen der Aufsichtsbehörden.

2. Orientierungshilfe zum Onlinezugangsgesetz

Der Gesetzgeber hat das OZG im letzten Jahr um spezielle Datenschutzregelungen ergänzt.[263] Mit ihnen soll eine noch effektivere Umsetzung des OZG aus Sicht des Datenschutzes ermöglicht werden. Um eine einheitliche Auslegung der neu in das OZG eingefügten Normen für die Praxis zu erreichen, hat die DSK unter unserer Mitwirkung Ende 2024 eine Orientierungshilfe zum OZG (OH OZG) veröffentlicht und diese nun noch einmal grundlegend aktualisiert.

Das OZG verankert das EfA-Prinzip als zentrales Nachnutzungsmodell.[264] Hierzu definiert es länderübergreifende Onlinedienste als IT-Komponenten zur Abwicklung elektronischer Verwaltungsleistungen von Bund oder Ländern, die insbesondere dem elektronischen Ausfüllen der diesbezüglichen Onlineformulare dienen.[265] Grundlegende Funktion dieser länderübergreifenden Onlinedienste ist, dass ein Bundesland die für eine oder mehrere Verwaltungsleistungen erforderlichen Antragsdaten zentral sammelt und dann an die für die Gewährung der Verwaltungsleistungen jeweils zuständigen Fachbehörden der anderen Bundesländer übermittelt.

263 Siehe JB 2023, B.I.2.; JB 2024, B.II.3.
264 Siehe JB 2024, B.II.3.
265 Siehe § 2 Abs. 8 OZG.

Um eine effektive Umsetzung des OZG zu gewährleisten, enthält das OZG nunmehr spezielle Datenschutzregelungen zu den länderübergreifenden Onlinediensten. Diese müssen einheitlich ausgelegt und angewendet werden. Dazu hat die DSK bereits im vergangenen Jahr die OH OZG veröffentlicht und diese nun auf der Grundlage der Erfahrungen aus der Aufsichts- und Beratungspraxis aktualisiert.[266]

Inhaltlich geht die OH OZG ausführlich auf den zentralen Begriff des „länderübergreifenden Onlinedienstes" ein, der regelmäßig Gegenstand von Auslegungsfragen in der Praxis ist. Darüber hinaus liegt der Fokus der OH OZG auf Erläuterungen zu den Rechtsgrundlagen der Datenverarbeitung in § 8a Abs. 1 und 2 OZG. Ebenso werden die Speicherfristen für den Fall der Zwischenspeicherung von personenbezogenen Daten in länderübergreifenden Onlinediensten[267] dargelegt. Ferner wird klargestellt: Aufgrund der Regelung des § 8a Abs. 4 OZG – wonach nur die den Onlinedienst betreibende Behörde als Verantwortlicher i. S. d. Datenschutzes einzuordnen ist – bedarf es bei der Bereitstellung von länderübergreifenden Onlinediensten nicht mehr des Abschlusses von Vereinbarungen zu einer gemeinsamen Verantwortlichkeit[268] oder von Auftragsverarbeitungsverträgen[269]. Die OH OZG stellt insoweit auch klar, dass solche Vereinbarungen zu länderübergreifenden Onlinediensten, soweit sie in der Praxis noch bestehen, nun angesichts der Regelung des § 8a Abs. 4 OZG aufgehoben werden müssen. Schließlich gibt die OH OZG Hinweise zur Funktion der Nutzerkonten („Bund-ID" bzw. „Deutschland-ID") im Zusammenhang mit den länderübergreifenden Onlinediensten.

Die OH OZG dient der Förderung einer einheitlichen Auslegung der speziellen Datenschutzregelungen des OZG für die in der Praxis mit der Umsetzung befassten Stellen. Die für die Begleitung der Umsetzung des OZG von der DSK eingesetzte Kontaktgruppe OZG 2.0 wird weiter gemeinsame Positionen zu den wichtigsten Praxisfragen im Zusammenhang mit diesen Regelungen erarbeiten und die OH OZG entsprechend erweitern und fortlaufend aktualisieren.

266 Abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_OZG_Version_1_1.pdf.
267 § 8a Abs. 3 OZG.
268 Siehe Art. 26 Datenschutz-Grundverordnung (DSGVO).
269 Siehe Art. 28 DSGVO.

V. Inneres

1. Entschließung zum Verhältnis von Datenschutz und Innerer Sicherheit

Im Juni hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Entschließung zum Verhältnis von Datenschutz und Innerer Sicherheit verabschiedet.[270] Anlass waren anstehende Novellierungen verschiedener Sicherheitsgesetze, so auch des Berliner Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG)[271]. Die Entschließung betont, dass Datenschutz ein wesentliches Element des Rechtsstaats und eine Voraussetzung für Sicherheit und Freiheit ist.

Die Entschließung weist zudem darauf hin, dass die Gewährleistung von Datenqualität, klaren Verantwortlichkeiten, effizienten Verfahrensstrukturen sowie digitaler Souveränität für die Gewährleistung von Sicherheit ebenso wichtig ist wie für den Datenschutz. Sicherheitsbehörden wollen qualitativ hochwertige und sorgfältig austarierte Datenbestände, weil sie rechtsstaatlich arbeiten und nur so gute Ergebnisse erzielen können. Die Arbeit der Datenschutzaufsichtsbehörden ist insofern eine wesentliche Instanz der Qualitätssicherung.

Die DSK fordert die umfassende Evaluation bestehender Befugnisse anstelle voreiliger Gesetzgebungsaktivitäten. Die in den vergangenen Jahren stetig erweiterten Eingriffsbefugnisse der Sicherheitsbehörden sollten hinsichtlich ihrer Anwendung in der Praxis und ihrer Wirksamkeit umfassend untersucht werden. Die vom Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht im Auftrag des Bundes durchgeführte Studie zur Überwachungsgesamtrechnung bietet hierfür eine gute Grundlage.[272]

---

270 DSK, Entschließung vom 16. Juni 2025: „Ohne Sicherheit keine Freiheit – Ohne Freiheit keine Sicherheit“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2025/20250617-DSK-Entschliessung_Innere-Sicherheit.pdf.

271 Siehe B.VII.1.

272 Abrufbar unter https://csl.mpg.de/de/projekte/ueberwachungsbarometer.

Bestehende Eingriffsbefugnisse der Sicherheitsbehörden müssen evidenzbasiert überprüft werden, bevor neue Eingriffsmöglichkeiten geschaffen werden. Datenschutzrechtliche Anforderungen flankieren notwendige Modernisierungsvorhaben im Sicherheitsbereich rechtsstaatlich.

2. Entschließung zur verfassungskonformen Ausgestaltung automatisierter Datenanalysen durch Polizeibehörden

Die DSK hat sich im September mit den rechtlichen und technischen Anforderungen an automatisierte Datenanalyseverfahren durch Polizeibehörden befasst. Der Einsatz solcher Analysemethoden betrifft nicht nur mutmaßliche Straftäter:innen, sondern potenziell alle Menschen, deren Daten in polizeilichen Datenbeständen gespeichert sind. Für den Einsatz solcher Verfahren sind spezifische gesetzliche Rechtsgrundlagen erforderlich, die verfassungsrechtlichen Maßstäben genügen und digitale Souveränität des Staates wahren.

In einer Entschließung formuliert die DSK grundlegende Anforderungen an den Einsatz automatisierter Datenanalyseverfahren durch Polizeibehörden.[273] Hintergrund ist die aktuelle Diskussion über die Einführung komplexer Datenanalyseverfahren für verschiedene Polizeien. Die bereits in einzelnen Bundesländern eingesetzten Verfahren können erhebliche Datenmengen umfassen. So bezieht sich etwa das in Bayern eingesetzte Verfahren auf circa 39 Millionen Personendatensätze. Neben mutmaßlichen Straftäter:innen können auch Geschädigte, Zeug:innen oder Personen, die den Polizeinotruf genutzt haben, in solche Analysen einbezogen sein.

Die Entschließung stützt sich wesentlich auf ein Urteil des Bundesverfassungsgerichts (BVerfG) zur automatisierten Datenanalyse.[274] Darin wird erklärt, dass das Gewicht des mit einer solchen Analyse verbundenen Grundrechtseingriffs durch Art und Umfang der zu verarbeitenden Daten sowie die vorgesehenen Analysemethoden bestimmt wird. Ein

273 Entschließung der DSK vom 17. September 2025: „Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten!“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2025/20250917-DSK-Entschliessung_Automatisierte-Datenanalyse.pdf.

274 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20.

besonderes Eingriffsgewicht liegt regelmäßig vor, wenn umfangreiche Datenbestände zu Personen analysiert werden, die selbst keinen Anlass für polizeiliche Maßnahmen gegeben haben, oder wenn Daten verschiedener Systeme trotz ursprünglich unterschiedlicher Zwecke in eine Gesamtauswertung einbezogen werden. Die DSK leitet aus den Vorgaben ab, dass allgemeine Befugnisse im Polizeirecht und in der Strafprozessordnung den Besonderheiten dieser komplexen Analysemethoden nicht ausreichend Rechnung tragen. Erforderlich sind spezifische gesetzliche Rechtsgrundlagen, die Art und Umfang der Daten sowie die Verarbeitungsmethoden klar begrenzen. Bei solchen schwerwiegenden Grundrechtseingriffen ist der Einsatz zudem nur zum Schutz gewichtiger Rechtsgüter wie Leib, Leben und Freiheit von Person sowie Bestand oder Sicherheit des Bundes oder eines Landes – und nur unter strenger Begrenzung des Anlasses für die Maßnahme – zulässig. Zudem sind Transparenz, individueller Rechtsschutz und aufsichtliche Kontrolle gesetzlich vorzusehen.

Einen weiteren Schwerpunkt legt die Entschließung auf die Gewährleistung der digitalen Souveränität. Werden Systeme von Fremdanbietern eingesetzt, muss der Ausschluss von Zugriffen aus oder Datentransfers in Drittstaaten gewährleistet sein, deren Rechtsordnung nicht mit dem europäischen Recht vereinbar ist. Als konkrete Chance zur Entwicklung datenschutzkonformer Lösungen sieht die DSK das IT-Großprojekt Polizei 20/20 (P20), in dessen Rahmen verfassungskonforme Auswerte- und Analysetools auf Basis transparenter und kontrollierbarer Open-Source-Produkte entwickelt werden können.

Komplexe Datenanalyseverfahren durch Polizeibehörden erfordern spezifische gesetzliche Grundlagen, die den verfassungsrechtlichen Maßstäben genügen. Zudem muss die digitale Souveränität bei der Auswahl der Verfahren gewährleistet werden.

VI. Gesundheit und Forschung

1. Anwendungshinweise zu den Anforderungen an Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken

Für die wissenschaftliche Forschung zu medizinischen Zwecken spielt die internationale Zusammenarbeit eine immer wichtigere Rolle. Falls im Rahmen von internationalen Forschungskooperationen personenbezogene Daten verarbeitet werden, müssen die Anforderungen der Datenschutz-Grundverordnung (DSGVO) hinsichtlich der Datenübermittlung in Länder außerhalb des Europäischen Wirtschaftsraums (EWR) beachtet werden. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat Anwendungshinweise zu verschiedenen Rechtsgrundlagen für die Übermittlung von personenbezogenen Daten (wie z. B. Gesundheitsdaten und Daten, die in Biomaterialien enthalten sind) an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken veröffentlicht.[275]

Die Zulässigkeit von Übermittlungen personenbezogener Daten an Drittländer kann nicht pauschal, sondern nur im konkreten Einzelfall bewertet werden, da zahlreiche Umstände für die Bewertung eine Rolle spielen. Dies gilt auch im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken. Datenübermittlungen an Drittländer werden stets in zwei Stufen geprüft.[276] Zunächst muss auf erster Stufe geprüft werden, ob es für die Verarbeitung eine Rechtsgrundlage gibt.[277] Insofern ist ebenfalls zu prüfen, ob eine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO vorliegt, die eine Verarbeitung besonderer Kategorien von Daten erlaubt. Darüber hinaus sind alle einschlägigen sonstigen Bestimmungen der DSGVO einzuhalten. Auf der zweiten Stufe ist dann zu prüfen, ob die Übermittlung personenbezogener Daten an ein Drittland auf eine der Bestimmungen des Kapitels 5 DSGVO gestützt werden kann.

---

275 Abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen.pdf.

276 Siehe Art. 44 Satz 1 DSGVO.

277 Siehe Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 und Art. 9 DSGVO.

Schließlich ist stets zu prüfen, ob auch eine hinreichende Information der Betroffenen über die (beabsichtigte) Übermittlung erfolgt.[278]

Die Anwendungshinweise der DSK unterstützen Forschende bei der Prüfung der Zulässigkeit der Übermittlung personenbezogener Daten an Drittländern im Rahmen von internationalen Forschungsprojekten. Sie zeigen auf, welche Besonderheiten bei der Prüfung der ersten und zweiten Stufe der Zulässigkeit zu beachten sind, und geben Empfehlungen zur Erfüllung der Informationspflichten.

2. Mehr Klarheit für Heilberufspraxen und Patient:innen beim Einsatz von Terminverwaltungsdienstleistern

Wir erhalten regelmäßig Anfragen und Beschwerden rund um den Einsatz von Terminverwaltungsdienstleistern im Gesundheitsbereich. Patient:innen und Arztpraxen ist insoweit häufig nicht klar, wer für die Verarbeitung personenbezogener Daten verantwortlich ist und welcher Einsatz wann zulässig ist. Um Orientierung und Hilfestellung zu geben, hat die DSK dazu ein Positionspapier veröffentlicht, an dessen Ausarbeitung wir maßgeblich beteiligt waren.[279]

Immer häufiger nutzen Patient:innen die Möglichkeit, Arzttermine online zu vereinbaren. Praxen setzen hier auf externe Dienstleister. Mithilfe dieser kann entweder über die Homepage der Arztpraxis oder direkt über die Homepage des jeweiligen Dienstleisters ein Termin vereinbart werden. Die Terminverwaltungsunternehmen stellen auch Terminkalender für die Praxen bereit, in die zusätzlich telefonisch vereinbarte Termine eingetragen werden können. Neben den Praxen und ihren Patient:innen ist also auch noch das Terminverwaltungsunternehmen in die Terminvereinbarung involviert.

Mit dem Positionspapier der DSK soll allen Seiten Orientierung gegeben werden. Eine Beauftragung von externen Unternehmen zum Terminmanagement, z. B. bei der

278 Siehe Art. 13, 14 DSGVO.

279 DSK, Beschluss vom 16. Juni 2025: „Datenschutz bei der Terminverwaltung durch Heilberufspraxen – Positionspapier zum datenschutzkonformen Einsatz von Dienstleistern für Online-Terminbuchungen und das Terminmanagement“, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/DSK-Beschluss_Positionspapier_Terminverwaltungsunternehmen.pdf.

Terminvergabe im Praxiskalender, kann als Auftragsverarbeitung[280] zulässig sein. In diesen Fällen bleibt die Arztpraxis verantwortliche Stelle für die Datenverarbeitung. Patient:innen müssen dann auch nicht in die Verarbeitung durch den Dienstleister einwilligen, allerdings über den Einsatz regelmäßig informiert werden.[281] Gleichzeitig hat die Arztpraxis weitere Anforderungen zu beachten, um den Einsatz datenschutzkonform auszugestalten. So ist etwa nur eine erforderliche Datenverarbeitung ohne Einwilligung zulässig. Für die medizinische Behandlung notwendig kann bspw. das Eintragen von bestimmten Patientdaten in einen Terminkalender sein, wenn die konkrete Patientin oder der konkrete Patient einen in der Zukunft liegenden Termin in der Praxis vereinbart. Für Terminnachrichten wie etwa Erinnerungen bedarf es dagegen einer ausdrücklichen Einwilligung von Patient:innen. Auch ist es unzulässig, pauschal alle Patientenstammdaten im Vorfeld an den Dienstleister zu übermitteln.

Gleichzeitig ist zu beachten: Bei einer Datenverarbeitung in Verbindung mit einem Nutzerkonto bei einem Terminverwaltungsunternehmen ist dieses Unternehmen als Vertragspartner der den Dienst nutzenden Patient:innen selbst Verantwortlicher, und nicht die Arztpraxis. Werden insoweit auch Gesundheitsdaten verarbeitet, benötigt das Terminveraltungsunternehmen im Regelfall eine wirksame Einwilligung der Nutzer:innen. Wichtig ist zudem, dass für Patient:innen für die Geltendmachung ihrer Rechte immer klar erkennbar sein muss, wer für eine Verarbeitung verantwortlich ist.

Terminverwaltungsunternehmen ermöglichen die Onlinevereinbarung von Arztterminen. Der Einsatz solcher Systeme durch Arztpraxen ist im Wege der Auftragsverarbeitung möglich. Um dem Schutz der besonders sensiblen Gesundheitsdaten Rechnung zu tragen, unterstützt die DSK Praxen und Patient:innen durch ein Positionspapier, das die wichtigsten Fragen in diesem Zusammenhang klärt. Andere Möglichkeiten der Terminvereinbarung, etwa telefonisch oder vor Ort, sollten dennoch weiter neben Onlinevereinbarungen möglich sein.

280 Art. 28 DSGVO.
281 Art. 13 DSGVO.

3. Weiterverarbeitung von personenbezogenen Daten zu wissenschaftlichen Forschungszwecken

In der Praxis kommt es häufig vor, dass ein Verantwortlicher Daten, die er für einen bestimmten Zweck verarbeitet hat, nunmehr für einen anderen Zweck weiterverarbeiten möchte. Im Falle der Weiterverarbeitung zu Forschungszwecken sieht die DSGVO eine Privilegierung vor. Wir haben uns mit der Frage befasst, ob sich der Verantwortliche hinsichtlich dieser Weiterverarbeitung auf die ursprüngliche Rechtsgrundlage stützen kann.

Der Europäische Datenschutzausschuss (EDSA) bereitet derzeit Leilinien zur wissenschaftlichen Forschung vor, die Forschenden eine Hilfestellung zu datenschutzrechtlichen Fragen im Zusammenhang mit ihren Forschungsprojekten geben soll. In diesem Zuge waren wir über die Compliance, eGovernment und Health Expert Subgroup (CEH ESG) des EDSA und die entsprechende deutsche Landesvertretung sowie über den Arbeitskreis Wissenschaft und Forschung der DSK mit verschiedenen Rechtsfragen und einer deutschen Position hierzu befasst.

Eine Frage taucht im Zusammenhang mit der Forschung, aber auch in anderen Kontexten regelmäßig auf: Unter welchen Voraussetzungen dürfen Daten, die zu einem bestimmten Zweck verarbeitet wurden oder werden, zu einem anderen Zweck weiterverarbeitet werden? Grundsätzlich hat ein Verantwortlicher zu prüfen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen Zweck, zu dem die Daten ursprünglich erhoben wurden, vereinbar ist.[282] Die Weiterverarbeitung von Daten zu wissenschaftlichen Zwecken wird durch die DSGVO allerdings privilegiert, d. h. sie gilt nicht als unvereinbar mit dem ursprünglichen Zweck.[283] Fraglich ist jedoch, ob die Rechtsgrundlage für die Erstverarbeitung auch für eine nachfolgende Weiterverarbeitung für Zwecke der wissenschaftlichen Forschung verwendet werden kann oder ob der Verantwortliche zumindest prüfen muss: Kann die Weiterverarbeitung auf die Rechtsgrundlage der Erstverarbeitung gestützt werden?

Nach der im EDSA vertretenen deutschen Auffassung kann die Weiterverarbeitung zu wissenschaftlichen Zwecken jedenfalls nicht immer auf die Rechtsgrundlage der

282 Siehe Art. 6 Abs. 4 DSGVO.
283 Siehe Art. 5 Abs. 1 lit. b, 2. Hs. DSGVO.

Erstverarbeitung gestützt werden, weil die der Zulässigkeit der Weiterverarbeitung zugrunde liegenden Normen[284] zusammengelesen werden müssen. Nach Art. 6 Abs. 4 DSGVO ist die Frage der Zweckbindung erst nach der Wahl der Rechtsgrundlage zu klären, d. h., zuerst ist das Vorliegen einer Rechtsgrundlage zu prüfen, erst nachfolgend ist dann zu bewerten, ob eine Zweckkompatibilität vorliegt. Die nach Art. 5 Abs. 1 lit. b, 2. Hs. DSGVO privilegierte Weiterverarbeitung zu wissenschaftlichen Forschungszwecken führt dazu, dass der Kompatibilitätstest verkürzt werden kann.

Wenn ein Verantwortlicher Daten, die er zu einem anderen Zweck verarbeitet hat, zu wissenschaftlichen Forschungszwecken weiterverarbeiten will, muss er prüfen, ob die Weiterverarbeitung auf die Rechtsgrundlage der Erstverarbeitung gestützt werden kann oder eine andere Rechtsgrundlage in Betracht kommt. Liegt eine solche Rechtsgrundlage vor, wird die Weiterverarbeitung zu wissenschaftlichen Forschungszwecken dergestalt privilegiert, dass Art. 6 Abs. 4 DSGVO nicht mehr geprüft werden muss.

284 Art. 5 Abs. 1 lit. b, 2. Hs. DSGVO und Art. 6 Abs. 4 DSGVO.

VII. Wirtschaft und Digitalwirtschaft

1. Code of Conduct des Gesamtverbands der Deutschen Versicherungswirtschaft

Zum Ende dieses Jahres haben wir nach intensiven Verhandlungen mit dem Gesamtverband der Versicherungswirtschaft e. V. (GDV) die Verhaltensregeln der Deutschen Versicherungswirtschaft genehmigt.

Verhaltensregeln, auch Code of Conduct (CoC) genannt, sind ein freiwilliges Instrument zur Selbstregulierung einer Branche oder eines speziellen Verarbeitungsbereiches auf dem Gebiet des Datenschutzes. Das Datenschutzrecht soll mit den Regeln für den jeweiligen Bereich präzisiert werden. In Art. 40 Abs. 5 Datenschutz-Grundverordnung (DSGVO) ist festgelegt, dass der Entwurf solcher Regeln der zuständigen Aufsichtsbehörde vorgelegt werden muss. Die Aufsichtsbehörde genehmigt die Regeln, wenn sie mit der DSGVO vereinbar sind, eine wirksame Anwendung der Verordnung erleichtern und die Datenschutzstandards in dem jeweiligen Bereich konkretisieren oder verbessern.

Die Verhaltensregeln der Deutschen Versicherungswirtschaft decken ein breites Spektrum an Verarbeitungen personenbezogener Daten durch Versicherer ab. Es werden bspw. Grundsätze der bereichsspezifischen Datenverarbeitung aufgeführt, das Vorgehen bei Auskunftsersuchen konkretisiert, aber auch automatisierte Entscheidungsfindungen bei Vertragsabschluss und Schadensregulierung geregelt.

Verhaltensregeln der Deutschen Versicherungswirtschaft bestanden in anderer Form schon vor Geltung der DSGVO. Mit Wirksamwerden der DSGVO hat der GDV eine neuerliche Genehmigung von Verhaltensregeln nach der DSGVO angestrebt und bei uns als zuständige Aufsichtsbehörde einen entsprechenden Antrag gestellt. Mit Unterstützung von Vertreter:innen der Aufsichtsbehörden aus Bayern, Baden-Württemberg, Niedersachen und Nordrhein-Westfalen haben wir zunächst ein umfangreiches Gutachten

zu den Verhaltensregeln erarbeitet. Im Wesentlichen haben wir darin kritisiert, dass die Verhaltensregeln die DSGVO nicht ausreichend präzisieren,[285] sondern häufig nur den Regelungsgehalt der Gesetzesnormen wiederholen. Zudem hätten einige Formulierungen in dem ursprünglichen Entwurf des CoC so ausgelegt werden können, dass die dortigen Regeln hinter dem Schutzniveau der DSGVO zurückbleiben.

Der GDV hat daraufhin im Rahmen von Verhandlungen umfangreiche Änderungen an den Verhaltensregeln vorgenommen, sodass diese die DSGVO nun vielfach präzisieren und konkretisieren. Wiederholende Passagen wurden gestrichen und Angleichungen an die Begrifflichkeiten der DSGVO vorgenommen, sodass Missverständnisse vermieden werden. Beispielsweise wurde die Regelung zu automatisierten Einzelfallentscheidungen präzisiert, indem für automatisierte Entscheidungen zulässige Fallgruppen aufgenommen wurden. Für die Verarbeitung von Gesundheitsdaten durch die Krankenversicherer bedarf es teilweise Einwilligungs- bzw. Schweigepflichtentbindungserklärungen. Die Regelung in den Verhaltensregeln wurde so angepasst, dass sie sowohl dem deutschen Zivilrecht als auch der Entwicklung im Datenschutzbereich, Minderjährige möglichst frühzeitig selbst über sie betreffende Datenverarbeitungen entscheiden zu lassen, entspricht. Die Informationspflichten zu eingesetzten Auftragsverarbeitern wurden deutlich konkretisiert. Unzulässige Datenverarbeitungen wurden gestrichen und die Regeln für die noch zu genehmigende Stelle, die die Verhaltensregeln überwacht,[286] nachgeschärft. Zudem wurden die Meldepflichten der Überwachungsstelle bei festgestellten Verstößen an die Aufsichtsbehörden ausgeweitet.

Die Verhaltensregeln wurden von allen deutschen Aufsichtsbehörden in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zur Kenntnis genommen und eine Genehmigung durch uns insgesamt befürwortet.

Die von uns genehmigten Verhaltensregeln der Deutschen Versicherungswirtschaft sollen dazu beitragen, eine wirksame Anwendung der DSGVO in der Praxis zu erleichtern und die Datenschutzstandards in diesem Bereich zu verbessern.

285 Siehe Art 40 Abs. 2 DSGVO.
286 Siehe Art. 40 Abs. 4 und Art. 41 Abs. 1 DSGVO.

2. Fortschritte bei Zertifizierungsverfahren

In diesem Jahr wurden zwei weitere Zertifizierungsstellen in Deutschland akkreditiert. Die in den Genehmigungsprozessen gesammelten Erfahrungen wurden in die „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ der DSK aufgenommen, um sie für zukünftige Programme nutzbar zu machen.

Bislang sind in Deutschland drei Zertifizierungsverfahren genehmigt worden. Dieses Jahr wurden von der Deutschen Akkreditierungsstelle und den zuständigen Aufsichtsbehörden zwei weitere Zertifizierungsstellen akkreditiert: Die Datenschutz cert GmbH und PricewaterhouseCoopers (PWC).

In die Genehmigungsverfahren für die Zertifizierungsprogramme sind regelmäßig alle deutschen Aufsichtsbehörden und der Europäische Datenschutzausschuss (EDSA) involviert. Ein wiederkehrender Diskussionsgegenstand war dabei die Zertifizierung von Auftragsverarbeitung, entweder durch eine eigene Zertifizierung des Auftragsverarbeiters oder durch die Zertifizierung eines Verantwortlichen, der Auftragsverarbeiter einbindet. Der EDSA hat hierzu in einer Stellungnahme bestimmte Verpflichtungen im Zusammenhang mit Auftragsverarbeitern und Unterauftragsverarbeitern erläutert.[287] Er hat dabei klargestellt, dass die Einbindung eines Auftragsverarbeiters das Schutzniveau nicht verringern darf. Außerdem dürfen als hinreichende Garantien der Auftragsverarbeiter[288] nur solche herangezogen werden, die auch tatsächlich nachgewiesen werden können. Daraus ergab sich die Frage, mit welchen Prüfmethoden die Zertifizierungsstelle das Vorliegen der Garantien in der Praxis überprüfen kann. Das Papier der DSK „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ wurde in einer Arbeitsgruppe mit unserer Beteiligung in diesem Punkt noch einmal überarbeitet und in der Version 3.0 verabschiedet.[289]

287 EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222024-certain-obligations-following_de.

288 Siehe Art. 28 Abs. 1 DSGVO.

289 Siehe https://datenschutzkonferenz-online.de/media/ah/DSK_Zertifizierungskriterien_Version_3_0.pdf.

Ein weiterer Diskussionsgegenstand war die Frage, wie in überwiegend allgemein gehaltenen Zertifizierungsprogrammen die Anforderungen an die technisch-organisatorischen Maßnahmen[290] formuliert und ihre Einhaltung durch die Zertifizierungsstelle überprüft werden kann. Vor diesem Hintergrund wurde auch der entsprechende Abschnitt in dem DSK-Papier unter unserer maßgeblichen Beteiligung überarbeitet. Es wurde klargestellt, dass nur eine anerkannte Methodik der Risikoermittlung, -bewertung und -behandlung Grundlage solcher Maßnahmen sein kann. Zudem wurden mögliche Prüfmethoden auf Grundlage von EDSA-Leitlinien ergänzt.[291]

Die Etablierung von Zertifizierungsprogrammen in Deutschland zeigt, dass zwischen theoretischer Konzeption und praktischer Umsetzung eine intensive Phase der Erfahrungssammlung und Konkretisierung erforderlich ist. Die kontinuierliche Überarbeitung der Anforderungspapiere auf Basis der in den Genehmigungsverfahren gesammelten Erfahrungen gewährleistet, dass die Zertifizierungsprogramme den gesetzlichen Anforderungen in der Praxis gerecht werden. Die Begleitung der praktischen Anwendung wird zeigen, ob die Anforderungen zu den erwarteten Verbesserungen führen.

3. Erste Erfahrungen mit der Verordnung über die Transparenz und das Targeting politischer Werbung

Seit dem 10. Oktober 2025 gilt die EU-Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO).[292] Sie sieht für das gezielte Ausspielen politischer Werbung im Internet spezifische Verbote sowie Dokumentations- und Informationspflichten für Verantwortliche vor. Die Datenschutzbehörden sind für die Aufsicht über die Einhaltung der Artikel der Verordnung zuständig, die sich mit gezielter politischer Onlinewerbung befassen, bei der personenbezogene Daten verarbeitet werden.

290 Siehe Art. 24 und 25 DSGVO.

291 EDSA, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_de.

292 Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024.

Politische Akteur:innen nutzen heutzutage vielfach digitale Medien, um ihre Botschaften zu transportieren. Dabei setzen sie auch auf Targetingverfahren, also auf die gezielte Ausspielung von Werbebotschaften an Personengruppen, basierend auf deren demografischen Daten, politischen Interessen oder Verhaltensweisen. Diese Daten werden zuvor im Hintergrund durch Werbenetzwerke mittels Trackingtechnologien erhoben, ausgewertet und bestimmten Interessenskategorien zugeordnet.

Die TTPW-VO sieht zusätzliche Anforderungen für die Verarbeitung personenbezogener Daten im Zusammenhang mit politischer Onlinewerbung unter Einsatz von Targeting- und Anzeigenschaltungsverfahren vor. Dies können bspw. personalisierte Wahlkampagnen auf Social-Media-Plattformen oder per Newsletter sowie politische Anzeigen auf Websites sein.

Nach Art. 18 TTPW-VO ist zielgerichtete personalisierte politische Werbung im Internet nur zulässig, wenn Verantwortliche die verwendeten personenbezogenen Daten von den betroffenen Personen selbst erhoben haben, diese ausdrücklich für diesen Zweck eingewilligt haben und kein Profiling auf Basis besonders schützenswerter Daten der Personen, wie der politischen Meinung oder Gesundheitsdaten, stattfindet. Ausnahmen gelten u. a. für Mitteilungen von politischen Parteien, Stiftungen, Verbänden oder anderen gemeinnützigen Einrichtungen an ihre (ehemaligen) Mitglieder sowie Newsletter-Abonnent:innen.

Die Verordnung sieht zudem eine Reihe von Dokumentations- und Informationspflichten für Verantwortliche vor, wenn sie Targeting- oder Anzeigenschaltungsverfahren bei politischer Werbung im Internet einsetzen.[293] Verantwortliche müssen z. B. interne Regelungen treffen, Protokolle über den Einsatz führen und den betroffenen Personen umfangreiche Informationen zur Verfügung stellen.

Die TTPW-VO sieht auch ein eigenes Beschwerderecht vor, nach dem Personen oder Einrichtungen mögliche Verstöße gegen diese Verordnung den Aufsichtsbehörden mitteilen können. Zuständig für die Überwachung der Vorgaben zum Targeting und zur Anzeigenschaltung im Zusammenhang mit politischer Werbung im Internet sind die Datenschutzbehörden. Für Verantwortliche mit Sitz in Berlin wie Parteien, Politiker:innen

293 Siehe Art. 19 TTPW-VO.

oder Werbedienstleistende ist unsere Behörde zuständig. Die datenschutzrechtlichen Aspekte der neuen Regelungen erläutern wir auf unserer Website.[294]

Wir haben uns in diesem Jahr auch in Zusammenarbeit mit anderen Aufsichtsbehörden umfangreich mit den neuen Anforderungen im Rahmen unseres Co-Vorsitzes des Arbeitskreises Medien der DSK auseinandergesetzt. Dort haben wir einen Unterarbeitskreis zu dem Thema geleitet und u. a. den Digital Services Coordinator (DSC) in der Bundesnetzagentur bei einer Handreichung zur TTPW-VO[295] gemeinsam mit den anderen Aufsichtsbehörden und den Landesmedienanstalten unterstützt. Daneben haben wir mehrfach auf politischer Ebene im Rahmen des Gesetzgebungsverfahrens zum deutschen Durchführungsgesetz zur TTPW-VO, dem Politische-Werbung-Transparenz-Gesetz (PWTG),[296] Stellung bezogen.

Politische Onlinewerbung auf Basis von gezielten Targetingverfahren birgt ein großes Risiko für das informationelle Selbstbestimmungsrecht und die freie Meinungsbildung. Der Einsatz dieser Verfahren kann u. a. dazu führen, dass Bürgerinnen und Bürger nur noch Werbeanzeigen sehen, die ihre bestehenden Ansichten bestätigen oder allein auf Aufmerksamkeit abzielen. Das gilt es besonders vor Wahlen zu vermeiden. Wir begrüßen daher, dass der europäische Gesetzgeber besondere Schutzmechanismen zur Wahrung der Grundrechte im Bereich der politischen Onlinewerbung geschaffen und hohe Anforderungen an deren Gestaltung festgelegt hat.

294 https://www.datenschutz-berlin.de/themen/werbung/politische-werbung/.

295 Abrufbar unter https://www.dsc.bund.de/DSC/DE/Aktuelles/Downloads/TTPWVerordnung.pdf?__blob=publicationFile&v=2.

296 Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung, abrufbar unter https://bmds.bund.de/service/gesetzgebungsverfahren/politische-werbung-transparenz-gesetz-pwtg.

VIII. Technischer Datenschutz

1. Entschließung zum Confidential Cloud Computing

Confidential Cloud Computing verspricht ein erhöhtes Sicherheitsniveau bei der Verarbeitung personenbezogener Daten in der Cloud, doch der Begriff wird von entsprechenden Anbieter:innen für verschiedene Technologien genutzt. Um Verantwortlichen Orientierung zu geben, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Entschließung verabschiedet. Diese definiert Angreifermodelle und Anforderungen an die Verschlüsselung, um personenbezogene Daten in Cloud-Umgebungen effektiv zu schützen.

Aufgrund wiederkehrender Anfragen zur datenschutzrechtlichen Einordnung der Nutzung von Cloud-Ressourcen, insbesondere im Gesundheitsbereich, haben wir im Arbeitskreis Technik der DSK eine Entschließung zum Themenkomplex „Confidential Cloud Computing“ erarbeitet. Diese wurde im Juni dieses Jahres veröffentlicht.[297]

Darin wird klargestellt, dass eine Abgrenzung der Technologien unter dem Begriff „Confidential Cloud Computing“ schwierig ist. Um verantwortlichen Stellen trotzdem Orientierung bieten zu können, werden in der Entschließung Punkte angesprochen, die bei der Verarbeitung personenbezogener Daten in Cloud-Umgebungen zu berücksichtigen sind. Der Fokus wird vor allem auf das Angreifermodell und das Schlüsselmanagement gelegt.

Das Angreifermodell beschreibt verschiedene Bedrohungsszenarien, mit denen bei Verarbeitungsvorgängen in einer Cloud-Umgebung zu rechnen ist. Das Angreifermodell muss abbilden, ob Schutzziele gegenüber anderen Nutzenden der gleichen Cloud-Umgebung (potenziell auf derselben Hardware) oder zusätzlich gegen Zugriffsmöglichkeiten innerhalb der Organisation der Betreiber:innen gewährleistet werden sollen. Die Entschließung weist ausdrücklich darauf hin, dass Betreiber:innen

297 DSK, Entschließung vom 16. Juni 2025, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/DSK-Entschliessung_Confidential_Cloud_Computing.pdf.

physikalischen Zugang zu den verarbeitenden Systemen haben. Da die Kontrolle über die Verfügbarkeit der Verarbeitung bei der Betreiberorganisation liegt, kann diese nicht gewährleistet werden, wenn man die Betreibenden selbst als potenzielle Angreifende einstuft.

Besondere Bedeutung kommt dem Schlüsselmanagement zu. Eine Geheimhaltung gegenüber der Betreiberorganisation ist nur möglich, wenn Betreiber:innen keinen Zugriff auf das Schlüsselmaterial und die Entschlüsselung haben. Kritisch sind vor allem Übergänge zwischen verschiedenen Verschlüsselungsdomänen. Müssen bspw. zwischen Speicherung und weiterer Verarbeitung die Schlüssel gewechselt werden, liegen die Daten kurzzeitig unverschlüsselt vor. Sicherheitsanalysen müssen daher Hard- und Software umfassen und die Einsatzszenarien transparent darstellen. Unter der Annahme, dass es keine physikalischen Angriffe gibt, können Techniken des Confidential Cloud Computing einen hohen Mehrwert an Sicherheit und Datenschutz bieten.

Confidential Cloud Computing kann das Sicherheitsniveau signifikant erhöhen, insbesondere gegen andere Nutzende auf derselben Hardware und gegen einzelne Innentäter:innen. Verantwortliche dürfen sich jedoch nicht allein auf das Marketing der Anbieter:innen verlassen, sondern müssen prüfen, ob die eingesetzten Technologien den spezifischen Schutzbedarf – gerade bei Gesundheitsdaten – tatsächlich decken.

2. Anwendung des Standard-Datenschutzmodells

Im November vergangenen Jahres hat die DSK beschlossen, das Standard-Datenschutzmodell (SDM) weiterzuentwickeln. In der Praxis ist die Nachfrage nach konkreten Umsetzungshinweisen für die datenschutzgerechte Organisations- und Technikgestaltung nach wie vor hoch. Durch neue Bausteine und methodische Verbesserungen wird das SDM noch praxistauglicher.

Das SDM hat in den letzten 10 Jahren einen zunehmenden Bekanntheitsgrad unter den Verantwortlichen und Auftragsverarbeitern erreicht. Beide Gruppen können und sollten auf das SDM zurückgreifen, wenn es darum geht, ihre Datenverarbeitung sowohl

organisatorisch als auch technisch grundrechtsorientiert zu gestalten und den Nachweis über die Einhaltung ihrer datenschutzrechtlichen Pflichten zu erbringen.

Im Auftrag der DSK zur Weiterentwicklung des SDM wird nicht nur der zentrale Stellenwert des SDM für die technische Prüfpraxis nochmals bekräftigt, sondern auch für die kommenden zwei Jahre das Ziel gesetzt, die aktuelle Version 3.1 des SDM[298] für die Praxis noch handlicher zu machen. Die Priorität liegt daher auf der Weiter- und Neuentwicklung von Bausteinen, die für typische Verarbeitungspraktiken, wie etwa das Löschen von Daten, die abstrakten Anforderungen im Hinblick auf den Stand der Technik konkretisieren.

Das Projekt zur Weiterentwicklung des SDM umfasst mehrere Arbeitspakete. Dieses Jahr wurden vier zentrale Pakete umgesetzt: die Aktualisierung der Bausteingliederung, die Überarbeitung des Bausteins zur Protokollierung, die Einführung eines Glossars sowie die Modernisierung der generischen Maßnahmen. Unsere Behörde hat bei der Bausteingliederung und dem Glossar aktiv mitgewirkt.

Die nächsten Arbeitspakete betreffen zum einen die Modernisierung der generischen Maßnahmen im SDM-Handbuch im Hinblick auf den neuesten Stand der Technik und zum anderen einen Leitfaden für die Anbindung externer Expertise. Bei ersterem liegt der Fokus vor allem auf einer klareren Sprache und einer stärkeren Bezugnahme auf bekannte Standards[299] sowie der Differenzierung zwischen Maßnahmen und Konzepten, wobei das letztere der Maßnahmenplanung dient. Mit dem Leitfaden stellt sich die DSK der Aufgabe, ein Format für die Kooperation mit der gewachsenen Community der SDM-Praktiker:innen bzw. der Fachkräfte im „Datenschutz-Engineering“ zu entwickeln, um das dort vorhandene wertvolle Erfahrungswissen über praktische und wirtschaftliche Datenschutzlösungen einzubinden. Und nicht zuletzt ist mit dem Arbeitspaket „Sonderedition“ eine Schritt-für-Schritt-Anleitung geplant, die, ähnlich wie der Standardprozess Datenschutz für den öffentlichen Bereich, das methodische Vorgehen zur datenschutzgerechten Technikgestaltung kurz und bündig erklärt.

298 Abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf.

299 Siehe Grundschutz++, ISO 27002.

Das SDM hat sich als zentraler Standard für die Prüfpraxis etabliert. Mit der systematischen Weiterentwicklung hin zu mehr Praxisnähe durch konkrete Bausteine wird das Modell seinem Anspruch gerecht, eine Brücke zwischen rechtlichen Anforderungen und technischer Umsetzung zu sein. Die geplante Einbindung externer Expertise zeigt: Standardisierung und Praktikabilität sind kein Widerspruch, sondern bedingen einander für einen effektiven Datenschutz.

D.

Wir in Europa und der Welt

I. Gesetzesvorhaben

1. DSK-Positionierung zur geplanten DSGVO-Reform

Die Europäische Kommission hat Vorschläge zur Anpassung der Datenschutz-Grundverordnung (DSGVO), der KI-Verordnung und weiterer Digitalrechtsakte gemacht.[300] Diese Änderungen sollen nach dem Plan der Kommission in einem Schnellverfahren vom Europäischen Gesetzgeber verabschiedet werden (sog. Omnibusverfahren). Wir haben unsere Expertise aus der praktischen Aufsichtsarbeit als diesjähriger Vorsitz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) direkt in den europäischen Prozess eingebracht.

Grundsätzlich sehen auch wir einen Reformbedarf im Datenschutzrecht. Insbesondere sollten die DSGVO und die Digitalrechtsakte besser aufeinander abgestimmt werden. Außerdem sollte sich das Datenschutzrecht stärker an der Relevanz der Verarbeitungsvorgänge für die Grundrechte der betroffenen Personen orientieren, was aber einer breiten Diskussion in einem ordentlichen Gesetzgebungsverfahren bedarf. Die Vorschläge der Europäischen Kommission enthalten nicht nur kleinere Anpassungen, sondern sehen zum Teil weitreichende Änderungen des Datenschutzrechts vor, die für ein Schnellverfahren ungeeignet sind. So soll bspw. die Definition des Begriffs der personenbezogenen Daten verändert werden, was in der Praxis bestimmte Datenverarbeitungen aus dem Schutzbereich der DSGVO herausnehmen sowie große Auswirkungen auf die Bewertung vieler Verarbeitungsvorgänge haben und damit zu neuen Rechtsunsicherheiten führen würde. Dabei war es eigentlich das Ziel der Kommission, das Datenschutzrecht zu vereinfachen, zu entbürokratisieren und kleine und mittlere Unternehmen zu entlasten. Dies ist leider in deren erstem Gesetzentwurf noch nicht gelungen. Vielmehr enthält er neue unbestimmte Rechtsbegriffe wie z. B. den der „nicht-datenintensiven Aktivitäten“, der erst durch Rechtsprechung konkretisiert werden müsste.

300 Siehe https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal.

Als Vorsitz der DSK haben wir auf diese und andere Defizite hingewiesen und insbesondere im Rahmen unserer Zusammenarbeit mit anderen europäischen Aufsichtsbehörden im Europäischen Datenschutzausschuss (EDSA) die Perspektive der praktischen Datenschutzaufsicht eingebracht.[301] Darüber hinaus haben wir in der DSK eigene Vorschläge erarbeitet, wie das Datenschutzrecht sinnvoll weiterentwickelt werden kann:[302]

Hersteller und Anbieter von IT-Diensten in die Pflicht nehmen

So haben wir vorgeschlagen, die Hersteller von Produkten stärker in die Pflicht zu nehmen, ihre Produkte datenschutzkonform auszugestalten. Damit würden nicht mehr die Anwender:innen – d. h. regelmäßig kleine und mittlere Unternehmen oder Vereine – bei der Auswahl und dem Einsatz solcher Produkte die datenschutzrechtliche Hauptlast tragen. Vielmehr sollen Hersteller und Anbieter von IT-Diensten verpflichtet werden, die Grundsätze des Datenschutzes bereits bei der Gestaltung ihrer Produkte stärker zu berücksichtigen. Mit der Herstellerhaftung würde die datenschutzrechtliche Verantwortung dorthin verlagert, wo die Entscheidungen über die Gestaltung von IT-Produkten getroffen werden. Das würde besonders die Position von kleinen und mittleren Unternehmen stärken, die oft nicht in der Lage sind, datenschutzkonforme Prozesse in den genutzten Produkten durchzusetzen, aber bislang allein die rechtliche Verantwortung tragen. Auch die Auftragsverarbeiter sollen verpflichtet werden, ihre Dienste von vornherein datenschutzkonform auszugestalten.

Einsatz von Künstlicher Intelligenz (KI) braucht klare gesetzliche Regelung

Bei der Verarbeitung personenbezogener Daten mithilfe von KI sieht die DSK Bedarf für DSGVO-Reformen, die über die Vorschläge der Kommission hinausgehen. Die DSK fordert, spezifische Rechtsgrundlagen für Entwicklung, Training und Betrieb von KI-Modellen und -Systemen gesetzlich festzulegen, um so für Rechtssicherheit zu sorgen und Innovationen zu ermöglichen. Außerdem bedarf es einer spezifischen Regelung für die Rechte von betroffenen Personen beim Einsatz von KI. Für Einzelfälle, in denen

301 Abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_de.

302 Siehe auch https://www.datenschutz-berlin.de/pressemitteilung/datenschutzkonferenz-macht-reformvorschlaege-fuer-die-datenschutz-grundverordnung/.

Betroffenenrechte technisch nur mit unverhältnismäßigem Aufwand umgesetzt werden können, sollten funktionsäquivalente bzw. kompensatorische Schutzmaßnahmen vorgesehen werden. Wer personenbezogene Daten in einem eingriffsintensiven KI-System verarbeitet, sollte die betroffenen Personen darüber ausdrücklich informieren müssen. Zudem sollten betroffene Personen das Recht erhalten, von Verantwortlichen Auskunft über den Einsatz eines KI-Systems zur Verarbeitung ihrer Daten zu bekommen.

Kinderschutz stärken

Kinder sind besonders schutzbedürftig – auch im digitalen Raum. Vielen Kindern (aber auch deren Erziehungsberechtigten) ist oft nicht bewusst, dass aus ihren Angaben und ihrem Verhalten neue Daten entstehen, die ihr Selbstbild, ihre sozialen Beziehungen und ihr Weltverständnis prägen können. Die DSGVO trägt der besonderen Schutz- und Fürsorgepflicht gegenüber Kindern bereits in vielen Punkten Rechnung – aber nicht in allen. Die DSK hat deshalb einen Zehn-Punkte-Plan zur Verbesserung des gesetzlichen Datenschutzes von Kindern verabschiedet.[303] Darin fordert sie u. a. kindgerechte Voreinstellungen in sozialen Netzwerken und ein Verbot von personalisierter Werbung.

Der Entwurf der Kommission zur DSGVO-Reform verfehlt das selbstgesteckte Ziel des Bürokratieabbaus und der Entlastung kleinerer und mittlerer Unternehmen. Im EDSA haben wir uns dafür eingesetzt, dass die Erfahrungen aufsichtsrechtlicher Praxis im Gesetzgebungsprozess berücksichtigt werden. Darüber hinaus haben wir als Vorsitz der DSK eigene Vorschläge zur Reform des Datenschutzrechts entwickelt. Wir werden den Gesetzgebungsprozess weiter begleiten und insbesondere darauf achten, dass die Reform nicht an den Bedürfnissen der Praxis vorbeigeht.

303 DSK-Entschließung vom 20. November 2025, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2025/20251120-DSK-Entschliessung_Datenschutz_von_Kindern.pdf.

2. Verfahrensverordnung für grenzüberschreitende Fälle

Im November diesen Jahres hat nach dem Europäischen Parlament auch der Rat der Europäischen Union (Ministerrat) dem Entwurf der Verordnung über zusätzliche Verfahrensregeln für die Durchsetzung der DSGVO (VVO)[304] zugestimmt.[305] Das Gesetz soll die Zusammenarbeit der Aufsichtsbehörden bei grenzüberschreitenden Fällen weiter vereinheitlichen. Durch die VVO werden Rechte und Pflichten für Verantwortliche, Beschwerdeführende und Aufsichtsbehörden neu eingeführt bzw. harmonisiert.

Der Verabschiedung der Verordnung ging ein zweijähriger Gesetzgebungsprozess zwischen der Europäischen Kommission, dem Rat der Europäischen Union und dem Europäischem Parlament voraus. Wir haben uns mit anderen deutschen und weiteren europäischen Aufsichtsbehörden an der vorhergegangenen Kommentierung des Gesetzentwurfs durch den EDSA beteiligt.[306] Insbesondere haben wir uns dabei für eine effiziente Verfahrensgestaltung und die Erhaltung bewährter Kooperationsgrundsätze eingesetzt. So hat der Gesetzgeber in Reaktion auf unsere Stellungnahmen das vereinfachte Kooperationsverfahren eingeführt sowie Einschränkungen der Einspruchsrechte im Kooperationsverfahren teilweise zurückgenommen.

Die VVO gibt neue Fristen für die Verfahrensdauer grenzüberschreitender Ermittlungen vor.[307] Die federführende Aufsichtsbehörde muss nun einen Beschlussentwurf i. d. R. 15 Monate nach Erhalt einer Beschwerde vorlegen, in besonders komplexen Fällen i. d. R. nach 27 Monaten. Der Ablauf dieser Fristen kann allerdings durch bestimmte Maßnahmen, wie zusätzliche Anhörungen bzw. Einsprüche, zwischenzeitlich pausiert werden. Die neuen Fristen werden die Kooperationsverfahren deutlich beschleunigen.

304 Verordnung (EU) 2025/2518 vom 26. November 2025 zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679.

305 Siehe auch https://www.europarl.europa.eu/news/en/press-room/20251017IPR30992/data-protection-clearer-rules-for-cross-border-enforcement.

306 Siehe EDSA/EDSB. Gemeinsame Stellungnahme 01/2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-012023-proposal_de; EDSA-Stellungnahme zum Gesetzgebungsprozess der Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-42024-recent-legislative-developments-draft_de.

307 Siehe Art. 12 VVO.

Neue Verfahrensschritte sollen zudem einen möglichst frühen Konsens zwischen der federführenden und den betroffenen Aufsichtsbehörden hinsichtlich des Ermittlungsumfangs ermöglichen.[308] So soll sichergestellt werden, dass die Ermittlungen der federführenden Behörde alle mutmaßlichen verfahrensgegenständlichen Verstöße abdecken. Die fristgebundenen Verfahrensschritte werden aber zusätzliche Ressourcen sowohl der federführenden als auch der betroffenen Aufsichtsbehörden binden.

Zugleich ist ein vereinfachtes Kooperationsverfahren für Fallkonstellationen vorgesehen, zu denen zwischen den Aufsichtsbehörden in der Vergangenheit bereits Einvernehmen bestand.[309] In diesen Fällen muss ein Beschlussentwurf i. d. R. bereits nach 12 Monaten vorliegen. Im Übrigen entspricht das vereinfachte Kooperationsverfahren im Wesentlichen dem derzeitigen Kooperationsverfahren.

Darüber hinaus ermöglicht die VVO europaweit einheitlich eine frühzeitige Beilegung von Beschwerden über Betroffenenrechte.[310] In diesen Fällen kann nun auch die beschwerdeannehmende Aufsichtsbehörde den Verantwortlichen hinsichtlich eines mutmaßlichen Verstoßes kontaktieren, um die Beschwerde beizulegen, z. B. durch Nachholen der Auskunftserteilung. Beschwerdeführende sollen so bei einer raschen und unkomplizierten Durchsetzung ihrer Betroffenenrechte gegenüber Verantwortlichen unterstützt werden.

Beschwerdeführende und Verantwortliche erhalten zudem neue Anhörungsrechte.[311] Die beteiligten Parteien sollen so bereits frühzeitig zu Ermittlungstand und etwaigen Maßnahmen Stellung nehmen können. Zusätzlich wird der Prozess der Akteneinsicht bei grenzüberschreitenden Fällen weiter harmonisiert.[312] Diese Vereinheitlichung soll Verfahrensbeteiligten mehr Rechte geben und zugleich die Behörden durch klare Regelungen entlasten.

308 Siehe u. a. Art. 10 VVO.
309 Siehe Art. 6 VVO.
310 Siehe Art. 5 VVO.
311 Siehe Art. 19 und 20 VVO.
312 Siehe Art. 26 VVO.

Die neue Verordnung ist ab dem 2. April 2027 für grenzüberschreitende Verfahren anwendbar. Unsere Behörde wird aufgrund unserer Beteiligung an zahlreichen grenzüberschreitenden Verfahren bei der Umsetzung der VVO eine maßgebliche Rolle spielen. Neben dem Anpassen der eigenen Verfahren tauschen wir uns kontinuierlich mit anderen deutschen und europäischen Aufsichtsbehörden aus, um eine effiziente und wirksame Umsetzung der neuen Regelungen sicherzustellen. Die neuen Fristen und Verfahren werden den Kooperationsmechanismus zwar beschleunigen, zugleich aber wesentlich mehr behördliche Ressourcen binden als bisher.

II. Mitarbeit im Europäischen Datenschutzausschuss

1. Digitale Souveränität durch den digitalen Euro

Der digitale Euro ist ein Projekt der Europäischen Zentralbank (EZB) und der Europäischen Kommission. Ziel ist es, eine digitale Form der gemeinsamen Währung für den Euroraum zu schaffen und die Europäische Union (EU) damit von nicht-europäischen Zahlungslösungen unabhängiger zu machen. Zur Frage, ob und wie der digitale Euro datenschutzkonform umzusetzen ist, haben wir uns auf europäischer Ebene, insbesondere im Rahmen einer Anhörung im Europäischen Parlament, eingebracht.

Zahlungsdaten gelten seit jeher als besonders aussagekräftig, da aus ihnen neben der finanziellen Situation bspw. auch Informationen über den Gesundheitszustand, das individuelle Verhalten und die Vorlieben, den Aufenthaltsort und die sozialen Beziehungen der Betroffenen abgeleitet werden können. Das heutige Bargeld setzt in dieser Hinsicht praktische Grenzen.

Insbesondere vor dem Hintergrund der zunehmenden Abhängigkeit Europas von digitalen Zahlungsdienstleistern aus Drittländern hat die EZB 2021 ein Projekt zur Evaluierung und Vorbereitung eines digitalen Zahlungsmittels beschlossen, für den die Europäische Kommission 2023 einen ersten Gesetzentwurf[313] vorgelegt hat. Ziel ist die Schaffung eines europäischen digitalen Zahlungsmittels als Ergänzung zum Bargeld, des sog. digitalen Euro.

Geplant ist bislang, den digitalen Euro sowohl in einer online- wie auch einer offlinefähigen Variante anzubieten. Gerade der Offlinevariante wurde von Anfang an die größte Ähnlichkeit zum heutigen Bargeld und damit auch ein hohes Datenschutzniveau zugemessen, denn sie würde den Nutzer:innen ermöglichen, ohne Internetverbindung

313 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einführung des digitalen Euro, KOM(2023) 369 endg., abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52023PC0369.

zu bezahlen. Es besteht jedoch das Risiko, dass das digitale Geld einfach kopiert und mehrfach ausgegeben wird (sog. Double-Spending). Ähnlich wie beim Bargeld, bei dem ausgeklügelte Sicherheitsmerkmale die Echtheit eines Geldscheins garantieren und Fälschungen erschweren, muss die Offlinevariante daher gegen das unbefugte digitale „Drucken" von Geld abgesichert werden.

Doch wie begegnet man der Herausforderung, Double-Spending zu verhindern, ohne das Datenschutzniveau abzusenken? Zu dieser Frage haben wir die Erstellung eines Gutachtens[314] angeregt, das beim Support Pool of Experts (SPE) des Europäischen Datenschutzausschusses (EDSA) zusammen mit anderen deutschen Aufsichtsbehörden sowie der französischen Datenschutzaufsichtsbehörde (CNIL) in Auftrag gegeben wurde.

Der beauftragte Gutachter kommt zu dem Schluss, dass eine Offlinevariante mit hohem Datenschutzniveau, die zugleich das Risiko des Double-Spendings ausreichend reduziert, möglich erscheint. Dafür sei allerdings weitere Forschungsarbeit notwendig und es müssten mit Blick auf die Geschichte vergangener Sicherheitsprobleme[315] komplexe Risikoabwägungen getroffen werden. Das Gutachten deutet überdies darauf hin, dass sich ein fälschungssicheres und auch Geldwäsche verhinderndes digitales Zahlungsmittel mit hohem Datenschutzniveau gerade als Semi-Offlinevariante (Zahler:in oder Zahlungsempfänger:in sind online) und sogar als Onlinevariante verhältnismäßig einfach umsetzen ließe.[316] Die hierfür benötigten kryptografischen Werkzeuge sind seit Jahrzehnten gut erforscht.

Das Gutachten und seine Erkenntnisse stießen auf reges Interesse bei der EZB sowie bei Mitgliedern des Europäischen Parlaments und des dortigen Ausschusses für Wirtschaft und Währung (ECON), in dem der digitale Euro federführend verhandelt wird.

Aktuell arbeitet das Europäische Parlament an einer Position zum Gesetzesvorschlag der Europäischen Kommission zum digitalen Euro. Der Rat der Europäischen Union

314 EDSA (Hg.), The Digital Euro and Its Token-Based Offline Modality, Expert Opinion by Tibor Jager, abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/digital-euro-and-its-token-based-offline_en.
315 Ebd., Kap. 4.1, S. 14 f.
316 Ebd., Kap. 7.5, S. 34 f.

hat sich bereits auf eine Verhandlungsposition geeinigt. Für Mai 2026 ist der Start der Trilog-Verhandlungen zwischen Rat und Parlament angesetzt. Sofern hier eine Einigung über den rechtlichen Rahmen des digitalen Euro erzielt wird, entscheidet die EZB auf dieser Grundlage über dessen Schaffung. Mit einer Einführung des digitalen Euro ist nicht vor 2029 zu rechnen.

Die Schaffung des digitalen Euro wäre auch aus Sicht des Datenschutzes eine entscheidende Weichenstellung, mit der über die Zukunft des digitalen Bezahlens entschieden wird. Ein digitaler Euro mit bargeldähnlichen Eigenschaften erscheint technisch grundsätzlich möglich. Wir setzen uns zusammen mit anderen deutschen und europäischen Aufsichtsbehörden weiter dafür ein, dass es eine datenschutzkonforme Bezahlmethode sein wird.

2. EDSA-Empfehlungen zu Gastkonten

Dürfen Onlineshops die Einrichtung eines Kundenkontos verlangen, wenn man dort etwas kaufen oder gar nur Informationen einholen will? Der EDSA hat unter unserer Beteiligung Empfehlungen[317] zu diesem Thema beschlossen.

Viele Onlineshops verlangen die Einrichtung eines Kundenkontos, wenn man dort etwas kaufen möchte. Selbst der reine Zugriff auf Informationen zum Angebot wird teilweise auf angemeldete Nutzende beschränkt. Der EDSA hat hierzu eine Vielzahl von Fallkonstellationen und denkbaren Rechtsgrundlagen bewertet. Im Ergebnis sind danach verpflichtende Kundenkonten nur unter ganz besonderen Umständen zulässig. Die Empfehlungen gelten dabei ausdrücklich auch für Onlinemarktplätze, auf denen Betreiber:innen den Vertragsschluss mit Dritten vermitteln.

Für den Kauf einer Sache ist regelmäßig kein Kundenkonto erforderlich. Anders kann dies bei Abonnements aussehen: Hier kann ein Kundenkonto notwendig sein, damit die Kund:innen Zugang zu den erworbenen Diensten erhalten können. Die Erforderlichkeit des Kundenkontos endet dann mit Ablauf des Vertrags. Verantwortliche müssen

317 Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites, abrufbar unter https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/recommendations-22025-legal-basis-requiring_en.

zudem nachweisen können, dass tatsächlich ein entsprechender Vertrag abgeschlossen wurde, also insbesondere, dass die betroffene Person insoweit einen Rechtsbindungswillen hatte.

Auch der Zugriff auf exklusive Angebote rechtfertigt keine verpflichtenden Kundenkonten, wenn die Angebote allen Personen zugänglich sind, die ein Konto anlegen (und dafür ihre Daten offenlegen). Anders kann die Bewertung etwa dann ausfallen, wenn die Angebote nur einer ausgewählten Gemeinschaft von Mitgliedern mit bestimmten nachgewiesenen Merkmalen – etwa bestimmten Berufsgruppen – vorbehalten ist und die Teilnahme an dieser Gemeinschaft eine langfristige Geschäftsbeziehung mit dem Verantwortlichen beinhaltet, die zum Hauptgegenstand des Vertrags wird. Eine solche langfristige Geschäftsbeziehung ist wiederum nicht Hauptgegenstand des Vertrags, wenn es bspw. nur um einen Kauf zu Sonderkonditionen für Studierende geht. Diese können ihren Status nämlich auch anderweitig nachweisen.

Soweit die mit dem Kundenkonto verbundenen Datenverarbeitungen nur nützlich sind – etwa im Hinblick auf die Ermöglichung einer Sendungsverfolgung, nachträglicher Änderungen von Bestellungen, leichterer Folgebestellungen, besserer Kundenbindung oder Betrugserkennung und -prävention – ist die verpflichtende Anlage eines Kundenkontos nicht erforderlich und daher unzulässig.

Unternehmen, die für Bestellungen oder den Zugriff auf Angebote bzw. Informationen die Anlage eines Kundenkontos verlangen, sollten überprüfen, ob dies in ihrem Fall ausnahmsweise zulässig ist. Anderenfalls müssen sie ihr Angebot rechtskonform umgestalten und auch eine Bestellung „als Gast“ ermöglichen. Bei der Prüfung ihrer Systeme sollten sie auch die weiteren hilfreichen Hinweise des EDSA aus den Empfehlungen beachten – bspw. dass steuer- und handelsrechtliche Vorschriften[318] in der Regel nur die Aufbewahrung bestimmter Unterlagen wie Rechnungen verlangen, aber nicht die Aufbewahrung der Daten, die zur Erstellung dieser Unterlagen verwendet wurden.

Wer einen Onlineshop oder Onlinemarktplatz betreibt, muss in aller Regel den Zugriff auf Angebote und Informationen sowie die Produktbestellung ohne Anlage eines Kundenkontos ermöglichen. Hier muss also eine Bestellung „als Gast“ möglich sein.

318 Siehe § 147 Abgabenordnung (AO) und § 257 Handelsgesetzbuch (HGB).

III. Internationale Zusammenarbeit

1. Internationale Konferenz der Informationsfreiheitsbeauftragten in Berlin

Vom 23. bis 25. Juni 2025 fand die Internationale Konferenz der Informationsfreiheitsbeauftragten, die „International Conference of Information Commissioners" (ICIC), in Berlin statt, die in diesem Jahr von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) organisiert wurde. Das Hauptthema der Konferenz, auf der auch unsere Behörde vertreten war, war der Zugang zu Umweltinformationen im digitalen Zeitalter.

Die ICIC ist ein weltweites Forum, bei dem jährlich Informationsfreiheitsbeauftragte, Nichtregierungsorganisationen (NROs), Wissenschaftler:innen und die Zivilgesellschaft zusammentreffen, um aktuelle Herausforderungen im Bereich der Informationsfreiheit zu diskutieren.[319] An den ersten zwei Tagen tauschten sich alle Teilnehmenden in Berlin aus, während der dritte Tag dem internen Austausch der Informationsfreiheitsbeauftragten vorbehalten war. Zum ersten Mal fand parallel auch eine Veranstaltung für NROs statt.

Im Rahmen von verschiedenen Veranstaltungen wurden u. a. Themen wie die aktuellen Herausforderungen für Informationsfreiheitsbeauftragte und NROs, der Informationszugang von vulnerablen Gruppen sowie die Auswirkungen von technologischen Entwicklungen wie etwa Open Data auf die Informationsfreiheit diskutiert. Der Fokus lag dabei auf dem Zugang zu Umweltinformationen. Im Anschluss wurde eine Erklärung zur Sicherung des Rechts auf Zugang zu Umweltinformationen in der digitalen Welt verabschiedet.[320] Zudem verabschiedeten auch die zivilgesellschaftlichen Organisationen eine Erklärung zum Recht auf Information und Umweltgerechtigkeit.[321]

---

319 Siehe https://information-commissioners.org.

320 Abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/EN/ICIC/2025-ICIC-Public-Statement.html?nn=253070.

321 Abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/EN/ICIC2025/CSO-Statement.pdf?__blob=publicationFile&v=2.

Beim Treffen der Regionalgruppe der europäischen Informationsfreiheitsbeauftragten wurde zudem das Europäische Netzwerk für Transparenz und Informationszugang (European Network for Transparency and Access to Information, ENTRI) gegründet, um den bereits bestehenden Austausch zwischen den europäischen Institutionen weiter zu vertiefen. Der Vorsitz des neuen Netzwerks wird für die kommenden drei Jahre von der BfDI übernommen. Zu den Gründungsmitgliedern gehört auch unsere Behörde.

Während in Deutschland im Koalitionsvertrag auf Bundesebene eine Verschlankung des Umweltinformationsgesetzes geplant ist,[322] hat die ICIC gezeigt, welche Relevanz der Zugang zu Umweltinformationen weltweit hat. An den Diskussionen auf internationaler Bühne über den Zugang zu Umweltinformationen und an den dort angesprochenen positiven Entwicklungen in anderen Ländern sollte sich Deutschland ein Beispiel nehmen und den Zugang zu Umweltinformationen ausbauen.

2. Internationale Zusammenarbeit in der Berlin Group

Die Internationale Arbeitsgruppe für Datenschutz in der Technologie (IWGDPT), auch Berlin Group genannt, traf sich in diesem Jahr zweimal: im Juli in Tiflis und im November in Montevideo. Die Gruppe veröffentlichte wegweisende Papiere zu Neurotechnologien[323] und Large Language Models[324] (LLMs) und brachte zwei weitere Arbeitspapiere zu Opt-Out-Signalen z. B. in Webbrowsern und zu Confidential Cloud Computing zum Abschluss.[325] Die weltweite Vernetzung von Datenschutzaufsichtsbehörden ermöglicht es, technologische Entwicklungen aus verschiedenen Perspektiven zu bewerten und international abgestimmte Empfehlungen zu erarbeiten.

Die internationale Zusammenarbeit stellt sicher, dass bei der Bewertung neuer Technologien die unterschiedlichen rechtlichen, kulturellen und technologischen

322 Siehe A.II.
323 Abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Berlin-Group/20250515-WP-Neurotechnologies.html.
324 Abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Berlin-Group/20241206-WP-LLMs.html.
325 Nach der Veröffentlichung abrufbar unter https://www.bfdi.bund.de/DE/Fachthemen/Gremienarbeit/Berlin-Group/Berlin-Group-node.html.

Rahmenbedingungen weltweit berücksichtigt werden. Die Arbeitsergebnisse der Gruppe spiegeln damit stets eine multiperspektivische Sicht auf globale Datenschutzherausforderungen wider.

So veröffentlichte die IWGDPT ein umfassendes Arbeitspapier zu Neurotechnologien. Das Papier befasst sich mit Technologien wie Brain-Computer-Interfaces, die direkte Schnittstellen zwischen menschlichem Gehirn und technischen Systemen schaffen. Diese Technologien ermöglichen es, neuronale Aktivität auszulesen und zu interpretieren, bergen jedoch erhebliche Risiken für die informationelle Selbstbestimmung, da sie Zugriff auf besonders sensible Gedanken- und Gefühlszustände ermöglichen. Das Papier analysiert die datenschutzrechtlichen Herausforderungen und gibt konkrete Empfehlungen für Gesetzgeber, Aufsichtsbehörden und Entwickler:innen.

Daneben wurde ein Arbeitspapier zu LLMs veröffentlicht. Das Papier untersucht die Risiken, die durch die Verarbeitung personenbezogener Daten beim Training und bei der Nutzung dieser Modelle entstehen, etwa durch unbeabsichtigte Offenlegung von Trainingsdaten oder durch die Generierung von Falschinformationen über Personen. Die IWGDPT erarbeitete insoweit Leitlinien zur datenschutzkonformen Entwicklung und zum Einsatz von LLMs.

Darüber hinaus wurden zwei weitere Arbeitspapiere fertiggestellt und zur Veröffentlichung beschlossen: Das Papier zu Global Opt-Out Preference Signals befasst sich mit technischen Mechanismen, die es Nutzer:innen ermöglichen, ihre Ablehnung von Tracking und Datenverarbeitung browserübergreifend zu signalisieren. Das zweite Papier behandelt das Thema Confidential Cloud Computing[326]. Hierbei werden Technologien eingeordnet und beschrieben, die es u. a. ermöglichen, Daten auch während der Verarbeitung in der Cloud verschlüsselt zu halten und damit den Zugriff durch Cloudanbieter:innen oder Nutzer:innen derselben Cloudanbieter:innen effektiv zu verhindern.

Bei den Treffen der IWGDPT, an denen unsere Behörde teilnahm, ging es auch um weitere zukunftsweisende Themen und deren Herausforderungen für den Datenschutz:

326 Siehe auch C.VIII.1.

- Eine Arbeitsgruppe zur 6G-Technologie und Joint Communication and Sensing (JCAS) untersucht die nächste Mobilfunkgeneration, bei der Kommunikations- und Sensorfunktionen kombiniert werden, wodurch eine umfassende Umgebungserfassung möglich wird.

- Eine Arbeitsgruppe zu synthetischen Daten analysiert und bewertet den Einsatz künstlich erzeugter Datensätze als Trainingsdaten für KI-Systeme, insbesondere für LLMs. Synthetische Daten können datenschutzfreundliche Alternativen zu realen personenbezogenen Daten sein, bergen jedoch Risiken hinsichtlich der Reproduktion von Verzerrungen aus Originaldaten.

- Eine weitere Gruppe widmet sich Extended Reality (XR), die Virtual Reality, Augmented Reality und Mixed Reality umfasst. Diese immersiven Technologien verschmelzen physische und digitale Welten und kommen in Bereichen wie Bildung, Training, Wartung und Unterhaltung zum Einsatz. Sie erfassen weitreichend biometrische Daten, Bewegungsmuster, Blickrichtungen und Umgebungsinformationen, wodurch tiefgreifende Profile über Nutzer:innen erstellt werden können. Die Arbeitsgruppe entwickelt Empfehlungen zum datenschutzkonformen Einsatz dieser Technologien.

- Zudem arbeitet eine neu gegründete Gruppe an Empfehlungen zum Umgang mit personenbezogenen Daten nach dem Tod betroffener Personen und entwickelt Leitlinien für die sog. digitale Nachlassverwaltung.

Die internationale Vernetzung von Datenschutzaufsichtsbehörden in der IWGDPT ist unverzichtbar, um technologische Entwicklungen frühzeitig zu erkennen und global abgestimmte Lösungsansätze zu entwickeln. Die multiperspektivische Zusammenarbeit ermöglicht es, kulturelle und rechtliche Unterschiede zu berücksichtigen und dennoch gemeinsame Standards für den Schutz personenbezogener Daten zu schaffen. Gerade bei grenzüberschreitend genutzten Technologien wie Cloud Computing und KI-Systemen ist diese koordinierte Herangehensweise entscheidend, um wirksamen Datenschutz weltweit zu gewährleisten. Die Arbeitspapiere der IWGDPT dienen Gesetzgeber, Aufsichtsbehörden und Technologieentwickler:innen als wichtige Orientierungshilfe für die datenschutzkonforme Gestaltung innovativer Technologien.

E.
Anhang

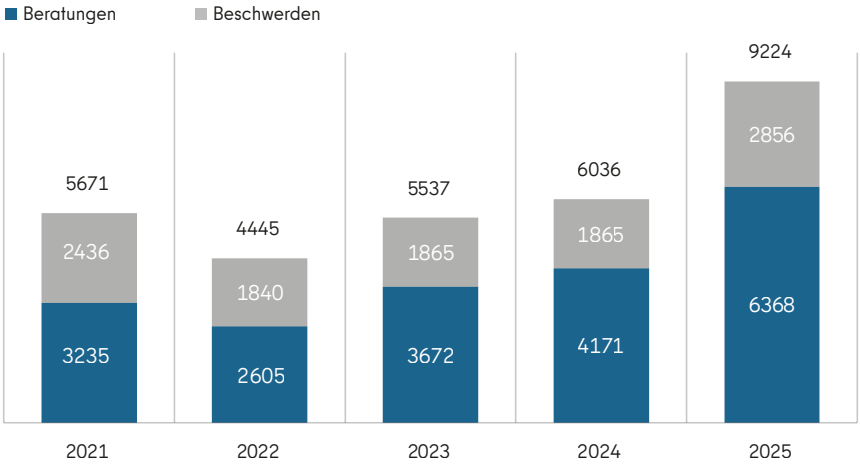
I. Statistik

In diesem Jahr haben sich so viele Menschen mit Beschwerden oder Anfragen an unsere Behörde gewandt wie noch nie zuvor. Auch die Zahl der gemeldeten Datenschutzvorfälle stieg an. 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 9.224 Eingaben von Bürger:innen ein neuer Höchststand seit Einführung der Datenschutz-Grundverordnung (DSGVO) erfasst.[327] Wie bereits im Vorjahr nahmen insbesondere die schriftlichen Beratungen zu. Über das Jahr verteilt wandten sich 6.368 betroffene Personen per Kontaktformular, E-Mail oder Brief mit Anfragen an uns, etwa weil sie Unterstützung bei der Geltendmachung ihrer Rechte oder Beratung zu einem Datenschutzverstoß brauchten. Dies bedeutet eine weitere Zunahme der Beratungsanfragen um rund 53 Prozent im Vergleich zum Vorjahr. Die

Eingaben

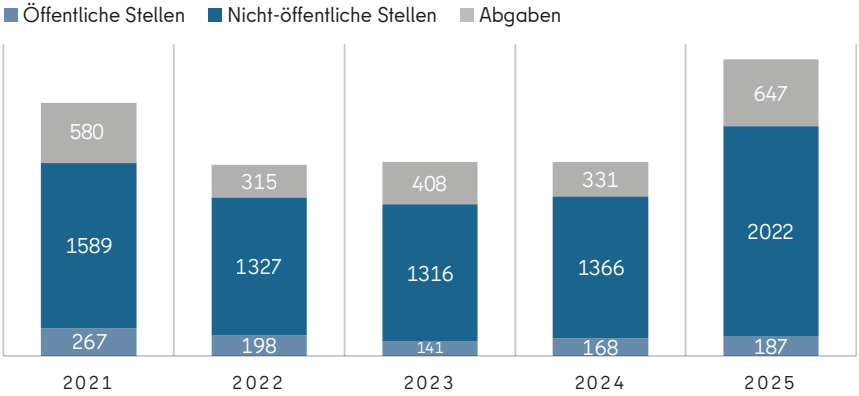


327 Siehe auch B.XV.

Anzahl der an uns gerichteten persönlichen Beschwerden von Betroffenen stieg ebenfalls um etwa die Hälfte auf den neuen Höchstwert von 2.856.

Für den Großteil der Beschwerden eröffneten wir Verfahren in eigener Zuständigkeit. Dies waren in diesem Jahr 2.209 Verfahren. Die meisten davon (2.022) richteten sich gegen nicht-öffentliche Stellen, die restlichen (187) betrafen Behörden und andere öffentliche Stellen. In 647 Fällen lagen die Beschwerden nicht in unserem Zuständigkeitsbereich, weshalb wir sie an die jeweils zuständigen Aufsichtsbehörden abgegeben haben.

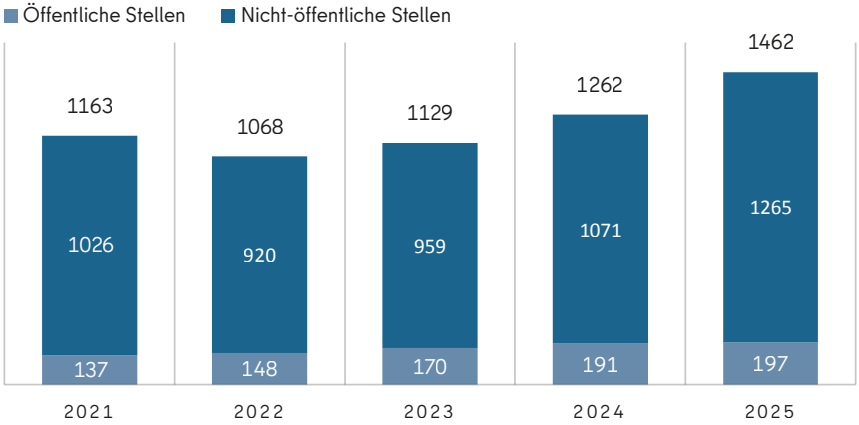
Beschwerden



2. Meldung von Datenschutzvorfällen

Datenschutzvorfälle sind Verletzungen des Schutzes personenbezogener Daten, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten führen. Verantwortliche in unserem Zuständigkeitsbereich sind grundsätzlich verpflichtet, einen Datenschutzvorfall innerhalb von 72 Stunden bei unserer Behörde zu melden. In diesem Jahr stieg die Gesamtanzahl der gemeldeten Datenschutzvorfälle im Vergleich zum Vorjahr erneut an. Während im Jahr 2024 insgesamt 1.262 Meldungen erfasst wurden, erhöhte sich diese Zahl in diesem Jahr auf 1.462. Öffentliche Stellen meldeten uns in diesem Jahr 197 Datenschutzvorfälle (Vorjahr: 191). Ebenso stieg die Anzahl der Meldungen von nicht-öffentlichen Stellen von 1.071 im Jahr 2024 auf 1.265 im Jahr 2025.

Meldungen von Datenschutzvorfällen



3. Anträge und Beschwerden nach dem Informationsfreiheitsgesetz

Nach dem Rekordjahr 2024 haben sich die bei uns eingegangenen Anträge auf Aktenauskunft bzw. Akteneinsicht nach dem Berliner Informationsfreiheitsgesetz (IFG) in diesem Jahr wieder an das Niveau des Jahres 2023 angeglichen. Insgesamt erhielten wir 38 Anträge, u. a. auf Informationen zu Datenschutzvorfällen, Datenschutzbeschwerden sowie Prüf- und Gesetzgebungsverfahren. Bei zehn Anfragen erteilten wir Auskunft oder Teilauskunft bzw. Akteneinsicht oder Teilakteneinsicht. In fünf Fällen lehnten wir die Auskunftserteilung ab, u. a. aufgrund des Schutzes personenbezogener Daten der Beschwerdeführenden. In 18 Fällen waren die angefragten Informationen entweder bei uns nicht vorhanden, die Anträge wurden nicht weiterverfolgt oder wir waren für die Beantwortung der Anfrage nicht zuständig. Schließlich konnten in fünf Fällen die Verfahren insbesondere aufgrund von umfangreichen Drittbeteiligungsverfahren noch nicht abgeschlossen werden.

Wir erhielten zudem 91 Eingaben, mit denen Bürger:innen uns gebeten haben, darauf hinzuwirken, dass ihre Anträge auf Aktenauskunft bzw. Akteneinsicht auf der Grundlage des IFG bei Einrichtungen im Land Berlin ordnungsgemäß bearbeitet werden. Im Vergleich zum Vorjahr (99 Beschwerden) bedeutet dies einen leichten Rückgang.

4. Europäische Verfahren

Die DSGVO sieht vor, dass in Fällen grenzüberschreitender Datenverarbeitung eine europaweite Zusammenarbeit der Aufsichtsbehörden 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 Aufsichtsbehörden melden, wenn eine Beschwerde vorliegt, die Verantwortlichen eine Niederlassung in ihrem Land haben oder die Datenverarbeitung erhebliche Auswirkungen auf die Bürger:innen ihres jeweiligen Landes hat.

In diesem Jahr wurden wir in fünf Verfahren als federführende Aufsichtsbehörde bestimmt. Eine Betroffenheit aufgrund bei uns eingegangener Beschwerden ergab sich in 161 Fällen. In zwei Verfahren erließen wir einen Beschlussentwurf bzw. einen endgültigen Beschluss.

Europäische Verfahren mit unserer Beteiligung 2025

Verfahren nach Art. 56 DSGVO (betroffen)	161
Verfahren nach Art. 56 DSGVO (federführend)	5
Verfahren nach Art. 60 ff. DSGVO (federführend)	2

5. Abhilfemaßnahmen

Stellen wir einen Verstoß von Verantwortlichen gegen die datenschutzrechtlichen Bestimmungen fest, können wir verschiedene Abhilfemaßnahmen ergreifen.[328] In diesem Jahr haben wir 53 Verwarnungen und eine Warnung ausgesprochen sowie 18 Bußgeldbescheide mit 59 Bußgeldern in Höhe von insgesamt 79.450 Euro erlassen. Die entsprechenden Verfahren waren bis Ende des Jahres jedoch noch nicht alle rechtskräftig abgeschlossen. Zudem sind 13 Zwangsgeldbescheide ergangen. In einem Fall haben wir einen Strafantrag gestellt. Über das Jahr verteilt wurden 107 Bußgeldverfahren eingestellt und 105 Verfahren neu eröffnet.

328 Siehe insbesondere Art. 58 Abs. 2 DSGVO.

Abhilfemaßnahmen 2025

Warnungen	1
Verwarnungen	53
Anweisungen und Anordnungen	0
Geldbußen	59

II. Abkürzungen

Abghs.-Drs.	Abgeordnetenhaus-Drucksache
Abs.	Absatz
AG	Arbeitsgruppe/Arbeitsgemeinschaft, Amtsgericht
AIG	Akteneinsichts- und Informationszugangsgesetz
AK	Arbeitskreis
Alt.	Alternative
AO	Abgabenordnung
ASOG	Allgemeines Sicherheits- und Ordnungsgesetz Berlin
AufenthG	Aufenthaltsgesetz
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BBBG	Gesetz über die Anstalt öffentlichen Rechts Berliner Bäder-Betriebe (Bäder-Anstaltsgesetz)
BDSG	Bundesdatenschutzgesetz
beA	besonderes elektronisches Anwaltspostfach
BfDI	Bundesbeauftragte für Datenschutz und Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BKartA	Bundeskartellamt
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BlnDSG	Berliner Datenschutzgesetz
BMG	Bundesmeldegesetz
BORA	Berufsordnung für Rechtsanwälte
BRAO	Bundesrechtsanwaltsordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVG	Berliner Verkehrsbetriebe
BVV	Bezirksverordnetenversammlung
BVwG	Bundesverwaltungsgericht der Republik Österreich
bzw.	beziehungsweise

ca.	circa
CEH ESG	Compliance, eGovernment and Health Expert Subgroup
CNIL	Commission Nationale de l'Informatique et des Libertés
CoC	Code of Conduct
CT	Computertomografie
d. h.	das heißt
DigLLV	Digitale Lehr- und Lernmittelverordnung
DSA	Digital Services Act
DSB	Datenschutzbeauftragte:r
DSC	Digital Services Coordinator
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz)
eAT	elektronischer Aufenthaltstitel
ebd.	ebenda
EDSA	Europäischer Datenschutzausschuss
EfA	Einer für alle
EGovG Bln	E-Government-Gesetz Berlin
ENTRI	European Network for Transparency and Right to Information
EPC	European Payment Council
ErwGr.	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
EZB	Europäische Zentralbank
FAER	Fahreignungsregister
FamFG	Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit
FITKO	Föderale IT-Kooperation
FWU	Institut für Film und Bild in Wissenschaft und Unterricht
GDV	Gesamtverband der Deutschen Versicherungswirtschaft e. V.
gem.	gemäß
GFK	Genfer Flüchtlingskonvention
GG	Grundgesetz

ggf.	gegebenenfalls
HGB	Handelsgesetzbuch
Hs.	Halbsatz
IBAN	International Bank Account Number
ICO	Information Commissioner‘s Office
i. d. R.	in der Regel
IP	Internet Protocol
i. S. d.	im Sinne des
i. V. m.	in Verbindung mit
ICIC	International Conference of Information Commissioners
IFG	Berliner Informationsfreiheitsgesetz
IFG Bund	Informationsfreiheitsgesetz des Bundes
IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
IKT	Informations- und Kommunikationstechnologie
IT	Informationstechnik
ITDZ	IT-Dienstleistungszentrum Berlin
IWGDPT	International Working Group on Data Protection in Technology
JAG	Berliner Juristenausbildungsgesetz
JB	Jahresbericht
JCAS	Joint Communication and Sensing
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
Kap.	Kapitel
KI	Künstliche Intelligenz
LABO	Landesamt für Bürger- und Ordnungsangelegenheiten
LEA	Landesamt für Einwanderung
LG	Landgericht
lit.	littera (Buchstabe)
LLM	Large Language Model (Sprachmodell)
LMÜTranspG	Lebensmittelüberwachungstransparenzgesetz
LOG	Landesorganisationsgesetz
LUSD	Lehrkräfte-Unterrichts-Schul-Datenbank

MRiDaVG	Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden
NRO	Nichtregierungsorganisation
OCR	Optical Character Recognition
o. g.	oben genannt
OH	Orientierungshilfe
OLG	Oberlandesgericht
OpenDataV	Open Data Verordnung
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
OZG	Onlinezugangsgesetz
PersVG Bln	Personalvertretungsgesetz Berlin
POLIKS	Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung
PWC	PricewaterhouseCoopers
PWTG	Politische-Werbung-Transparenz-Gesetz
RAG	Retrieval-Augmented Generation
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
Rn.	Randnummer
SchuldatenV	Schuldatenverordnung
SchulG	Schulgesetz
SDM	Standard-Datenschutzmodell
SenASGIVA	Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung
SenInnSport	Senatsverwaltung für Inneres und Sport
sog.	sogenannt
SPE	Support Pool of Experts
StGB	Strafgesetzbuch
StVG	Straßenverkehrsgesetz
TFA	Technisches Finanzamt
TTPW-VO	Verordnung über die Transparenz und das Targeting politischer Werbung
u. a.	unter anderem
UAG	Unterarbeitsgruppe
UAK	Unterarbeitskreis

u. U.	unter Umständen
UIG	Umweltinformationsgesetz
UKlaG	Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen
URL	Uniform Resource Locator
Var.	Variante
VG	Verwaltungsgericht
VGebO	Verwaltungsgebührenordnung
VIG	Verbraucherinformationsgesetz
VoP	Verification of Payee
VSG Bln	Verfassungsschutzgesetz Berlin
VVO	Verordnung über zusätzliche Verfahrensregeln für die Durchsetzung der DSGVO
VwVfG	Verwaltungsverfahrensgesetz
WÜD	Wiener Übereinkommen über diplomatische Beziehungen
XR	Extended Reality
z. B.	zum Beispiel
Ziff.	Ziffer
ZPO	Zivilprozessordnung

www.datenschutz-berlin.de

BERLIN