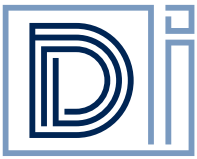


Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Datenschutz und Informationsfreiheit

Jahresbericht 2022

Jahresbericht

der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2022

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 2021 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2022 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 GbR

Satz: werk & satz.

Druck: Spree Druck Berlin GmbH

Inhalt

16 Informationsfreiheit

17 Aus der Dienststelle

18 Statistik

Abkürzungsverzeichnis

Abghs.-Drs.	Drucksache des Abgeordnetenhauses
ADHGB	Allgemeines Deutsches Handelsgesetzbuch
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
ArbGG	Arbeitsgerichtsgesetz
ASOG Bln	Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin
AsylG	Asylgesetz
AufenthG	Aufenthaltsgesetz
AVV	Allgemeine Verwaltungsvorschrift
BAMF	Bundesamt für Migration und Flüchtlinge
BDSG	Bundesdatenschutzgesetz
BerlHG	Berliner Hochschulgesetz
BerlSenG	Berliner Seniorenmitwirkungsgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BfJ	Bundesamt für Justiz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BlnDSG	Berliner Datenschutzgesetz
BLUSD	Berliner Lehrkräfte-Unterrichts-Schul-Datenbank
BMG	Bundesmeldegesetz
BMI	Bundesministerium des Innern und für Heimat
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVG	Berliner Verkehrsbetriebe

BZRG	Bundeszentralregistergesetz
BZSt	Bundeszentralamt für Steuern
DAB	Digital Audio Broadcasting
DiDat	Ausschuss für Digitalisierung und Datenschutz
DigiBitS	Digitale Bildung trifft Schule
DPC	Irische Datenschutzaufsichtsbehörde
DRiG	Deutsches Richtergesetz
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichts-behörden des Bundes und der Länder
EDSA	Europäischer Datenschutzausschuss
EG	Erwägungsgrund
EGovG Bln	E-Government-Gesetz Berlin
EHW	Ermittlungsunterstützender Hinweis
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
FITKO	Föderale IT-Kooperation
FormAnpassG	Gesetz zur Anpassung der Formanforderungen im Berliner Landesrecht
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GPA	Global Privacy Assembly
GVBl.	Gesetz- und Verordnungsblatt
HGB	Handelsgesetzbuch
HRV	Handelsregisterverordnung
HU	Humboldt-Universität zu Berlin
IFG	Berliner Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
IKT	Informations- und Kommunikationstechnik

IMI	Binnenmarkt-Informationssystem
IP	Internetprotokoll
IT	Informationstechnologie
ITDZ	IT-Dienstleistungszentrum Berlin
JB	Jahresbericht
JI-Richtlinie	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates
JuHiS	Jugendhilfe im Strafverfahren
KG	Kammergericht
KUL	KinderUni Lichtenberg
LABO	Landesamt für Bürger- und Ordnungsangelegenheiten
LAGeSo	Landesamt für Gesundheit und Soziales
LDA	Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg
LEA	Landesamt für Einwanderung
LG	Landgericht
LKA	Landeskriminalamt
LKG	Landeskrankenhausgesetz
LMÜTranspG	Lebensmittelüberwachungstransparenzgesetz
LMÜTranspG-DVO	Lebensmittelüberwachungstransparenzgesetz-durchführungsverordnung
LUSD	Lehrkräfte-Unterrichts-Schul-Datenbank
LVwA	Landesverwaltungsamt
MDM	Mobile Device Management
MiStrA	Anordnung über Mitteilungen in Strafsachen
MStV	Medienstaatsvertrag
ÖPNV	Öffentlicher Personennahverkehr
OLMERA	Onlinemelderegisterauskunft
OVG	Oberverwaltungsgericht

OWASP	Open Web Application Security Project
OZG	Onlinezugangsgesetz
PDV	Polizeidienstvorschrift
POLIKS	Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung
RBB	Rundfunk Berlin-Brandenburg
RegVBG	Registerverfahrensbeschleunigungsgesetz
SCC	Standardvertragsklauseln
SchulG	Schulgesetz für das Land Berlin
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SUrlV	Sonderurlaubsverordnung
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UIG	Umweltinformationsgesetz
UKW	Ultrakurzwelle
UrhG	Urheberrechtsgesetz
VG	Verwaltungsgericht
VIG	Verbraucherinformationsgesetz
VS	Verschlusssache
WEG	Gesetz über das Wohnungseigentum und das Dauerwohnrecht
WPD	Wissenschaftlicher Parlamentsdienst
ZensG	Zensusgesetz
ZensusAGBln	Zensusausführungsgesetz Berlin
ZensVorbG	Zensusvorbereitungsgesetz
ZPO	Zivilprozessordnung
ZustKat Ord	Zuständigkeitskatalog Ordnungsaufgaben

Vorwort

Am 6. Oktober dieses Jahres wurde ich vom Abgeordnetenhaus für die Dauer von fünf Jahren zur Berliner Beauftragten für Datenschutz und Informationsfreiheit gewählt. Ich freue mich sehr auf die neue Aufgabe und bin dankbar, diesen Weg mit hochqualifizierten Expert:innen an meiner Seite beschreiten zu dürfen. Ihr unermüdlicher und engagierter Einsatz für den Datenschutz und die Informationsfreiheit bildet die Grundlage für diesen Jahresbericht.

Nach wie vor warten wir auf die Verabschiedung eines modernen Transparenzgesetzes für Berlin. Stellt die Verwaltung proaktiv diejenigen Informationen zur Verfügung, die Grundlage für administratives Handeln und politische Entscheidungen sind, ermöglicht sie die zeitnahe Auseinandersetzung und Nachvollziehbarkeit der Entscheidungen. Letztlich profitiert auch die Verwaltung selbst von der Veröffentlichung, indem sie von anderen Behörden benötigte Informationen über ein Transparenzportal auf dem kurzen Dienstweg erhält. Ein solches Portal setzt voraus, dass Verwaltungsinformationen elektronisch verfügbar sind und ohne Medienbruch aus digitalisierten Verfahren bereitgestellt werden können. Auch vor diesem Hintergrund ist es wichtig, dass die Digitalisierung der Berliner Verwaltung weiter Fahrt aufnimmt. Mit der gleichzeitigen Fortentwicklung des Onlinezugangsgesetzes werden hoffentlich immer mehr Verwaltungsleistungen digital zur Verfügung gestellt. Zugleich müssen die fehlenden datenschutzrechtlichen Grundlagen ergänzt und die Verantwortlichkeiten klar und eindeutig abgebildet werden. Es muss stets transparent bleiben, was genau bei der Inanspruchnahme digitaler Verwaltungsleistungen mit personenbezogenen Daten passiert und wer für was verantwortlich ist. Denn das Vertrauen der Menschen ist ausschlaggebend für die Akzeptanz der Verfahren.

Bei der Kontrolle der Datenverarbeitung von Polizei und Staatsanwaltschaft stoßen wir auf rechtliche Hindernisse, da es im Berliner Landesrecht weiterhin an der Umsetzung der europarechtlich vorgesehenen effektiven Durchsetzungsinstrumente für unsere Behörde fehlt. Der Druck aus Brüssel wächst, hat doch die EU-Kommission die fehlenden Befugnisse zum Anlass genommen, gegen Deutschland ein Vertragsverletzungsverfahren einzuleiten.

Unsere Aufgabe ist es, Grundrechte zu schützen und die Menschen dabei zu unterstützen, von Digitalisierung und Technikeinsatz zu profitieren, ohne dabei auf Selbstbestimmung, Anonymität, freie Informationsbeschaffung und Meinungsbildung sowie sonstige unbeobachtete Freiräume der Entfaltung zu verzichten. Für die heranwachsenden Generationen und damit für den Bildungs- und Schulbereich ist dies von besonderer Bedeutung: Wir müssen Kinder und Jugendliche befähigen, sich diese Freiräume auch in der Zukunft zu erhalten. Gleichzeitig sollen sie unter Einsatz digitaler Lernmittel und im digitalen Unterricht unbeobachtet lernen können. Genau diese Maßstäbe gilt es bei der Beschaffung digitaler Endgeräte und der Fortentwicklung der Rechtsgrundlagen im Schulbereich sowie des Berliner Schulportals einzuhalten.

Auch im Bereich der Wirtschaft und der Internetökonomie helfen die Anforderungen des Datenschutzes, Entscheidungsfreiräume, Interventionsmöglichkeiten und Kommunikationsvielfalt zu bewahren. Mit dem Digitalpaket und der Datenstrategie der Europäischen Union sowie der geplanten Regulierung des politischen Targetings stehen neue rechtliche Entwicklungen bevor, die unsere Arbeit mitbestimmen werden. Das Wirken unserer Behörde wird auch in Zukunft an der ihr zugewiesenen rechtsstaatserhaltenden und grundrechtsschützenden Funktion ausgerichtet sein. Ich freue mich auf die Entwicklungen in diesem hochdynamischen Tätigkeitsbereich.

Eine aufschlussreiche Lektüre wünscht Ihnen

Meike Kamp
Berliner Beauftragte für Datenschutz und Informationsfreiheit

1 Digitale Verwaltung

1.1 Stand der Digitalisierungsprojekte – Das Problem liegt im Detail

Berlin hat im Bereich der Verwaltungsdigitalisierung nach wie vor erheblichen Aufholbedarf. In einigen Bereichen hat der Senat begonnen, zentrale Bausteine einer digitalen Verwaltung zu realisieren. Die konkrete Umsetzung ist mit vielen technischen Herausforderungen verbunden und wirft zahlreiche Datenschutzfragen auf, mit denen wir uns in diesem Jahr intensiv beschäftigt haben.

Mittlerweile können Behörden wichtige Verwaltungsleistungen auch sehr kurzfristig über einen digitalen Antrag zur Verfügung stellen. Darüber hinaus beginnt für Teile der ca. 120.000 Verwaltungsmitarbeiter:innen der Abschied von der Papierakte. Das Bezirksamt Mitte führt derzeit bspw. im Rahmen eines Pilotprojekts den IKT-Basisdienst „Digitale Akte“ ein.[1] Im Zuge unserer Beratungen zur Einführung der digitalen Akte[2] haben wir die IKT-Steuerung bei der Senatsverwaltung für Inneres, Digitalisierung und Sport, die den IKT-Basisdienst „Digitale Akte“ zur Verfügung stellt, dabei unterstützt, ein Rahmendatenschutzkonzept zu entwickeln. Dieses dient nun den Fachbehörden als Grundlage für eine datenschutzkonforme Einführung der digitalen Akte.

In diesem Zusammenhang haben wir auch das Sozialamt Mitte bei der Erstellung des Datenschutzkonzepts und der Datenschutz-Folgenabschätzung beraten. Die dabei entstandenen Dokumente sollen nun auch in den Sozialämtern der anderen Bezirke Verwendung finden. Nach gleichem Muster werden wir weitere Fachämter und Servicestellen von Bezirksämtern dabei unterstützen, datenschutzrechtliche Dokumentationen zur digitalen Akte zu erstellen, die dann von anderen Behörden „nachgenutzt“ werden

1 Die Senatsverwaltung für Inneres, Digitalisierung und Sport stellt der Verwaltung fachübergreifend die wichtigsten internen und externen Komponenten zur Erbringung der E-Government-Angebote als sog. IKT-Basisdienste (Basisdienste der Informations- und Kommunikationstechnik) zur Verfügung (siehe § 10 Abs. 2 Satz 3 E-Government-Gesetz Berlin (EGovG Bln) und § 24 Abs. 2 Satz 1 EGovG Bln), z. B. in Form der „Digitalen Akte“ und des „Digitalen Antrags“.

2 Siehe JB 2021, 2.1.

können. Insgesamt kann so eine erhebliche Reduzierung des Aufwands für die einzelnen Fachbehörden erzielt werden, die die digitale Akte einführen. Dies soll Vorbild für die zukünftige Einführung weiterer IKT-Basisdienste sein.

Als einen besonderen Erfolg der Verwaltungsdigitalisierung hat der Senat im März den Start des digitalen Verfahrens zur Beantragung eines Aufenthaltstitels für ukrainische Geflüchtete beim Landesamt für Einwanderung (LEA) verbucht. Dieses Verfahren beruht auf dem IKT-Basisdienst „Digitaler Antrag“.[3] Der Verwaltung steht damit ein effektives Werkzeug zur kurzfristigen Bewältigung großer Antragsaufkommen zur Verfügung. Allerdings sind hier noch datenschutzrechtliche Grundsatzfragen zu klären. So entsprachen die datenschutzrechtlichen Informationen, die den Nutzenden beim digitalen Antrag bereit gestellt wurden, nicht den Vorgaben der Datenschutz-Grundverordnung (DSGVO): Aus der Datenschutzerklärung ging nicht hervor, welche Behörde die personenbezogenen Daten der Betroffenen auf welche Weise verarbeitet. Es wurde pauschal auf eine gemeinsame Verantwortlichkeit[4] zwischen der IKT-Steuerung, die den Dienst zur Verfügung stellt, und dem LEA verwiesen, obwohl die IKT-Steuerung die personenbezogenen Daten der antragstellenden Geflüchteten mangels rechtlicher Grundlage gar nicht verarbeiten dürfte. Vor diesem Hintergrund unterstützen wir die beteiligten Stellen nun dabei, die Informationen und Dokumentationen zum digitalen Antrag entsprechend anzupassen.

Es ist wichtig, dass bei der Nutzung digitaler Verwaltungsleistungen für die Betroffenen stets transparent bleibt, welche der zahlreichen einbezogenen öffentlichen und privaten Stellen ihre personenbezogenen Daten auf welcher Grundlage verarbeiten und wer die richtige Ansprechperson für die Erfüllung ihrer Betroffenenrechte aus der DSGVO ist.[5] Nur mit eindeutigen Verantwortungsstrukturen und größtmöglicher Transparenz im Hinblick auf den Umgang mit personenbezogenen Daten wird die Verwaltung das Vertrauen der Bürger:innen in die Digitalisierung gewinnen können.

3 Siehe JB 2020, 2.1.
4 I. S. v. Art. 26 DSGVO.
5 Siehe z. B. Art. 15 DSGVO (Recht auf Auskunft) und Art. 17 DSGVO (Recht auf Löschung).

1.2 Umsetzung des Onlinezugangsgesetzes in Bund und Ländern – Wann platzt der Knoten?

Mit der notwendigen Anpassung des Onlinezugangsgesetzes (OZG) müssen die erforderlichen datenschutzrechtlichen Grundlagen geschaffen werden, die in der bisherigen Fassung des OZG aus dem Jahr 2017 fehlen.

Bereits seit längerem ist absehbar, dass Bund und Länder ihren mit dem OZG festgelegten Zeitplan, die wichtigsten 575 Verwaltungsleistungen bis Ende dieses Jahres für die Bürger:innen digital über Verwaltungsportale verfügbar zu machen,[6] nicht einhalten können. Vor diesem Hintergrund plant das federführende Bundesministerium des Innern und für Heimat (BMI) im Rahmen des im Februar als „OZG 2.0" vorgestellten Projekts, das OZG anzupassen, um die Weichen für eine kurzfristige Beschleunigung der OZG-Umsetzung zu stellen.

Bereits im Herbst 2020 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Unterarbeitsgruppe eingerichtet, die sich mit den datenschutzrechtlichen Fragen im Zusammenhang mit der OZG-Umsetzung befasst und dazu einen fortlaufenden Beratungs- und Abstimmungsprozess mit dem BMI und der Föderalen IT-Kooperation (FITKO) führt.[7] Mit Blick auf das aktuelle Gesetzgebungsverfahren zum OZG hat die DSK die Unterarbeitsgruppe Ende 2021 in die Kontaktgruppe „OZG 2.0" umgewandelt. Wir haben den Vorsitz übernommen und koordinieren die Beratungen mit dem BMI. Es freut uns, dass die zuständige Fachabteilung des BMI auch aufgrund unserer intensiven Beratung die aus Sicht des Datenschutzes wichtigsten Regelungsvorhaben aufgegriffen hat. Die weitere Verzögerung des Gesetzgebungsverfahrens stellt ein erhebliches Problem dar: Ohne entsprechende Anpassungen kann eine datenschutzkonforme Umsetzung des OZG angesichts fehlender Rechtsgrundlagen für die Datenverarbeitung nicht gewährleistet werden. Vor diesem Hintergrund muss das Verfahren nun unmittelbar zum Abschluss gebracht werden.

6 Siehe JB 2020, 2.2; JB 2021, 2.3.
7 Siehe JB 2021, 2.3.

Mit der Anpassung des OZG soll bei der Verwaltungsdigitalisierung in Deutschland endlich der Knoten platzen. Als Voraussetzung dafür müssen ohne weitere Verzögerungen auch die bisher noch fehlenden Regelungen zum Datenschutz umgesetzt werden.

2 Inneres und Sport

2.1 Wachsender Druck aus Brüssel – Keine wirksamen Durchsetzungsbefugnisse bei Polizei und Staatsanwaltschaft

In der Vergangenheit hat unsere Behörde in Berlin und Brüssel immer wieder darauf hingewiesen, dass wichtige europäische Vorgaben im Bereich der Kontrolle von Behörden, die für die Verhütung und Verfolgung von Straftaten sowie für die Strafvollstreckung zuständig sind, nicht in Berliner Landesrecht umgesetzt worden sind. Nun erhalten wir in dieser Frage Unterstützung von der Europäischen Kommission, die ein förmliches Vertragsverletzungsverfahren gegen Deutschland eingeleitet hat.

Die Europäische Kommission kann ein Vertragsverletzungsverfahren einleiten, wenn ein Mitgliedstaat der Europäischen Union (EU) einen mutmaßlichen Verstoß gegen EU-Recht nicht behebt. Vorliegend geht es um die mangelhafte Umsetzung der sog. JI-Richtlinie [8], die die Verarbeitung personenbezogener Daten durch Behörden zur Verhütung und Verfolgung von Straftaten sowie zur Strafvollstreckung unionsweit einheitlich regelt.

Behörden sind, wenn sie Daten zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung verarbeiten, vom Geltungsbereich der unmittelbar anwendbaren Datenschutz-Grundverordnung (DSGVO) ausgenommen.[9] Für Polizei, Staatsanwaltschaften, Strafgerichte und den Strafvollzug sollen die Vorgaben der JI-Richtlinie gelten, die – anders als die unmittelbar anwendbare DSGVO – in nationales Recht umgesetzt werden muss. Das soll den Mitgliedstaaten einerseits größere Freiheiten in Einzelfragen einräumen, birgt aber andererseits die Gefahr, dass EU-Recht uneinheitlich und weniger effektiv umgesetzt wird. So auch in Berlin: Die Befugnisse unserer Behörde beschränken sich nach der einschlägigen Landesgesetz

8 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.

9 Art. 2 Abs. 2 lit. d DSGVO.

gebung darauf, über beanstandete Verarbeitungsvorgänge von Behörden, die für die Verhütung und Verfolgung von Straftaten sowie für die Strafvollstreckung zuständig sind, nach einem obligatorischen Einigungsversuch dem zuständigen Ausschuss des Abgeordnetenhauses zu berichten.[10] So droht die Aufsichtsarbeit unserer Behörde stets nur rein politisch verhandelt zu werden, ohne durchsetzbar und justiziabel zu sein.

Die JI-Richtlinie aus dem Jahr 2016, deren Vorgaben bis Mai 2018 vollständig in nationales Recht hätten umgesetzt werden müssen, sieht dazu bspw. vor, dass die Aufsichtsbehörde eine verantwortliche Stelle oder einen Auftragsverarbeiter direkt anweisen können muss, Verarbeitungsvorgänge mit den entsprechenden Vorschriften in Einklang zu bringen. Dies kann insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Datenverarbeitung erfolgen.[11] Wichtig ist laut JI-Richtlinie, dass die Abhilfebefugnisse wirksam sind. Die Abhilfebefugnisse müssen sich direkt gegen die verantwortliche Stelle richten können und dürfen nicht von weiteren Bedingungen abhängig sein, wie etwa von der Erheblichkeit eines Verstoßes oder von einer vorherigen Beanstandung.

Diese europäischen Vorgaben sind bis heute auf Bundes- und Landesebene nur teilweise umgesetzt. Die Europäische Kommission hat deswegen nun ein förmliches Vertragsverletzungsverfahren eingeleitet, das an die Bundesrepublik Deutschland als Mitgliedstaat der EU adressiert ist, aber auch die Versäumnisse des Berliner Landesgesetzgebers aufgreift und mit deutlichen Worten als unzureichend kennzeichnet. Die Kommission betont dabei, dass die gern zitierte Erwartung, Behörden würden sich im Zweifel rechtskonform verhalten, keine wirksame Maßnahme im Sinne der JI-Richtlinie darstellt. Sollten die Vorgaben nicht umgesetzt werden, wird die Kommission am Ende entscheiden müssen, ob sie diese Versäumnisse vor den Europäischen Gerichtshof (EuGH) bringt.[12]

Die Notwendigkeit einer wirksamen Anordnungsbefugnis auch im Bereich der Verhütung von Straftaten sowie der Strafverfolgung und -vollstreckung haben wir in Beratungen und Stellungnahmen gegenüber dem Abgeordnetenhaus immer wieder angemahnt. Gerade in diesen Bereichen sind die Grundrechtseingriffe gegenüber

10 Siehe § 13 Abs. 2, 3 Berliner Datenschutzgesetz (BlnDSG).
11 Art. 47 Abs. 2 JI-Richtlinie.
12 Siehe Art. 258 Vertrag über die Arbeitsweise der Europäischen Union (AEUV).

betroffenen Personen im Allgemeinen oft besonders empfindlich oder besonders zahlreich. Die Gesetzgeber von Bundes- und Landesebenen wären gut beraten, es in dieser wichtigen Frage nicht auf einen Konflikt mit Brüssel ankommen zu lassen. Je genauer die Umsetzung der JI-Richtlinie von dort in den Blick genommen wird, desto enger wird letztlich auch der Bewegungsspielraum in der Umsetzung.

2.2 Was lange währt, währt immer noch – Überlange Bearbeitungszeiten bei Selbstauskünften durch die Polizei

Immer wieder erreichen uns Beschwerden von Bürger:innen, dass die Auskunftsverfahren bei der Polizei zu lange dauern. Auch weil sich der Landesgesetzgeber dagegen entschieden hat, für Selbstauskünfte in diesem Bereich eine zwingende Frist festzuschreiben, ist die Durchsetzung wichtiger Rechte der Bürger:innen beeinträchtigt.

Die Datenverarbeitung durch die Polizei unterliegt in weiten Teilen nicht den Vorschriften der DSGVO,[13] sodass dort auch die sonst übliche Monatsfrist für Auskünfte über die Verarbeitung personenbezogener Daten von Betroffenen aus Art. 15 Abs. 3 DSGVO keine Anwendung findet. Zwar sieht die stattdessen einschlägige JI-Richtlinie vor, dass das Recht auf Auskunft „problemlos“ geltend gemacht werden können soll.[14] Dies hätte etwa durch eine verbindliche Frist für die Auskunftserteilung abgesichert werden können, doch der Gesetzgeber hat bei der Umsetzung der Richtlinie in Landesrecht leider keine Frist vorgesehen.[15]

Eine zügige Bearbeitungsdauer ist für die wirksame Durchsetzung von Betroffenenrechten unabdingbar: Nur mit dem Wissen, welche Daten im Einzelnen verarbeitet werden, können Bürger:innen entscheiden, ob sie sich gegen solche Maßnahmen zur Wehr setzen möchten. Gerade dort, wo personenbezogene Daten ohne Wissen der Betroffenen oder gegen ihren Willen verarbeitet werden, muss der oder dem Einzelnen eine effektive Kontrolle möglich sein. Auch die Berichtigung der verarbeiteten Daten kann nur fordern, wer die Unrichtigkeit überhaupt kennt. Die Erfahrung aus der Beschwerde

13 Siehe Art. 2 Abs. 2 lit. d DSGVO.
14 Erwägungsgrund (EG) 43 Satz 1 JI-Richtlinie.
15 Siehe §§ 43, 45 BlnDSG.

praxis zeigt, dass zeitnahe Antworten an Betroffene dazu beitragen, über Transparenz Vertrauen herzustellen und so entsprechende Sorgen zu nehmen. Bereits im Frühjahr 2019 haben wir dieses Thema gegenüber der Polizeipräsidentin angesprochen.[16] Nach erneuter Stellungnahme der Polizei zu dieser Frage bestehen bei etwa einem Viertel der Datenauskunfts- und Löschanträge noch Bearbeitungsrückstände von sieben bis acht Monaten, der Rest würde früher beschieden. Wir hoffen, dass hier durch bereits erfolgte und angekündigte Neueinstellungen weitere Besserung eintritt.

Die Rechte auf Auskunft über die Speicherung personenbezogener Daten und auf Löschung dieser Daten sind wesentliche Betroffenenrechte. Als wichtiger Bestandteil des Selbstdatenschutzes stellen sie einen Kernbestandteil des informationellen Selbstbestimmungsrechts dar. Die effektive Umsetzung muss gewährleistet sein, insbesondere dürfen nicht überlange Bearbeitungszeiten den Charakter der Anträge als Kontrollinstrumente konterkarieren. Insofern empfehlen wir dringend, mit der Einführung einer gesetzlichen Frist zur Auskunftserteilung einen Gleichlauf zu den Vorgaben der DSGVO herzustellen.

2.3 Datenspeicherung zu Kindern und Jugendlichen im Umfeld des organisierten Verbrechens

Gegen strafunmündige Kinder dürfen keine strafrechtlichen Ermittlungsverfahren geführt werden. Dennoch kann es unter bestimmten Voraussetzungen erforderlich sein, dass seitens der Polizei entsprechende Daten zu strafrechtlich relevanten Vorfällen zum Zwecke der Gefahrenabwehr verarbeitet werden.

Aus den Reihen des Abgeordnetenhauses wurden wir auf eine parlamentarische Anfrage zu polizeilichen Maßnahmen in Bezug auf „Verbundeinsätze, ‚Clankriminalität' und Gewerbeüberwachung"[17] aufmerksam gemacht, hier insbesondere hinsichtlich der Speicherung personenbezogener Daten von Tatverdächtigen. Aus der Antwort der Senatsverwaltung für Inneres, Digitalisierung und Sport ergibt sich, dass die Polizei in ihrem Dateisystem POLIKS insgesamt 19 minderjährige Personen mit dem ermittlungs

16 Siehe JB 2019, 3.3.
17 Schriftliche Anfrage vom 25. Februar 2022, Abghs.-Drs. 19/11121.

unterstützenden Hinweis (EHW) „Clankriminalität“ gespeichert hat. Von diesen waren zum Berichtszeitpunkt vier Betroffene noch keine 14 Jahre alt und damit strafunmündig.[18]

Ermittlungsunterstützende Hinweise sollen dazu beitragen, polizeiliches Handeln zielgerichtet zu steuern, und dienen damit der gesetzlichen Aufgabenerfüllung sowie idealerweise dem Schutz der Betroffenen und der eingesetzten Polizeibediensteten. Laut Antwort der Senatsverwaltung vom März 2022 waren dem EHW „Clankriminalität“ in POLIKS 425 Personen zugeordnet;[19] im Sommer 2020 waren dies noch 154 Personen.[20] In vergleichbarem Ausmaß stieg die Anzahl der Betroffenen, die in POLIKS unter dem EHW „Clankriminalität Umfeld“ gespeichert worden waren: Im Sommer 2020 waren dies lediglich 14 Personen,[21] im März 2022 bereits 87 Personen.[22]

Unter „Clankriminalität“ versteht das Bundeskriminalamt (BKA) nach dem Bundeslagebild 2020 „die Begehung von Straftaten durch Angehörige ethnisch abgeschotteter Subkulturen. Sie ist geprägt von verwandtschaftlichen Beziehungen, einer gemeinsamen ethnischen Herkunft und einem hohen Maß an Abschottung der Täter, wodurch die Tatbegehung gefördert oder die Aufklärung der Tat erschwert wird. Dies geht einher mit einer eigenen Werteordnung und der prinzipiellen Ablehnung der deutschen Rechtsordnung.“[23] Der Begriff ist in der kriminalpolitischen Diskussion allerdings umstritten, da die Gefahr besteht, dass bestimmten Bevölkerungsgruppen oder Familienverbänden klischeehaft kriminelles Verhalten zugeschrieben wird. Dementsprechend wird dessen Verwendung kritisiert.[24] Das BKA hat auf diese Kritik offenbar reagiert und fasst die Kriterien in seinem aktuellen Bericht sachlicher.[25]

18 Siehe § 19 Strafgesetzbuch (StGB).
19 Siehe Abghs.-Drs. 19/11121.
20 Siehe Abghs.-Drs. 18/23777.
21 Siehe Abghs.-Drs. 18/23777.
22 Siehe Abghs.-Drs. 19/11121. Rechtsgrundlage für solche Hinweise sind die §§ 18, 28, 42 ff. Allgemeines Sicherheits- und Ordnungsgesetz (ASOG Bln) i. V. m. Errichtungsanordnungen, die für jeden Hinweis gesondert abgefasst werden müssen. Die Prüf- und Löschfristen ergeben sich aus §§ 43, 48 ASOG Bln sowie aus der Verordnung über Prüffristen bei polizeilicher Datenspeicherung (Prüffristenverordnung).
23 BKA: Organisierte Kriminalität, Bundeslagebild 2020, Wiesbaden 2021, S. 24.
24 Siehe Thomas Feltes und Felix Rauls: „‚Clankriminalität‘ und die ‚German Angst‘“, in: Sozial Extra (2020), Bd. 44, S. 372 ff.
25 Siehe BKA: Organisierte Kriminalität, Bundeslagebild 2021, Wiesbaden 2022, S. 23.

Wir haben zu den Einträgen in POLIKS eine aussagekräftige Stichprobe überprüft. Dabei hat die Polizei dargelegt, dass in der Regel Sachverhalte zu den Einträgen vorlagen, in denen die Betroffenen mehrfach und gemeinschaftlich mit Familienangehörigen u. a. im Zusammenhang mit Rohheitsdelikten polizeilich in Erscheinung getreten waren. Die Gründe für die Speicherung ergaben sich direkt aus den gespeicherten Datensätzen und wurden zwar in Teilen nicht pädagogisch ausgewogen, so doch neutral wiedergegeben. Die Begründung der entsprechenden Kategorisierung erschien unter Berücksichtigung der kriminologischen Grundannahmen der Polizei folgerichtig, die Einordnung beruhte weder ausschließlich noch überwiegend auf ethnischen Merkmalen. Die Eintragungen ließen sich unter die festgelegten Merkmale fassen, die Begründung für die Aufnahme in den Datenbestand erschien in der Regel ausführlich und aufgabenorientiert.

Die Frage, inwieweit mit Blick auf die organisierte Kriminalität die Bezugnahme auf spezifische Merkmale für die erfolgreiche Ermittlungsarbeit und Gefahrenabwehr zwingend erforderlich ist, sollte sich die Polizei im Austausch mit Wissenschaft und Zivilgesellschaft immer wieder stellen. Anhaltspunkte für Verstöße konnten wir bei den kontrollierten Datensätzen allerdings nicht feststellen.

2.4 Digitales Gedankenlesen – Smartphone-Forensik durch die Ausländerbehörde

Bereits 2019 haben wir uns mit der Auswertung von Datenträgern zur Identitäts- sowie Staatsangehörigkeitsfeststellung ausreisepflichtiger Ausländer:innen durch die Ausländerbehörde[26] befasst. Damals setzte die Ausländerbehörde – anders als das Bundesamt für Migration und Flüchtlinge (BAMF) – keine spezielle Software zur Auswertung ein. Einen datenschutzrechtlichen Verstoß konnten wir seinerzeit nicht feststellen. Aufgrund neuer Erkenntnisse haben wir in diesem Jahr erneut die Prüfung der Maßnahmen der Ausländerbehörde aufgenommen.

26 Dies ist nach Nr. 36 Zuständigkeitskatalog Ordnungsaufgaben (ZustKat Ord) inzwischen das Landesamt für Einwanderung (LEA), soweit nicht die Bezirksämter gemäß Nr. 22a Abs. 2 ZustKat Ord zuständig sind.

Für die Auswertung von Datenträgern[27] von Ausländer:innen existiert eine bundesgesetzliche Vorschrift,[28] die durch das Gesetz zur Neubestimmung des Bleiberechts und der Aufenthaltsbeendigung eingeführt wurde.[29] Diese Regelung ermächtigt die zuständigen Behörden,[30] Datenträger der betroffenen bzw. zur Mitwirkung verpflichteten Ausländer:innen auszuwerten, um deren Identität und Staatsangehörigkeit festzustellen und ggf. eine Rückführungsmöglichkeit in einen anderen Staat geltend zu machen. Die Auswertung von Datenträgern steht unter den rechtlichen Zulässigkeitsvoraussetzungen, dass dies für die Feststellung der Identität und Staatsangehörigkeit der Ausländerin bzw. des Ausländers und für die Feststellung und Geltendmachung einer Rückführungsmöglichkeit in einen anderen Staat erforderlich ist und der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann.[31] Ferner darf eine solche Auswertung nur von Mitarbeitenden vorgenommen werden, die die Befähigung zum Richteramt, d. h. zwei juristische Examina,[32] besitzen.[33] Eine Auswertung von Datenträgern ist zudem stets dann unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass hierdurch allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.[34]

Aufgrund unserer Prüfung von 2019 gingen wir bislang davon aus, dass bei der Ausländerbehörde die Mobiltelefone von Ausländer:innen manuell bzw. händisch durch entsprechend den gesetzlichen Vorgaben qualifizierte Beschäftigte ausgewertet werden. Aus der Medienberichterstattung erfuhren wir in diesem Jahr, dass das zuständige Landesamt für Einwanderung (LEA) bereits seit 2020 anstelle des bisherigen manuellen Verfahrens eine Software bei der Datenträgerauswertung einsetzt, wobei die Lizenzen sowie Geräte hierfür durch die Polizei im Auftrag des Landesamts erworben worden seien. Im Rahmen unserer neuen Prüfung bestätigte sich dies. Das LEA teilte mit, dass zur Nutzung der Hard- und Software eine Servicevereinbarung mit der Polizei bzw. dem Landeskriminalamt (LKA) abgeschlossen worden sei. In der Praxis zieht die Ausländerbehörde bei Vorliegen der gesetzlichen Voraussetzungen[35] das Mobilgerät der

27 Hauptsächlich dürfte es sich dabei um Mobiltelefone, insbesondere Smartphones, handeln.
28 § 48 Abs. 3a Aufenthaltsgesetz (AufenthG).
29 Siehe Gesetz vom 27. Juli 2015, BGBl. I, S. 1386 ff.
30 Siehe § 71 AufenthG.
31 § 48 Abs. 3a Satz 1 AufenthG.
32 Siehe § 5 Abs. 1 Deutsches Richtergesetz (DRiG).
33 § 48 Abs. 3a Satz 4 AufenthG.
34 § 48 Abs. 3a Satz 2 AufenthG.
35 Siehe § 48 Abs. 3a AufenthG.

betroffenen Person ein und übersendet dieses an das LKA. Das LKA führt sodann die Datensicherung und Datenaufbereitung im Auftrag des LEA mittels der entsprechenden Software auf einem dort befindlichen Computer durch. Die aus den Mobilgeräten gewonnenen Datensätze werden anschließend auf wechselbaren Speichermedien (CD, USB-Stick o. Ä.) an das LEA übersandt und durch dessen Mitarbeitende mit einem zweiten Computer und der zugehörigen Analysesoftware eingelesen.

Im Rahmen unserer Prüfung erhielten wir zunächst keine Antwort auf unsere Fragen zu den konkret genutzten Softwareprodukten. Das wurde damit begründet, dass dies den technischen Leistungsumfang des LKA offenlegen würde und hierdurch unter Umständen entscheidende Nachteile bei der künftigen Aufklärung von Straftaten entstünden. Vor dem Hintergrund unserer gesetzlichen Verschwiegenheitspflichten, den grundsätzlich umfassenden Mitwirkungspflichten bei der Aufklärung von Datenschutzprüfungen und der Tatsache, dass wir nicht nur die zuständige Aufsichtsbehörde der Ausländerbehörde, sondern auch der Polizei sind, ist eine solche Verweigerung bei der Auskunftserteilung nicht gerechtfertigt.

Wir haben das LEA zudem darauf hingewiesen, dass aufgrund der Art der eingesetzten Software und der großen Eingriffstiefe der darauf basierenden Maßnahmen von einem hohen Risiko für die Rechte und Freiheiten der Betroffenen auszugehen ist. Betrachtet man den praktischen Einsatz von Smartphones, ist offensichtlich, dass diese Geräte inzwischen mehr als reine Kommunikationsmittel sind. Für viele Menschen stellen sie eine zentrale Schaltstelle zwischen öffentlichen und privaten Gedanken und Meinungen dar. Nicht nur lassen sich bspw. aufgrund der mit anderen Personen ausgetauschten Nachrichten Rückschlüsse auf sexuelle Orientierungen oder politische Ansichten ziehen; über Funktionen wie eine Terminverwaltung gelangen auch sehr schnell Gesundheitsdaten auf das Gerät. Nach der DSGVO sind solche Daten, die den besonderen Kategorien personenbezogener Daten zugerechnet werden, besonders geschützt und dürfen nur unter bestimmten Bedingungen verarbeitet werden.[36] Das Bundesverwaltungsgericht (BVerwG) hat zudem im Hinblick auf die in Asylverfahren bei der Regis-

36 Art. 9 DSGVO; gemäß Art. 35 Abs. 3 lit. b DSGVO ist eine Datenschutz-Folgenabschätzung u. a. erforderlich, wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO erfolgt; siehe dazu auch https://www.datenschutz-berlin.de/datenschutz/datenschutz-folgenabschaetzung.

trierung regelmäßig erfolgende Auswertung digitaler Datenträger[37] entschieden, dass diese bei Fehlen von Pässen oder Passersatzpapieren ohne hinreichende Berücksichtigung sonstiger vorliegender Erkenntnisse und Dokumente nicht rechtmäßig ist.[38] Auch vor dem Hintergrund dieser Grundsatzentscheidung dauert unsere Prüfung der Maßnahmen des LEA zur Auswertung von Datenträgern derzeit noch an. Ferner sind insbesondere Fragen zur Verantwortlichkeit und zu den ergriffenen technisch-organisatorischen Maßnahmen zu klären.

Unsere Datenschutzprüfung wird zur Klärung der noch offenen Fragen fortgesetzt, auch wenn das LEA uns mitgeteilt hat, dass das Auslesen mittels der Spezialsoftware zeitnah eingestellt und die Servicevereinbarung mit dem LKA aufgehoben werden soll, da der hohe Aufwand bei der Sichtung der gewonnenen Daten nicht im Verhältnis zum Erfolg der Maßnahmen stünde.

2.5 Die Ausländerakte vergisst nicht

Ein Bürger stellte bei der Einsichtnahme in die zu ihm bei der Ausländerbehörde[39] geführten Akte fest, dass dort noch verschiedene Unterlagen zu lange zurückliegenden strafrechtlichen Verfahren enthalten waren. Darunter waren zum Teil mehr als 20 Jahre alte gerichtliche Beschlüsse. Ein Dokument betraf sogar eine Verfehlung aus seiner Jugendzeit. Da diese Verfahren bereits aus dem Bundeszentralregister gelöscht waren, hatte die betroffene Person Zweifel an der Rechtmäßigkeit dieser langen Aufbewahrung und wandte sich an uns.

Im Rahmen unserer Prüfung stellten wir fest, dass die Ausländerbehörde die Abschriften der betreffenden Strafurteile seinerzeit aufgrund gesetzlicher Mitwirkungspflichten der Strafverfolgungsbehörden erhalten hatte. Auch nach den heute geltenden Bestimmungen müssen öffentliche Stellen die zuständige Ausländerbehörde unverzüglich unterrichten, wenn sie im Zusammenhang mit der Erfüllung ihrer Aufgaben von einem

37 Siehe § 15a Abs. 1 Satz 1 Asylgesetz (AsylG), der nahezu wortgleich mit § 48 Abs. 3a Satz 1 AufenthG ist.
38 BVerwG, Urteil vom 16. Februar 2023, 1 C 19.21.
39 Die Aufgaben der Ausländerbehörde liegen nach Nr. 36 ZustKat Ord beim LEA, soweit nicht die Bezirksämter gemäß Nr. 22a Abs. 2 ZustKat Ord zuständig sind.

Ausweisungsgrund Kenntnis erlangt haben.[40] Die für die Einleitung und Durchführung eines Strafverfahrens zuständigen Stellen sind außerdem verpflichtet, die Ausländerbehörde unverzüglich über die Einleitung und die Erledigung von Strafverfahren zu informieren.[41]

Allerdings unterliegen die in der Ausländerakte aufbewahrten Dokumente gesetzlichen Vernichtungs- bzw. Löschungspflichten. So besteht eine Verpflichtung zur unverzüglichen Löschung von (rechtmäßig) zur Ausländerakte gelangten Unterlagen bzw. Daten, wenn sie für eine anstehende ausländerrechtliche Entscheidung unerheblich sind und voraussichtlich auch für eine spätere ausländerrechtliche Entscheidung nicht erheblich werden können.[42] Dies betrifft ausdrücklich auch solche Unterlagen, die ohne Ersuchen der Ausländerbehörde an diese übermittelt wurden. Zudem dürfen der betroffenen Person in Fällen, in denen die Eintragung über eine Verurteilung im Bundeszentralregister getilgt worden bzw. zu tilgen ist, die Tat und Verurteilung im Rechtsverkehr nicht mehr vorgehalten und nicht mehr zu ihrem Nachteil verwertet werden.[43] Für strafrechtliche Verurteilungen, die diesem materiellen Verwertungsverbot unterliegen, kann die Erheblichkeit für eine spätere ausländerrechtliche Entscheidung damit regelmäßig ausgeschlossen werden. Hierbei handelt es sich um ein umfassendes Verbot, das von allen staatlichen Stellen ab Tilgung bzw. Tilgungsreife zu beachten ist – unabhängig davon, auf welche Weise sie die entsprechenden Informationen erhalten haben.[44]

Im Rahmen unseres Anhörungsverfahrens räumte das für die Führung der Ausländerakte inzwischen verantwortliche LEA ein, dass sich die betreffenden Unterlagen noch in der Akte befanden. Inwiefern eine weitere Aufbewahrung der Unterlagen zu den strafgerichtlichen Verfahren für eine konkrete ausländerrechtliche Entscheidung erforderlich war, wurde hingegen nicht ausgeführt. Das LEA erklärte vielmehr, dass diese zwischenzeitlich hätten vernichtet werden müssen, und bedauerte, dass dies unterblieben war. Wir erteilten daraufhin eine Verwarnung. Die löschungsreifen Unterlagen wurden, wie uns die betroffene Person bestätigte, umgehend aus der Akte entfernt.

40 § 87 Abs. 2 AufenthG.
41 § 87 Abs. 4 Satz 1 AufenthG i. V. m. Nr. 42 der Anordnung über Mitteilungen in Strafsachen (MiStrA).
42 § 91 Abs. 2 AufenthG i. V. m. Ziffer 91.2.2 der Allgemeinen Verwaltungsvorschrift zum Aufenthaltsgesetz.
43 Siehe § 51 Abs. 1 Bundeszentralregistergesetz (BZRG).
44 Siehe BVerwG, Beschluss vom 23. September 2009, 1 B 16.09.

Bei der Führung von Akten und Dateien durch die Ausländerbehörde muss darauf geachtet werden, dass darin nur für das aufenthaltsrechtliche Verfahren erforderliche Dokumente und Daten vorgehalten werden. Die gesetzlichen Löschungs- und Vernichtungsfristen sind unbedingt einzuhalten.

2.6 Zensus 2022 – Die große Volkszählung

Dieses Jahr war es wieder soweit: Viele Berliner:innen erhielten Post vom Amt für Statistik Berlin-Brandenburg. Sie wurden dazu aufgefordert, anhand eines Fragebogens zahlreiche Fragen zu ihren persönlichen Lebensumständen zu beantworten und damit Informationen über sich preiszugeben. Private Eigentümer:innen von Wohnungen oder Gebäuden mit Wohnraum waren zudem dazu angehalten, Angaben zu ihrem Wohneigentum zu machen.

Aufgrund einer Verordnung der EU[45] muss in sämtlichen Mitgliedstaaten und damit auch deutschlandweit alle zehn Jahre eine Zählung der Bevölkerung durchgeführt werden. Eine solche Volkszählung wird auch als Zensus bezeichnet. Neben Angaben zur Bevölkerung werden im Rahmen der Gebäude- und Wohnungszählung auch Informationen zum Gebäude- und Wohnungsbestand ermittelt. In Deutschland fand die letzte umfassende Zählung der Bevölkerung im Jahr 2011 statt. Ein ursprünglich für 2021 vorgesehener Zensus wurde um ein Jahr verschoben, da die umfangreichen Vorbereitungsmaßnahmen aufgrund der Corona-Pandemie nicht fristgerecht umgesetzt werden konnten.

Mit dem Zensus wird insbesondere ermittelt, wie viele Menschen in Deutschland leben, wie sie wohnen und arbeiten. Auf diese statistischen Erhebungen stützen sich viele Entscheidungen im Bund, in den Ländern und in den Gemeinden. Um europaweit einheitliche Daten über die Bevölkerung und deren Wohnsituation zu erhalten, hat die EU einen Katalog mit zu erhebenden Merkmalen festgelegt. In erster Linie werden hierfür Daten aus den Melderegistern genutzt.[46] Die Meldebehörden übermitteln hierfür Daten aller gemeldeten Personen an die Statistischen Landesämter. Zusätzlich wird eine

45 Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen.

46 Dieses Verfahren nennt sich dementsprechend auch „registergestützter Zensus“.

Haushaltserhebung per Stichprobe durchgeführt. Die zu befragenden Haushalte bzw. Personen werden per Zufallsauswahl ermittelt und durch das zuständige Statistische Landesamt angeschrieben. Diese Haushaltsbefragung dient der Qualitätssicherung der Ermittlung der amtlichen Zahl der Einwohner:innen. Es werden hierdurch Über- und Untererfassungen aufgedeckt und Fehlbestände im Datenbestand der Melderegister festgestellt. Ergänzend werden bei den Haushaltsstichproben auch Befragungen durchgeführt, bei denen umfangreiche Auskünfte gegeben werden müssen.

Die Volkszählung im Jahr 1983 war Anlass für das erste Grundsatzurteil des Bundesverfassungsgerichts (BVerfG) bezüglich des Datenschutzes. So hat das BVerfG das seinerzeit erlassene Gesetz zur Durchführung der Volkszählung für teilweise verfassungswidrig erklärt und die Zählung damit gestoppt. In diesem sog. Volkszählungsurteil wurde das Grundrecht auf informationelle Selbstbestimmung erstmals formuliert.[47] Es gehört seitdem zu den tragenden Säulen des deutschen Datenschutzes. In Bezug auf die registergestützte Erhebungsmethode, bei der bestehende Datenbestände der staatlichen Verwaltungsregister als Basisinformationen genutzt und durch Haushaltsstichproben ergänzt werden, hat das BVerfG im Jahr 2018 bestätigt, dass dieses Vorgehen verfassungskonform ist.[48] Hierdurch wird eine sog. Vollzählung, bei der sämtliche Bürger:innen Deutschlands gezählt und befragt werden, vermieden. Da so insgesamt weniger Haushalte befragt werden müssen, wird auch die Erhebung von Daten einzelner Personen auf ein Minimum beschränkt.

Es ist nicht von der Hand zu weisen, dass im Rahmen der Zensusdurchführung in großem Umfang personenbezogene Daten verarbeitet werden. Für die betroffenen Personen müssen die Datenverarbeitungen daher unbedingt nachvollziehbar sein. Die Beachtung des Transparenzgebots ist vor allem deswegen so wichtig, da die verarbeiteten Informationen nicht allein bei den Bürger:innen erhoben werden. Es bedarf u. a. deshalb spezifischer Rechtsgrundlagen für das Vorgehen beim Zensus.[49]

47 Siehe BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83.
48 Siehe BVerfG, Urteil vom 19. September 2018, 2 BvF 1/15.
49 Hinsichtlich des Zensus 2022 finden sich diese vor allem im Zensusvorbereitungsgesetz 2022 (ZensVorbG 2022) und im Zensusgesetz 2022 (ZensG 2022) sowie speziell für Berlin im Zensusausführungsgesetz Berlin 2022 (ZensusAGBln 2022).

2.7 Offene Verteiler bleiben ein Problem bei Sportvereinen und Fitnessstudios

Zwar ist der Versand der ersten E-Mail inzwischen über 50 Jahre her: Das leidige Problem der „offenen Verteiler" gehört bedauerlicherweise aber immer noch nicht der Vergangenheit an.

Wer E-Mails schreibt, hat die Möglichkeit, den Text gleichzeitig an mehrere Empfänger:innen zu versenden. In den üblichen E-Mail-Programmen werden dazu neben dem klassischen Empfängerfeld „An:" die Felder „CC:" (für „Carbon Copy") und „BCC:" (für „Blind Carbon Copy") angeboten. Wenn die E-Mail-Adressen den Empfänger:innen untereinander nicht offenbart werden dürfen, ist nur die letztgenannte Möglichkeit datenschutzkonform. Immer wieder gelangen jedoch durch die unbedachte Nutzung der Felder „An:" oder „CC:" die E-Mail-Adressen aller Empfänger:innen in die falschen Hände. Wenn es um die Werbung eines Fitnessstudios geht, mag der Inhalt der E-Mail selbst unverfänglich sein, die mitgelieferten E-Mail-Adressen der anderen Empfänger:innen sind es nicht. In der Vereinsarbeit kommt es auch vor, dass Mitglieder, die mit ihren Mitgliedsbeiträgen im Rückstand sind, über eine Gruppe angeschrieben werden. Dabei sollte allerdings sichergestellt sein, dass nicht alle Gruppenmitglieder voneinander erfahren, wer ebenfalls noch säumig ist.

Wenn sich auch die entsprechenden Vorfälle in der Regel auf schlichte Versehen zurückführen lassen, so sollten sie doch stets Anlass sein, die entsprechenden Verarbeitungsvorgänge einer kritischen Prüfung zu unterziehen und Mitarbeiter:innen im Umgang mit personenbezogenen Daten nachzuschulen.

Es wird eher die Regel als die Ausnahme sein, dass die Verwendung eines offenen Verteilers zu einer Meldepflicht bei der zuständigen Aufsichtsbehörde wegen einer Datenpanne führt.[50] Ebenfalls kann es erforderlich sein, die betroffenen Personen zu benachrichtigen.[51] Verantwortliche sind gut beraten, sich mit den entsprechenden Pflichten vorab vertraut zu machen, sodass es im Idealfall gar nicht erst zu einer

50 Siehe Art. 33 DSGVO; siehe auch JB 2018, 1.3.
51 Siehe Art. 34 DSGVO.

Datenschutzverletzung kommt. Die verantwortliche Stelle kann eine Datenpanne u. a. über unsere Website bei uns melden.[52]

2.8 Nicht erst seit der Pandemie: Homeoffice in der Vereinsarbeit und die Nutzung privater Geräte

Was für manche Arbeitnehmer:innen mit Beginn der Pandemie noch neu gewesen sein mag, ist für viele Ehrenamtliche in der aktiven Vereinsarbeit schon lange üblich. Gerade dort, wo es an Ressourcen mangelt und kein Vereinsheim mit eigener digitaler Infrastruktur zur Verfügung steht, sind personenbezogene Daten auch bisher schon von Ehrenamtlichen zu Hause auf privaten Endgeräten verarbeitet worden.

Wir empfehlen, wenn irgend möglich, die Anschaffung von digitalen Endgeräten, die ausschließlich Vereinszwecken dienen. Diese können gesondert gesichert werden. Damit droht weder die Gefahr der Vermischung mit privaten Daten, noch sollte die Übertragung von Datenbestand und Geräten bei Amtswechseln den Verein vor besondere Herausforderungen stellen. Dennoch ist die Nutzung privater Endgeräte zur Verwaltung von Mitgliederdaten nicht grundsätzlich unzulässig, erhöht aber für den Verein und für die Mitglieder den Aufwand und die Risiken. Wir raten grundsätzlich von der Vermischung privater und vereinsbezogener Daten ab, nicht zuletzt, weil sich erfahrungsgemäß auch in der Vereinsarbeit nicht ausschließen lässt, dass nach Beendigung der Zusammenarbeit personenbezogene Daten auf privaten Geräten verbleiben, sei es aus Fahrlässigkeit oder gar nach Trennung im Streit. Ob diese Risiken wirksam aufgefangen werden können, muss die Vereinsführung in eigener Zuständigkeit abwägen und verantwortlich entscheiden.

Als mindeste Sicherheitsvorkehrung raten wir zur ausschließlichen Nutzung eines eigenen, lokalen und vollständig verschlüsselten Speichermediums, wie etwa einem USB-Stick oder einer externen Festplatte. Gleichzeitig sollte eine Zugangskontrolle zu einem privat genutzten Gerät mittels Passwortsicherung bestehen, die garantiert, dass das private Gerät ausschließlich vom Vereinsmitglied genutzt wird und insbesondere auch keine Haushaltsangehörigen Zugriff auf personenbezogene Daten der Mitglieder des

52 Siehe https://www.datenschutz-berlin.de/datenschutz/datenpanne.

Vereins haben. Das Anlegen eines separaten Gerätekontos für die Vereinsarbeit ist zu empfehlen. Neben den Daten selbst ist auch der Datentransport zu verschlüsseln. Eine Selbstverständlichkeit sollte sein, dass aktuelle Betriebs- und Sicherheitssoftware (z. B. Virenscanner und Firewall) sowie sämtliche Sicherheitsupdates installiert sind bzw. regelmäßig zeitnah installiert werden.

Des Weiteren muss ein Löschkonzept bestehen, z. B. zu der Frage, wie Daten endgültig gelöscht werden können. Dazu gehört auch eine bindende Vereinbarung mit dem Vereinsmitglied über den sicheren Umgang mit personenbezogenen Daten. Ein Passus zur Geheimhaltung ist dabei unerlässlich. Der Verein sollte sich zudem ausdrücklich das Recht ausbedingen, mit vereinsbezogenen Daten auf dem privaten Endgerät grundsätzlich in derselben Weise verfahren zu können wie mit solchen in den eigenen Systemen: Der Verein sollte auf die Daten uneingeschränkt zugreifen und sie im Bedarfsfall auch löschen können. Bei Beendigung der Zusammenarbeit muss das Vereinsmitglied verpflichtet werden, die Daten zurückzugeben oder unwiederbringlich zu löschen. Das alles entbindet die Verantwortlichen allerdings nicht davon, die verschiedenen Datenkategorien zu beachten und pflichtgemäß abzuwägen: Beschäftigtendaten etwa oder Kontodaten von Mitgliedern sollten mit größter Vorsicht behandelt und nur übergeben werden, wenn die Bearbeitung trotz aller Anstrengung nicht anders gewährleistet werden kann.

Sofern sich der Vereinsvorstand entscheidet, einen Clouddienst zu nutzen, muss der Verein vorab einen Auftragsverarbeitungsvertrag[53] mit dem Clouddienstanbieter schließen. Die Verlagerung der Daten in die Cloud darf freilich nicht zu einer Absenkung des Datenschutzniveaus führen, das gilt insbesondere für die verschlüsselte Übertragung und Aufbewahrung der Daten, die Pflicht zur Sicherungskopie[54] und die Auswahl eines vertrauenswürdigen Diensts, der DSGVO-konform arbeitet.

53 Siehe Art. 28 DSGVO.
54 Siehe Art. 5 Abs. 1 lit. f DSGVO.

2.9 Zieleinlauf nur gegen Foto?

Wiederholt erreichen uns Nachfragen und Beschwerden von besorgten Eltern, die für ihre Kinder in die Veröffentlichung von Fotos bei Sportveranstaltungen einwilligen sollen. Wir schreiten insbesondere ein, wenn die Teilnahme an der Veranstaltung von einer solchen Zustimmung abhängig gemacht wird, auch bei Veranstaltungen für Erwachsene.

Wenn sich Veranstalter:innen auf eine Einwilligung als Rechtsgrundlage für die beabsichtigte Datenverarbeitung berufen wollen, ist zu beachten, dass die Einwilligung auf der freien Entscheidung der oder des Betroffenen beruhen muss.[55] Nur dann ist sie wirksam. Darüber hinaus muss die Einwilligung in informierter Weise erteilt worden sein.[56] Entscheidend ist auch das sog. Kopplungsverbot. Danach ist „dem Umstand in größtmöglichem Umfang Rechnung [zu tragen], ob u. a. die Erfüllung eines Vertrags [...] von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind".[57] Diese Vorschrift gilt für die Teilnahme an Sportveranstaltungen gleichermaßen wie für die Mitgliedschaft in Vereinen.

Kann die Teilnahme an einer Veranstaltung nur so wahrgenommen werden, dass gleichzeitig eine Zustimmung zu einer Datenverarbeitung erteilt werden muss, die nicht zwingend erforderlich ist, gilt das nicht als freiwillige Einwilligung. Zwingend erforderlich sind in der Vereinsarbeit und zur Durchführung von Sportveranstaltungen klassischerweise nur Name, Startnummer und Kontaktdaten der Sportler:innen, ggf. auch deren Geschlecht sowie deren Geburts- und Zahlungsdaten, nicht aber die Abbildung der Personen im Rahmen der Veranstaltung. Für die Freiwilligkeit der Einwilligung in solche Fotos spielt es daher keine Rolle, ob die betroffene Person auch die Möglichkeit hätte, stattdessen an einer anderen Veranstaltung teilzunehmen oder einfach überhaupt nicht anzutreten.

Es ist nicht von vornherein auszuschließen, dass bspw. der veranstaltende Verein zu Dokumentationszwecken oder für seine Öffentlichkeitsarbeit Fotoaufnahmen machen

55 Siehe Art. 4 Nr. 11 DSGVO; Art. 6 Abs. 1 Satz 1 lit. a DSGVO; Art. 7 DSGVO; EG 42 DSGVO.
56 Art. 4 Nr. 11 DSGVO.
57 Art. 7 Abs. 4 DSGVO.

lässt. Gerade bei der Veröffentlichung der Fotos auch über den Kreis seiner Mitglieder hinaus, insbesondere bei Fotos von Kindern, ist bei der nötigen Interessenabwägung durch die Verantwortlichen jedoch besondere Vorsicht geboten. Dies gilt auch bei der Veröffentlichung von Namen, Spielaufstellungen, Ergebnis- oder Gewinnerlisten. Zwingend erforderlich scheint diese Art der Veröffentlichung – wenn sie auch üblich ist – nicht: Einer Angabe als „N. N." o. Ä. steht bei Betroffenen, die keine Veröffentlichung wünschen, nichts entgegen.[58]

Für externe Fotograf:innen, die aus eigenem finanziellen Interesse etwa Zieleinlauffotos von Sportveranstaltungen fertigen und verkaufen, sind nicht die Veranstalter:innen oder der Verein verantwortlich; gleichwohl gilt hier gleichermaßen, dass für eine Veröffentlichung regelmäßig die Einwilligung der abgebildeten Personen erforderlich ist. Noch mal anders gestaltet sich die Situation bei Pressefotograf:innen, die aber ebenfalls gehalten sind, von Kindern ohne Einwilligung der Eltern keine Einzelfotos zu veröffentlichen.

Uns ist wichtig, dass Vereine und Veranstalter:innen mit einwandfreien Datenschutzerklärungen arbeiten und sich über die Rechtsgrundlagen im Klaren sind, die ihnen eine Verarbeitung personenbezogener Daten erlauben. Erzwungene Einwilligungen hingegen liefern keine wirksamen Rechtsgrundlagen für zusätzlich erwünschte Verarbeitungen. Eine Verknüpfung von Mitgliedschaft, Teilnahme oder Vertragserfüllung mit der Verarbeitung von Daten, die dazu nicht benötigt werden, ist nicht erlaubt und wird von uns verfolgt.

58 Siehe auch JB 2019, 3.9; JB 2021, 3.7.

3 Justiz und Rechtsanwaltschaft

3.1 Der Umfang justizieller Tätigkeit – Wann wir für Gerichte zuständig sind

Immer wieder erreichen uns Bitten von Bürger:innen, Entscheidungen von Gerichten oder Verhalten von Richter:innen in der mündlichen Verhandlung auf datenschutzrechtliche Aspekte hin zu prüfen. Nach dem ausdrücklichen Willen des Grundgesetzes[59] halten wir uns aber aus allem raus, was die wichtige richterliche Unabhängigkeit beeinträchtigen könnte.[60] Ein sehnlich erwartetes Urteil des Europäischen Gerichtshofs (EuGH) sollte Klarheit in der Frage bringen, welche Tätigkeiten damit im Einzelnen gemeint sind.[61] Leider bleibt auch danach noch Vieles offen.

Hintergrund des beim EuGH anhängigen Verfahrens war, dass ein Gericht in den Niederlanden Journalist:innen Einsicht in Gerichtsakten gewährte, um diese in die Lage zu versetzen, genauer Bericht zu erstatten. Die personenbezogenen Daten der Verfahrensbeteiligten wurden dabei regelmäßig nicht unkenntlich gemacht. Der EuGH musste entscheiden, ob diese Gewährung von Akteneinsicht von der Kontrollausnahme gedeckt ist und damit keine Aufsichtsbefugnis der niederländischen Datenschutzaufsichtsbehörde besteht. Der EuGH findet dafür zunächst deutliche Worte: „Die Wahrung der Unabhängigkeit der Justiz setzt [...] voraus, dass die richterlichen Funktionen in völliger Autonomie ausgeübt werden, ohne dass die Gerichte [...] von irgendeiner Stelle Anordnungen oder Anweisungen erhalten, sodass sie auf diese Weise vor Eingriffen oder Druck von außen geschützt sind, die die Unabhängigkeit des Urteils ihrer Mitglieder gefährden und deren Entscheidungen beeinflussen könnten.“[62] Die Verarbeitungen, die die Aufsichtsbehörden nicht prüfen dürften, seien daher nicht nur

59 Art. 97 Abs. 1 Grundgesetz (GG).

60 Auch der europäische Gesetzgeber und das Abgeordnetenhaus sind hier eindeutig: Siehe Art. 55 Abs. 3 Datenschutz-Grundverordnung (DSGVO); § 8 Abs. 3 Berliner Datenschutzgesetz (BlnDSG); § 46 Abs. 1 Satz 2 BlnDSG.

61 Siehe EuGH, Urteil vom 24. März 2022, C 245/20.

62 EuGH C 245/20, Rn 33.

Verarbeitungen „im Rahmen konkreter Rechtssachen [...], sondern in weiterem Sinn alle Verarbeitungsvorgänge [...], die von den Gerichten im Rahmen ihrer justiziellen Tätigkeiten vorgenommen werden“.[63]

Das Gericht führt damit das Problem auf sich selbst zurück, denn was genau den Rahmen der justiziellen Tätigkeiten der Gerichte setzt, sollte ja eigentlich gerade klargestellt werden. Der EuGH lässt jedenfalls keinen Zweifel daran, dass überall dort, wo die „Kontrolle [...] mittelbar oder unmittelbar die Unabhängigkeit der Mitglieder oder der Entscheidungen der Gerichte beeinflussen könnte“,[64] keine Zuständigkeit der Datenschutzaufsichtsbehörden bestehen soll. Dennoch ist die Entscheidung nicht so zu lesen, dass sie andere Verantwortliche, die dem Gericht nur zuarbeiten, von unserer Aufsichtstätigkeit ausnimmt, denn ausgenommen sind nach dem Wortlaut nur die Gerichte selbst. Im Ergebnis soll jedenfalls die vorliegend streitige Akteneinsicht noch im aufsichtsfreien Raum verbleiben, da sie zur „Kommunikationspolitik zu Rechtssachen“ gehöre.[65] Sie stünde jedenfalls „klar in Verbindung“ mit der Ausübung der justiziellen Tätigkeit;[66] eine für die Praxis leider wenig trennscharfe Schlussfolgerung.

Es wird damit weiterhin im Einzelfall zu klären sein, welche Tätigkeit inhärent justizieller Natur ist.[67] Hinzu kommt nun die – für uns nicht ganz neue – Frage, welche Tätigkeit, die für sich genommen nicht die Rechtsprechung prägt, möglicherweise dennoch die Unabhängigkeit der Gerichte so berührt, dass diese bei einer Kontrolle durch uns nicht mehr unvoreingenommen entscheiden könnten. Die stets nötige Klärung kann nur im Dialog mit den Gerichten stattfinden und wird auf absehbare Zeit unsere Arbeit in diesem Bereich beherrschen, das Arbeitsaufkommen bei den Gerichtsverwaltungen keinesfalls verringern und unsere Beschwerdeführer:innen weiter Nerven kosten.

63 EuGH C 245/20, Rn 34.
64 Ebd.
65 EuGH C 245/20, Rn 37.
66 EuGH C 245/20, Rn 38 f.
67 Siehe hierzu auch die sehr gelungene Annäherung unserer nordrhein-westfälischen Kolleg:innen unter https://www.ldi.nrw.de/zustaendigkeit-der-ldi-nrw-bezueglich-der-taetigkeit-von-gerichten.

Bei alldem ist anzumerken, dass in den Niederlanden eine spezifische richterlich besetzte „Kommission zum Schutz personenbezogener Daten für Verwaltungsgerichte“ eingerichtet ist[68] und die Betroffenen im Ausgangsfall damit eine tatsächlich zuständige Ansprechpartnerin gehabt hätten.[69] Anders in Deutschland: Von der Einrichtung „besonderer Stellen im Justizsystem“, die laut DSGVO entsprechende Beschwerden bearbeiten und die Einhaltung der DSGVO sicherstellen sollen,[70] sind wir hierzulande noch weit entfernt. Die Dienstaufsicht durch die Präsident:innen der Gerichte ist hierfür nicht ausreichend, da Interessenkonflikte vorliegen können. Auch der EuGH betont, dass die DSGVO keinesfalls beabsichtige, die Gerichte jeglicher Aufsicht zu entziehen.[71]

3.2 Jetzt kostenlos und ohne Anmeldung: Das offene Handelsregister

Seit der Verabschiedung des Allgemeinen Deutschen Handelsgesetzbuchs (ADHGB) im Jahr 1861 wird auch das Handelsregister in Berlin – vormals unter der Aufsicht der Korporation der Berliner Kaufmannschaft – nunmehr bei den Gerichten geführt und erfüllt dort seinen seit jeher wichtigen Beitrag zum Vertrauensschutz im Rechtsverkehr. Um diese Aufgabe zu beleben, muss das Register für alle Interessent:innen öffentlich einsehbar sein.[72] Mit dem Registerverfahrensbeschleunigungsgesetz (RegVBG) wurde im Jahr 1993 zudem die Möglichkeit geschaffen, das Handelsregister in elektronischer Form zu führen.[73] Seit August sind nun die dort gemachten Angaben kostenlos und ohne Anmeldung für jede Person elektronisch einsehbar.[74]

68 EuGH C 245/20, Rn 9.
69 Siehe EuGH C 245/20, Rn 13.
70 Erwägungsgrund (EG) 20 Satz 3 DSGVO.
71 Siehe EuGH C 245/20, Rn 24.
72 Bereits das ADHGB weist darauf hin, siehe Art. 12 ADHGB: „Bei jedem Handelsgerichte ist ein Handelsregister zu führen, in welches die in diesem Gesetzbuche angeordneten Eintragungen aufzunehmen sind. Das Handelsregister ist öffentlich. Die Einsicht desselben ist während der gewöhnlichen Dienststunden einem Jeden gestattet. Auch kann von den Eintragungen gegen Erlegung der Kosten eine Abschrift gefordert werden, die auf Verlangen zu beglaubigen ist.“
73 Siehe RegVBG vom 20. Dezember 1993, BGBl. I, S. 2182 ff.
74 Siehe § 10 Abs. 2 Handelsgesetzbuch (HGB); umgesetzt durch den Bundesgesetzgeber nach der europäischen Digitalisierungsrichtlinie (EU) 2019/1151.

Im Zuge dessen haben viele Betroffene die Eintragungen zu ihrer Person geprüft und festgestellt, dass dort nicht erforderliche Angaben – wie zum Teil Privatadressen, Personalausweiskopien und Unterschriften – gespeichert und veröffentlicht worden sind. Dazu haben uns zahlreiche Eingaben von Bürger:innen erreicht, die wir an die verantwortliche Stelle, das Amtsgericht Charlottenburg als Berliner Registergericht, verwiesen haben. Unserer Aufsichtstätigkeit sind dort Grenzen gesetzt, wo die Unabhängigkeit der Gerichte berührt sein könnte. Zwar ist eine Eintragung ins Handelsregister keine rechtsprechende Tätigkeit in Streitsachen, sie zeichnet sich jedoch in ihrer Zugehörigkeit zur freiwilligen Gerichtsbarkeit dadurch aus, dass sie von Richter:innen vorgenommen wird.[75] Die justizielle Tätigkeit der Gerichte ist von unserer Kontrollbefugnis ausgenommen.[76]

Soweit sich die Probleme nicht im ersten Kontakt klären lassen, empfehlen wir Betroffenen, die eine datenschutzrechtliche Überprüfung der Verfahrensweise innerhalb des Gerichts erwirken möchten, sich an den Präsidenten des Amtsgerichts Charlottenburg zu wenden. Dieser führt die Dienstaufsicht über die Registerrichter:innen. Eine besondere Stelle zur Aufsicht über Datenverarbeitungsvorgänge in der justiziellen Tätigkeit, wie sie die DSGVO vorsieht,[77] ist bisher leider nicht eingerichtet.

Es ist für uns gut nachvollziehbar, dass Betroffene sich um den Missbrauch ihrer Daten angesichts des nunmehr erleichterten elektronischen Zugangs sorgen.[78] Einschränkungen der freien Verfügbarkeit aller Registerdaten – insbesondere der zur Eintragung im konkreten Fall nicht erforderlichen Daten – sollten daher im Interesse der betroffenen Personen bei den Verantwortlichen und durch den Gesetzgeber zügig vorgenommen werden.

75 § 25 Abs. 1 Satz 1 Handelsregisterverordnung (HRV).
76 Siehe auch 3.1.
77 EG 20 Satz 3 DSGVO.
78 Siehe auch 10.3.

3.3 Verwechslung vor dem Bundeszentralamt für Steuern: Kein vergnüglicher Fall

Für die Kontrolle von Bundesämtern wie dem Bundeszentralamt für Steuern (BZSt) sind nicht wir, sondern der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in Bonn zuständig.[79] Im vorliegenden Fall fragte sich allerdings ein Beschwerdeführer, warum ein Berliner Gerichtsvollzieher seine Konten pfändete, denn er war sich keiner offenen Schuld bewusst. Der Fehler war schnell gefunden: Nicht er war der Schuldner, sondern ein Namensvetter, mit dem er nicht nur den Vor- und Nachnamen teilte, sondern auch das Geburtsdatum. Auseinanderzuhalten waren die Datenzwillinge lediglich anhand ihres Geburtsorts – den aber hatte der Gerichtsvollzieher bei einer Kontoabfrage beim BZSt nicht abgefragt.

Haben Gläubiger:innen offene Forderungen und dazu die Hoffnung, es sei noch etwas einzutreiben, können sie sich an die örtlich zuständigen Gerichtsvollzieher:innen wenden, die dann alles Weitere in die Wege leiten. Mit einem sog. Pfändungs- und Überweisungsbeschluss kommen diese – einen vollstreckbaren Titel vorausgesetzt – schnell an die Konten der mutmaßlich Säumigen. Ist ein Konto nicht bekannt, hilft eine Anfrage beim BZSt im Rahmen des sog. Kontenabrufverfahren. Dort nämlich laufen Informationen zu Kontostammdaten aller Bankkund:innen zusammen. Was ehemals zur Prüfung der Einkünfte aus Kapitalvermögen eingeführt wurde, findet inzwischen vielfach Anwendung, u. a. in der Zwangsvollstreckung.[80]

Aus den Kontostammdaten ergibt sich jedoch häufig nicht die aktuelle Adresse der Kontoinhaber:innen. Nicht selten wird seitens der Bank offenbar nur die Adresse gespeichert, unter der das Konto eröffnet wurde. So konnten im vorliegenden Fall weder der abrufende Gerichtsvollzieher noch die Gläubiger:innen den Datensätzen entnehmen, dass möglicherweise zwei verschiedene Personen aus unterschiedlichen Orten als Kontoinhaber:innen in Frage kommen könnten. Erschwerend kam hinzu, dass bei der Abfrage über das BZSt keine Möglichkeit besteht, einen Geburtsort als Suchkriterium anzugeben. Der Geburtsort wird in den Suchergebnissen auch nicht mitgeliefert. Darin hätten sich unser falscher Schuldner und sein Datenzwilling eindeutig unterschieden. Der Gerichtsvollzieher war vorliegend verpflichtet, den Gläubiger:innen die beim BZSt

79 § 9 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG).
80 Siehe § 802l Abs. 1 Zivilprozessordnung (ZPO).

ermittelten Daten selbst dann mitzuteilen, wenn er Zweifel an deren Richtigkeit gehabt hätte. Er darf sie nur zurückhalten, wenn ihm die Unrichtigkeit der Daten bekannt ist.[81]

Dem Beschwerdeführer gelang es letztlich gegen einigen Widerstand und unter großem Aufwand, die Pfändungen seiner Konten rückgängig zu machen. Das BZSt teilte dem BfDI außerdem mit, dass nun eine Doppelgängerliste geführt werde, in die entsprechende Fälle nach Bekanntwerden aufgenommen würden. Durch gesetzliche Anpassungen stünden für eine eindeutige Identifizierung nunmehr die steuerliche Identifikationsnummer zur Verfügung, auch seien die automatisierten Plausibilitätsprüfungen verbessert worden, indem Zweifelsfälle händisch bearbeitet würden.

3.4 Bundeszentralregisterauszug von der Staatsanwaltschaft

Ein Beschwerdeführer schrieb uns, ein Gericht habe in einem familiengerichtlichen Verfahren unter Zuhilfenahme der Staatsanwaltschaft Berlin einen Bundeszentralregisterauszug erhalten, anstatt selbst beim Bundesamt für Justiz (BfJ) um einen Auszug zu ersuchen.

Die Staatsanwaltschaft hatte auf ein Schreiben des Gerichts mit entsprechender Aufforderung – es sei in einem familiengerichtlichen Verfahren die Erziehungsfähigkeit des Beschwerdeführers zu prüfen – für sich eine Auskunft aus dem Bundeszentralregister gezogen und an das Gericht übersandt. Dabei gab die Staatsanwaltschaft bei der Abfrage beim BfJ als Verwendungszweck an, es laufe ein Ermittlungsverfahren gegen die betroffene Person, was nicht der Fall war.

Nach der Gegenvorstellung des Beschwerdeführers bei der Staatsanwaltschaft regten sich zu Recht Zweifel an der Zulässigkeit der Abfrage unter falschen Voraussetzungen und der Übermittlung an das Gericht. Die Staatsanwaltschaft forderte den Auszug daraufhin vom Gericht zurück; ein ungewöhnlicher Vorgang, aber nach bereits erfolgter Auskunft nunmehr der einzig verbleibende. Das Gericht lehnte eine Rückübersendung jedoch ab.

81 Siehe Landgericht (LG) Würzburg, Beschluss vom 29. Juli 2014, 3 T 773/14.

Die Generalstaatsanwältin schloss sich auf unsere Nachfrage der Einschätzung der Staatsanwaltschaft an und sah in der Übermittlung zudem eine unerlaubte Zweckänderung.[82] Sie versicherte uns, dass es bei der Staatsanwaltschaft im Allgemeinen Routine sei, Registerauszüge bei Aktenversendungen an andere Stellen, die nicht mit dem Strafverfahren unmittelbar befasst sind, zurückzuhalten und Auskünfte aus den Registern nur zu eigenen Zwecken zu beantragen, was die Senatsverwaltung für Justiz, Vielfalt und Antidiskriminierung soweit bestätigte. Der Vorfall sei zum Anlass genommen worden, die Einhaltung der datenschutzrechtlichen Belange gesondert in den Blick zu nehmen. Wir haben das Verfahren mit einer Mangelfeststellung gegenüber der Staatsanwaltschaft abgeschlossen.

Die Frage, ob das Gericht auf eine eigene Anfrage vom BfJ unbeschränkte Auskunft erhalten hätte, muss mangels Zuständigkeit unbeantwortet bleiben. Das Gericht hätte den Zweck seines Ersuchens ausführen[83] und das BfJ das Ersuchen im Hinblick auf eine Auszugserteilung an das Gericht prüfen müssen. Beides ist hier nicht erfolgt.

3.5 Darf die Staatsanwaltschaft zur Datenauskunft Personalausweiskopien verlangen?

Auch gegenüber der Staatsanwaltschaft sollen Bürger:innen ihre Auskunftsrechte effektiv geltend machen können.[84] Da es sich in der Regel um eine Auskunft besonders geschützter Daten handelt,[85] stellt die Staatsanwaltschaft hohe Anforderungen an die Identifizierung von Antragstellenden, wenn in dieser Hinsicht Zweifel bestehen.

Das Verfahren, in dem der Auskunftsantrag bearbeitet wird,[86] ist abgestuft und unterscheidet u.a. danach, ob sich bestimmte identifizierende Merkmale aus dem vorliegenden Aktenbestand ergeben. Erst bei begründeten Zweifeln an der Personen

82 Siehe § 500 Strafprozessordnung (StPO) i.V.m. §§ 49, 47 Nr. 2, 3 BDSG.
83 § 41 Abs. 3 Satz 1, 2 BZRG.
84 Siehe JB 2021, 3.2.
85 Siehe Art. 10 DSGVO.
86 Siehe § 500 Abs. 1 StPO i.V.m. §§ 59, 57 BDSG.

identität darf die Staatsanwaltschaft weitere Informationen bei der antragstellenden Person selbst erheben.[87] Hier kommt die Anforderung einer Personalausweiskopie ins Spiel, die allerdings auch eine Hürde bei der Geltendmachung des Auskunftsrechts darstellen kann.

Die Bedenken der Staatsanwaltschaft sind grundsätzlich nachvollziehbar: Gerade aus dem familiären oder häuslichen Nahbereich kommen unberechtigte Auskunftsanfragen in Betracht, da ggf. starke Interessen an der Auskunft über Lebenspartner:innen, Nachbar:innen oder Kinder bestehen und der Zugriff auf die Postsendung mit der Auskunft leicht möglich ist. Aus unserer Sicht ist die Kopie oder gar der Scan des Personalausweises jedoch gerade in diesen Fällen kaum geeignet, die Personenidentität zwischen der Person, auf die sich die Auskunft bezieht, und der bzw. dem Antragsteller:in zu belegen. Eben jene Personen aus dem Nahbereich können auch Zugriff auf Ausweisdokumente haben, sodass diese durch das Anfordern einer Kopie nicht sicher abgeschreckt würden. Anstelle der Informationen aus einem Ausweisdokument, dessen Kopie zudem teilweise geschwärzt werden dürfte, ergeben sich aus dem Aktenbestand oft andere, zuverlässigere Identifikationsmerkmale.[88]

Auf unsere Zweifel an der Ausweiskopie als wirksames und zulässiges Mittel der zuverlässigen Identifizierung in den skizzierten Szenarien haben wir die Staatsanwaltschaft hingewiesen. Um Auskunftsrechte gegenüber der Staatsanwaltschaft geltend zu machen, ist nur in Ausnahmefällen das Vorlegen einer Ausweiskopie eine sinnvolle Maßnahme. Zur Antragstellung genügt grundsätzlich ein formloses Schreiben; die Auskunft ist kostenfrei.[89]

87 Siehe Verwaltungsgericht (VG) Berlin, Urteil vom 31. August 2020, 1 K 90.19.

88 Zur Einholung von Personalausweiskopien im Bereich der DSGVO siehe bereits JB 2018, 9.2.

89 § 59 Abs. 3 Satz 1 BDSG. Ein Muster zur Antragstellung findet sich auf unserer Website unter https://www.datenschutz-berlin.de/buergerinnen-und-buerger/selbstdatenschutz/ueberpruefung-ihrer-daten/innere-sicherheit/staatsanwaltschaft.

3.6 Grundsatz der Datenminimierung auch in rechtsanwaltlichen Schriftsätzen

Uns erreichen regelmäßig Beschwerden über die Verarbeitung personenbezogener Daten durch Rechtsanwält:innen im Rahmen von zivilrechtlichen Rechtsstreitigkeiten bzw. Gerichtsverfahren. Oft beschweren sich die betroffenen Personen, dass in den Schriftsätzen und Klagebegründungen ihre personenbezogenen Daten an das Gericht, die gegnerische Partei oder andere Empfänger:innen übermittelt werden, obwohl diese nicht oder nicht im jeweiligen Umfang zur Ausübung der rechtlichen Interessen notwendig erscheinen.

Rechtsanwält:innen sind hinsichtlich ihres Vortrags in rechtlichen bzw. gerichtlichen Verfahren grundsätzlich datenschutzrechtlich verantwortlich.[90] Als unabhängige Organe der Rechtspflege tragen sie in ihrer Eigenschaft als Rechtsberater:innen und Vertreter:innen selbst die Verantwortung für den Inhalt der Schriftsätze, auch wenn sie hierbei zur Wahrnehmung der rechtlichen Interessen ihrer Mandant:innen handeln. Soweit sie also in Ausübung eines Mandats personenbezogene Daten von Dritten verarbeiten, entscheiden sie auch über die Zwecke und Mittel der Verarbeitung dieser Daten und sind insofern nicht etwa Auftragsverarbeiter[91] für die Mandant:innen, sondern selbst Verantwortliche. Hieraus folgt, dass sie Daten nur dann verarbeiten dürfen, wenn hierfür eine Rechtsgrundlage[92] besteht und die Datenschutzgrundsätze[93] gewahrt werden.

Soweit die Verarbeitung bzw. Übermittlung personenbezogener Daten zum Zweck der Rechtsverfolgung und -verteidigung auf eine rechtliche Grundlage gestützt werden kann,[94] wird die Datenverarbeitung hinsichtlich Art und Umfang durch die gesetzliche Forderung beschränkt, dass die Verarbeitung zu diesen Zwecken „erforderlich“ sein muss. Bei der Bestimmung der Erforderlichkeit ist insbesondere der Grundsatz der Datenminimierung zu beachten, der die rechtmäßige Zweckbestimmung und folglich auch die Erforderlichkeit der Datenverarbeitung eingrenzt. Der Grundsatz der Daten

90 Sie sind sog. Verantwortliche i. S. v. Art. 4 Nr. 7 DSGVO.
91 I. S. v. Art. 4 Nr. 8 DSGVO.
92 Siehe Art. 6 Abs. 1 DSGVO.
93 Siehe Art. 5 DSGVO.
94 Bspw. auf Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

minimierung verlangt, dass nur Daten, die dem konkreten Zweck dienen, und auch nur so viele Daten, wie für die Zweckerreichung notwendig sind, verarbeitet werden dürfen.[95] Hieraus folgt für die Datenverarbeitung im Rahmen der Mandatsausübung, dass Rechtsanwält:innen stets prüfen müssen, ob personenbezogene Daten bspw. für die Geltendmachung eines Anspruchs vor Gericht erheblich bzw. zur Wahrung der klägerischen Darlegungslast für die anspruchsbegründenden Tatsachen notwendig sind. Nicht erforderliche Daten sind wegzulassen bzw. unkenntlich zu machen. Dies kann mit einem Hinweis auf datenschutzrechtliche Pflichten gegenüber dem Gericht begründet werden. Bei Zweifeln, ob ein Sachvortrag durch die Beibringung der geschwärzten Unterlagen hinreichend substanziiert ist, kann um gerichtlichen Hinweis gebeten werden, wenn aus Sicht des Gerichts die vollständige Kopie erforderlich sein sollte.

Der Grundsatz der Datenminimierung ist durch Rechtsanwält:innen auch bei Tätigwerden für ihre Mandant:innen und insbesondere im Rahmen der gerichtlichen Durchsetzung von Ansprüchen bzw. bei der Rechtsverteidigung zu beachten. Auf die Übermittlung nicht erforderlicher Daten muss verzichtet werden.

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

4 Jugend und Bildung

4.1 Ausführungsvorschriften für die Jugendhilfe im Strafverfahren – Datenschutz von vornherein mitgedacht

Wegen zahlreicher Gesetzesänderungen war es notwendig, die Ausführungsvorschriften für die Jugendhilfe im Strafverfahren (JuHiS) zu aktualisieren.[96] In diesem Zusammenhang erfolgte auch eine Anpassung an die Vorschriften der Datenschutz-Grundverordnung (DSGVO). Die zuständige Senatsverwaltung für Bildung, Jugend und Familie hat uns frühzeitig in den Prozess einbezogen und um unsere Beratung gebeten.

In einem sehr konstruktiven Austausch mit der Jugendverwaltung haben wir unsere Änderungs- und Ergänzungsvorschläge eingebracht. Im Einzelnen ging es z. B. um Anpassungen im Hinblick auf die nach der DSGVO bestehenden Informationspflichten. Ein weiterer Aspekt waren Regelungen zur Weiterleitung personenbezogener Daten durch die JuHiS an die Bewährungshilfe für Jugendliche bzw. an freie Träger der Jugendhilfe, bei denen ein besonderes Augenmerk auf die Transparenz der Datenverarbeitung für die Jugendlichen zu richten war. Da es sich bei den durch die JuHiS verarbeiteten personenbezogenen Daten um Sozialdaten handelt, die einem besonderen Schutz unterliegen, ist es besonders wichtig, dass die Ausführungsvorschriften die teilweise sehr abstrakten gesetzlichen Vorschriften in einer praxisgerechten Weise konkretisieren.

Es hat sich gezeigt, dass sachgerechte Abstimmungen in kurzer Zeit erfolgen können, wenn wir frühzeitig beteiligt werden und die Senatsverwaltung für Bildung, Jugend und Familie rechtzeitig beraten können. Für die JuHiS konnten so Ausführungsvorschriften in Kraft treten, die sowohl praxisgerecht als auch datenschutzkonform sind.

96 Abrufbar unter https://www.berlin.de/sen/jugend/recht/220501-av_jgh.pdf.

4.2 Handlungsleitfaden für die Kindertagespflege bei Verdacht einer Kindeswohlgefährdung

Die Senatsverwaltung für Bildung, Jugend und Familie erarbeitet einen Handlungsleitfaden, um Kindertagespflegepersonen hinsichtlich des Umgangs und des Verfahrensablaufs beim Verdacht auf eine Kindeswohlgefährdung zu unterstützen. Wir haben die Senatsverwaltung zu einzelnen Fragen beraten.

Haben Kindertagespflegepersonen den Verdacht, dass bei einem von ihnen betreuten Kind eine Gefährdung des Kindeswohls im Raum steht, ist es wichtig, dass sie wissen, was zu tun ist. Neben den fachlichen, persönlichen und emotionalen Herausforderungen in einer solchen Situation haben die Kindertagespflegepersonen auch datenschutzrechtliche Fragen zu klären. Denn personenbezogene Daten von Kindern und Personensorgeberechtigten dürfen regelmäßig nur dann an das Jugendamt übermittelt werden, wenn hierfür eine gesetzliche Grundlage besteht. In der Regel wird eine Mitteilung an das Jugendamt nur dann in Betracht kommen, wenn die Gefährdung nicht anders abgewendet werden kann.

Ein Teil unserer Beratung betraf daher die Frage, welche Rechtsgrundlage für die Datenweitergabe an das Jugendamt in Betracht kommen kann. Damit im Fall einer Kindeswohlgefährdung auch Kindertagespflegepersonen rechtssicher handeln können, hat der Bundesgesetzgeber die Vorschriften im Kinder- und Jugendrecht angepasst. Der Kreis derjenigen Institutionen, die einen Schutzauftrag bei einer Kindeswohlgefährdung haben, wurde ausdrücklich um Kindertagespflegepersonen erweitert. So ist nunmehr geregelt, dass auch Kindertagespflegepersonen bei Bekanntwerden gewichtiger Anhaltspunkte für die Gefährdung eines von ihnen betreuten Kindes eine Gefährdungseinschätzung vornehmen müssen. Dabei ist eine insoweit erfahrene Fachkraft – eine Person, die für die Einschätzung einer Kindeswohlgefährdung qualifiziert ist – beratend hinzuziehen.[97] Ferner sind die Erziehungsberechtigten sowie das Kind in die Gefährdungseinschätzung einzubeziehen, soweit hierdurch der wirksame Schutz des Kindes nicht in Frage gestellt wird. Dabei müssen Kindertagespflegepersonen grundsätzlich eine „originär-eigene“ Einschätzung der Gefährdungsrisiken und -lage des von ihnen

97 § 8a Abs. 5 Sozialgesetzbuch Achtes Buch (SGB VIII).

betreuten Kindes vornehmen. Die Inanspruchnahme der Beratung durch eine insoweit erfahrene Fachkraft ist daher von besonderer Relevanz.

Kindertagespflegepersonen sind ferner verpflichtet, bei den Erziehungsberechtigten auf die Inanspruchnahme von Hilfen hinzuwirken, wenn sie diese für erforderlich halten. Falls die Gefährdung nicht anders abgewendet werden kann, besteht zudem eine Verpflichtung zur Mitteilung an das Jugendamt. Damit ist die Hinzuziehung des Jugendamts – wie auch bei Fachkräften von sonstigen Einrichtungen und Diensten – in der Regel erst dann möglich, wenn dies für die Gefährdungsabwendung absolut notwendig ist. Um gegenüber den Erziehungsberechtigten Transparenz zu schaffen, haben wir empfohlen, auf diese gesetzlichen Verpflichtungen bereits zu Beginn der Kindertagespflege hinzuweisen.

Die Gefährdungseinschätzung von Kindertagespflegepersonen bei Anhaltspunkten für eine Kindeswohlgefährdung kann im Einzelfall schwierig sein, sodass die Inanspruchnahme einer dafür qualifizierten Fachkraft von besonderer Bedeutung ist. Wichtig ist, den Kindertagespflegepersonen Hilfestellung zu geben, wie sie sich im Fall gewichtiger Anhaltspunkte für eine Kindeswohlgefährdung verhalten sollen, um auch datenschutzrechtlich auf der sicheren Seite zu sein.

4.3 Say Cheese! – Bild-, Ton- und Videoaufnahmen in Kindertagesstätten

Das Erstellen von Fotos gehört zum Kitaalltag. Hinsichtlich der einzuhaltenden datenschutzrechtlichen Rahmenbedingungen ergeben sich allerdings immer wieder Fragen. Auch in diesem Jahr erreichten uns wieder verschiedene Anfragen von Kindertageseinrichtungen und betroffenen Personen, unter welchen Voraussetzungen Fotos, Videos und Tonaufnahmen von Kindern in der Kindertageseinrichtung angefertigt und weitergegeben werden dürfen.

Im Regelfall bedarf es für die Anfertigung von Bild-, Ton- und Videoaufnahmen von Kindern sowie deren Weitergabe, Veröffentlichung oder anderweitigen Verwendung der wirksamen Einwilligung der Sorgeberechtigten des Kindes. Die Einwilligung hat

sich dabei an den Vorgaben der DSGVO zu orientieren.[98] Dies bedeutet, dass die Einwilligung informiert und freiwillig erfolgen muss. In der Einwilligungserklärung sollte neben einer möglichst konkreten Beschreibung der Zwecke der Aufnahmen[99] zudem explizit festgelegt werden, in welcher Weise die Aufnahmen genutzt bzw. (weiter)verwendet[100] und wem sie gezeigt oder an wen sie weitergegeben werden. In der Praxis bietet es sich an, für die einzelnen Aufnahmearten (Bild-, Ton- oder Videoaufnahmen) jeweils Ankreuzfelder vorzusehen. Zudem sollte die Kita darauf hinweisen, dass die Sorgeberechtigten das Recht haben, ihre einmal erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Die Einwilligung sollte von der Kita schriftlich und unbedingt vor Erstellung der Aufnahmen eingeholt werden. Die von uns gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Familie herausgegebene, bereits in 2. Auflage erschienene Broschüre „Datenschutz bei Bild-, Ton- und Videoaufnahmen“[101] bietet nach wie vor Hilfestellung für den Kitaalltag.

Bei der Weitergabe von Aufnahmen an die Sorgeberechtigten ist auch zu beachten, technische und organisatorische Maßnahmen zum Schutz und zur Sicherheit der Aufnahmen zu ergreifen: Wenn die Aufnahmen bspw. mithilfe eines Datenträgers verteilt werden sollen, müssen die Aufnahmen z. B. durch Verschlüsselung so geschützt sein, dass im Falle des Verlusts des Datenträgers keine Dritten unbefugt Kenntnis nehmen können. Insbesondere beim Einsatz von Kommunikationsdiensten, wie etwa beim Versand via Messengerdienst, muss die Kindertageseinrichtung Sorge dafür tragen, dass diese datenschutzkonform genutzt werden können. Dies ist in der Praxis nicht immer der Fall.

Der Erstellung von Bild-, Ton- und Videoaufnahmen in einer Kindertageseinrichtung steht nichts im Wege, wenn wirksame Einwilligungen der Sorgeberechtigten der Kinder eingeholt werden. Beim Einsatz von Messengerdiensten muss im Vorhinein geprüft werden, ob der Einsatz datenschutzkonform erfolgen kann.

98 Siehe Art. 7 DSGVO i. V. m. Art. 4 Nr. 11 DSGVO.

99 Etwa Fotoaufnahmen auf Ausflügen oder Veranstaltungen, Zeigen von Filmsequenzen auf einem Elternabend, Erstellung von Lehrmaterial etc.

100 Bspw. zur Veröffentlichung auf der Website, für Printpublikationen, als Aushänge in den Räumlichkeiten etc.

101 Abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/broschueren/2020-BlnBDI-Datenschutz_Bild_Ton_Video.pdf.

4.4 Schuldigitalisierung und Datenschutz

Wie in den Vorjahren waren wir auch in diesem Jahr mit unterschiedlichen Themen der Digitalisierung der Schulen befasst. Nachdem wir im letzten Jahr auch von positiven Entwicklungen berichten konnten, z. B. von der Novellierung der Datenschutzregelungen des Berliner Schulgesetzes (SchulG), bei welcher wir das Abgeordnetenhaus umfassend beraten haben,[102] war dieses Jahr in weiten Teilen von Stillstand geprägt. Die Bildungsverwaltung hat unsere Beratung zu vielen datenschutzrechtlichen Themen entweder nicht eingeholt oder unsere Empfehlungen nicht aufgenommen.

4.4.1 Gesetzliche Grundlagen

Wir haben bereits mehrfach darauf hingewiesen, dass die seit Jahren andauernde Überarbeitung der seit 1994 geltenden Schuldatenverordnung[103] und nun auch die Schaffung der Verordnung über den Einsatz digitaler Lehr- und Lernmittel endlich abgeschlossen werden muss. Zusätzlich zu den im Oktober 2021 in Kraft getretenen schulgesetzlichen Regelungen muss eine konkrete Ausgestaltung der gesetzlichen Rahmenbedingungen im Interesse der Schulpraxis in den genannten Verordnungen zeitnah erfolgen. Wir begleiten den Prozess bereits seit 2018, müssen aber feststellen, dass immer noch nicht alle datenschutzrechtlichen Anforderungen berücksichtigt worden sind.

Positiv hervorzuheben ist, dass die Senatsverwaltung für Bildung, Jugend und Familie von ihrer noch Mitte des Jahres vertretenen Position, es reiche aus, lediglich die Schuldatenverordnung zu novellieren, abgerückt ist und uns im Herbst den Entwurf einer Digitalen Lehr- und Lernmittelverordnung vorgelegt hat. Da die Schuldatenverordnung eher auf die Verarbeitung personenbezogener Daten im administrativen Bereich der Schulen anwendbar ist, halten wir es für sehr wichtig, dass alle im Zusammenhang mit der Digitalisierung der Schulen im Schulalltag stehenden Datenverarbeitungen, z. B. beim Einsatz von Lernplattformen und Videokonferenzsystemen sowie bei der Nutzung digitaler Endgeräte oder bei der elektronischen Kommunikation, in einer gesonderten Verordnung geregelt werden. Eine solche Verordnung kann dann auch jederzeit an

102 Siehe JB 2021, 1.2.1.
103 Siehe JB 2021, 1.2.2.

eine sich ändernde Technologie angepasst werden. Leider sind die von der Bildungsverwaltung vorgeschlagenen Regelungen in dem Entwurf noch zu unbestimmt, um den Schulen eine praxisgerechte Hilfestellung zu geben. Wir haben dies gegenüber der Senatsverwaltung problematisiert und eine Schärfung der Regelungen empfohlen. Den Prozess werden wir weiterhin begleiten.

4.4.2 Berliner Schulportal

Die Senatsverwaltung für Bildung, Jugend und Familie hat im letzten Jahr das Schulportal als zentrale Schaltstelle für eine Vielzahl verschiedener Dienste und Dienstleistungen im Schulkontext öffentlich angekündigt. Über dieses Schulportal soll bspw. die Anmeldung von Lehrkräften und Schüler:innen in den Lernmanagementsystemen „Lernraum Berlin“ und „itslearning“ sowie anderen Lernplattformen, die den Schulen von der Bildungsverwaltung angeboten werden, ermöglicht werden. Bereits jetzt ist im Schulportal für einen Teil der Lehrkräfte der Zugang zu den E-Mail-Konten integriert, über die eine dienstliche E-Mail-Kommunikation geführt werden soll. Die Senatsverwaltung plant für die Zukunft eine erhebliche Ausweitung der Funktionen des Schulportals. So sollen sich dort auch Erziehungsberechtigte anmelden können, um gewisse Dienstleistungen, wie z. B. die Ausstellung von Schulbescheinigungen, in Anspruch nehmen zu können. Da über das Schulportal zentrale Dienste zur Verfügung gestellt werden und ein Zugriff auf die personenbezogenen Daten einer Vielzahl unterschiedlicher Nutzer:innen und Nutzergruppen erfolgt, der künftig noch weiter ausgebaut werden soll, ist es notwendig, dass das Schulportal sicher betrieben wird.

Bei der Entwicklung des Schulportals wurden wir bislang nur unzureichend einbezogen. Die uns übergebenen Unterlagen wie das Datenschutz- und IT-Sicherheitskonzept wiesen gravierende Mängel im Hinblick auf die Einhaltung der datenschutzrechtlichen Regelungen und insbesondere bzgl. der IT-Sicherheit auf. Bereits bei der Novellierung des SchulG haben wir darauf hingewiesen, dass für den Betrieb und auch die Funktionalitäten des Schulportals angesichts der Vielzahl der dort verarbeiteten personenbezogenen Daten von Schüler:innen und Lehrkräften eine gesetzliche Grundlage erforderlich ist. Bisher existiert eine solche nur für den Teilbereich des Identitätsmanagements. Dies haben wir gegenüber der Senatsverwaltung für Bildung, Jugend und Familie auch deutlich gemacht. Leider hat die Schulverwaltung uns in den weiteren Prozess nicht mehr einbezogen.

Neben der Schaffung der fehlenden gesetzlichen Grundlage muss die Bildungsverwaltung insbesondere den IT-Sicherheitsprozess vorantreiben und feststellen, welche Maßnahmen zur Absicherung des Schulportals notwendig sind, um diese dann umgehend umsetzen zu können. Dies hätte in Form einer Datenschutz-Folgenabschätzung vor Aufnahme des Betriebs geschehen müssen. Da das Schulportal derzeit schon produktiv verwendet wird, muss eine solche dringend nachgeholt werden.

4.4.3 Endgeräte und E-Mail-Adressen für Lehrkräfte

Die Senatsverwaltung für Bildung, Jugend und Familie hat für alle Lehrkräfte mobile Endgeräte beschafft und diese auch bereits ausgegeben. Die Geräte werden zentral verwaltet. Die Anmeldung erfolgt über eine eigene Benutzerkennung für Lehrkräfte aus dem Schulportal. Über die Endgeräte werden den Lehrkräften auch dienstliche E-Mail-Adressen zur Verfügung gestellt. Auch hier wurden wir in die Konzeption nicht eingebunden. Eine Datenschutz-Folgenabschätzung liegt bislang ebenso nicht vor.

4.4.4 Positivliste

Die Senatsverwaltung für Bildung, Jugend und Familie ist gesetzlich verpflichtet, festzulegen, welche digitalen Lehr- und Lernmittel für die Schulen in Betracht kommen.[104] Diese Positivliste soll den Schulen die Auswahl geeigneter Software erleichtern, indem die Produkte bereits durch die Senatsverwaltung auf deren Eignung in pädagogischer und datenschutztechnischer wie -rechtlicher Hinsicht geprüft werden. Bei der Erstellung dieser Liste wurde unsere Behörde bisher nicht beteiligt. Da uns die Prüfkriterien bis zum Redaktionsschluss nicht vorlagen und auch nicht öffentlich einsehbar waren, ist der Prozess der Bewertung der Bildungsverwaltung für uns nicht nachvollziehbar. Grundsätzlich sehen wir es als problematisch an, dass die Liste nicht öffentlich zugänglich ist. Ebenso wenig ist uns bekannt, nach welchen Kriterien die Senatsverwaltung die Datenschutzkonformität der Produkte prüft. Wir können insofern nicht bewerten, ob die Prüfung zu einem für die Schulen verwertbaren Ergebnis führen kann. Entscheidend ist, dass die Schulen ihren Pflichten als Verantwortliche nach der DSGVO nachkommen können.[105] Die Senatsverwaltung ist daher verpflichtet, diesen die Ergebnisse ihrer Prüfungen zur Verfügung zu stellen.

104 § 7 Abs. 2a Satz 2 SchulG.
105 Siehe Art. 4 Abs. 7 DSGVO.

Wir hätten die Bildungsverwaltung in diesem so zentralen Punkt der Prüfung der Datenschutzkonformität von an Schulen eingesetzten digitalen Produkten gern beraten. Unsere Expertise wurde allerdings erneut nicht in Anspruch genommen. Zu gegebener Zeit werden wir die Liste im Rahmen unserer Aufsichtszuständigkeit einsehen und bewerten.

4.4.5 Endgeräte für Schüler:innen

Zum Ende des Jahres haben wir von Plänen des Senats erfahren, künftig Schüler:innen flächendeckend mit digitalen Endgeräten auszustatten. Nach dem uns vorgelegten Konzept soll es sich bei diesen Geräten, die bereits 2023 an die Schüler:innen der 7. Klasse ausgegeben werden sollen, um Tablets eines US-amerikanischen Anbieters handeln. Problematisch ist, dass zur Nutzung dieser Geräte personenbezogene Daten an den Hersteller übermittelt werden müssen. Dabei ist nicht transparent, in welchem Umfang auch personenbezogene Daten von Schüler:innen betroffen wären. Zudem sollen die Geräte zentral verwaltet werden, wozu ein sog. Mobile Device Management (MDM) eingesetzt werden soll. Ein solches MDM lässt umfangreiche Zugriffsmöglichkeiten auf die Geräte zu: Viele MDM ermöglichen etwa, aus der Ferne Standortdaten abzurufen und Software zu installieren; mit einigen MDM lassen sich sogar aus der Ferne Bild- und Tonaufnahmen erstellen.

Da uns die Bildungsverwaltung auch hier nicht einbezogen hat, liegen uns keine Informationen vor, die uns eine Bewertung ermöglichen. Aufgrund der uns zur Verfügung stehenden Informationen müssen wir allerdings davon ausgehen, dass der Betrieb dieser Geräte wohl nicht datenschutzkonform erfolgen kann. Dies gilt insbesondere im Falle der Privatnutzung der Geräte durch die Schüler:innen. Die Bildungsverwaltung muss vor dem Kauf dieser Geräte Maßnahmen ergreifen, um das Risiko zu minimieren, dass personenbezogene Daten von Schüler:innen an den Gerätehersteller übermittelt werden. Zudem muss sichergestellt werden, dass die Geräte nicht zur Überwachung der Kinder und Jugendlichen genutzt werden können. Entsprechendes haben wir auch im Rahmen der Anhörung zu diesen Plänen im Bildungsausschuss des Abgeordnetenhauses vorgetragen und empfohlen, eine geräte- und betriebssystemunabhängige Lösung in Betracht zu ziehen.

4.4.6 Berliner Lehrkräfte-Unterrichts-Schuldatenbank

Der Beratungsprozess zwischen der Bildungsverwaltung und unserer Behörde zur Berliner Lehrkräfte-Unterrichts-Schuldatenbank (BLUSD bzw. LUSD) wurde auch in diesem Jahr fortgesetzt. Wir nehmen hier einen sehr konstruktiven Austausch wahr. Unsere Hinweise werden von der Bildungsverwaltung angenommen und meist auch umgesetzt.

Ein konkretes Problem besteht derzeit darin, dass die Schulen zur Nutzung der LUSD gesetzlich verpflichtet sind, diese Regelung aber nicht für die Schulämter gilt. Während zwar die meisten Schulämter inzwischen die LUSD für die Erfüllung ihrer Aufgaben nutzen, hat uns die Bildungsverwaltung darauf hingewiesen, dass einzelne Bezirke nur ungern von der unverschlüsselten, also nicht datenschutzkonformen E-Mail-Übermittlung personenbezogener Daten im Ein- und Umschulungsprozess abrücken möchten. Hier besteht Handlungsbedarf vonseiten des Gesetzgebers. Wir sind gern bereit, uns beratend für eine praxisgerechte Lösung einzusetzen.

Mit Ausnahme einiger weniger Bereiche müssen wir erneut feststellen, dass erhebliche Defizite im Hinblick auf die datenschutzgerechte Digitalisierung von Schulen bestehen. Zurückzuführen sind diese auch darauf, dass die Bildungsverwaltung unsere Beratung entweder zu spät oder überhaupt nicht einholt bzw. unsere Empfehlungen nicht aufgreift. Häufig lassen sich einmal gestellte Weichen im späteren Projektverlauf entweder gar nicht oder nur schwer und mit erheblichem (finanziellen) Aufwand korrigieren. Datenschutz ist aber kein Hindernis. Frühzeitig mitgedacht, eröffnet er auch neue Möglichkeiten. Wir stehen weiterhin mit konstruktiver Beratung zur Verfügung und erwarten, dass unsere Empfehlungen im Interesse aller Betroffenen von der Senatsverwaltung aufgenommen werden.

5 Gesundheit

5.1 Auftragsverarbeitung in Krankenhäusern – Novellierung des Landeskrankenhausgesetzes (eine Fortsetzung)

2020 hatte der Gesetzgeber die Vorgaben für die Auftragsverarbeitung in Krankenhäusern im Landeskrankenhausgesetz (LKG) neugefasst. Dem war ein mehrjähriger Abstimmungsprozess zwischen zuständiger Senatsverwaltung, Senatskanzlei, Krankenhäusern und unserer Behörde vorangegangen.[106] Die Regelung sollte erst zwei Jahre später, im Oktober dieses Jahres, in Kraft treten. Kurz vor diesem Termin haben die Koalitionsfraktionen dann einen ganz neuen Entwurf vorgelegt.

Im Zuge der Novellierung zahlreicher Landesgesetze im Jahr 2020 waren im LKG, das spezielle Datenschutzregelungen für Krankenhäuser enthält, die notwendigen Anpassungen an die Datenschutz-Grundverordnung (DSGVO) vorgenommen worden.[107] Dabei wurde die 2017 erfolgte Novellierung des Strafgesetzbuchs berücksichtigt, die eine generelle Offenbarungsbefugnis für die Inanspruchnahme von Dienstleister:innen zur Auftragsverarbeitung einführte. Dementsprechend wurde die für die Krankenhäuser sehr praxisrelevante Regelung zur Auftragsverarbeitung im LKG angepasst.[108] Bis 2020 konnten Krankenhäuser Daten von Patient:innen im Auftrag nur selbst verarbeiten oder im Auftrag durch ein anderes Krankenhaus verarbeiten lassen. Zusätzlich war eine Verarbeitung durch Auftragsverarbeiter:innen möglich, wenn die zu verarbeitenden Daten vor der Übergabe so verändert wurden, dass die Dienstleister:innen nicht erkennen konnten, auf welche Patient:innen sich diese beziehen. Stellte diese Regelung vor 2017 noch eine über das Bundesgesetz hinausgehende Befreiung von der Schweigepflicht dar, wurde sie danach von vielen Krankenhäusern als einengend empfunden. Im Zuge

106 Siehe JB 2020, 5.1.

107 Siehe Art. 5 des Gesetzes zur Anpassung datenschutzrechtlicher Bestimmungen in Berliner Gesetzen an die Verordnung (EU) 2016/679 (Berliner Datenschutz-Anpassungsgesetz EU) vom 12. Oktober 2020, GVBl. 2020, S. 807, 818 f.

108 Siehe § 24 Abs. 7 LKG.

der Digitalisierung sahen diese dringenden Bedarf nach einer Öffnung der restriktiven Regelung zur Inanspruchnahme von Dienstleister:innen.

Im Ergebnis eines ausführlichen Beratungsprozesses mit unserer Behörde entstand daraufhin ein Regelungsentwurf, der den Krankenhäusern neue Möglichkeiten für die Verarbeitung der Daten von Patient:innen eröffnet hätte, indem sie hierfür auch auf eigene Tochter- oder andere Konzernunternehmen bzw. diejenigen anderer Krankenhäuser hätten zurückgreifen können. Kurz vor Verabschiedung des entsprechenden Gesetzesentwurfs entschied das Abgeordnetenhaus jedoch, diese Regelung erst zwei Jahre später, im Oktober 2022, in Kraft treten zu lassen. Datenschutzrechtlich bedeutete dies, dass ohne eine spezielle Regelung im LKG, zumindest für den zweijährigen Übergangszeitraum, lediglich die allgemeinen Regelungen der DSGVO über die Auftragsverarbeitung zu beachten waren. Eine für die Patient:innen nachteilige Situation, die der Bundesgesetzgeber im Rahmen seiner Gesetzgebungskompetenz für andere Berufsgruppen vermieden hatte.

Doch es kam anders als in der Fassung des Gesetzes aus dem Jahr 2020 vorgesehen. Kurz vor dem Termin des Inkrafttretens im Oktober 2022 legten die Koalitionsfraktionen einen neuen Entwurf vor. Die im Oktober 2022 vorgenommene Reform hatte zum Ziel, einerseits den Krankenhäusern die Auftragsverarbeitung in größerem Umfang zu ermöglichen, als es die zeitweise ausgesetzte Regelung erlaubte, andererseits aber die Schutzlücke zu schließen, die insbesondere bei der sorglosen Inanspruchnahme global agierender Dienstleister:innen droht. Denn während in Deutschland über die Vorschriften zum Geheimnisschutz sichergestellt wird, dass Auftragsverarbeiter:innen den gleichen Schutz wie ihre Auftraggeber:innen zu gewährleisten haben und sich ansonsten strafbar machen würden,[109] gilt dies nicht mehr, wenn der Anwendungsbereich des deutschen Strafgesetzbuchs verlassen wird. Es muss daher von einer Regelung gewährleistet werden, dass nur solche Dienstleistungen in Anspruch genommen werden, bei deren Erbringung im Ausland die verarbeiteten Daten den gleichen strafrechtlichen und strafprozessualen Schutz erfahren wie in Deutschland. Zudem muss ein Zugriff von Mutterkonzernen aus Drittstaaten auf die Daten von Patient:innen ausgeschlossen werden, unabhängig davon, ob dieser für Zwecke der Produktfortentwicklung oder der Erfüllung von Anordnungen der Behörden von unsicheren Drittstaaten erfolgt.

109 Siehe § 203 Abs. 3, 4 Strafgesetzbuch (StGB).

Diese Erwägungen haben wir in der Beratung zu dem uns vorgelegten Gesetzesentwurf vorgetragen.

Die vom Abgeordnetenhaus nun verabschiedete Fassung der Vorschrift trägt den Datenschutzanforderungen Rechnung.[110] Gegenüber der Regelung, die im Oktober 2022 in Kraft treten sollte, ist die Vorschrift weitgehender, da sie auch Datenverarbeitungen zulässt, die nicht durch ein Krankenhaus oder ein Unternehmen eines Krankenhauskonzerns wahrgenommen werden. Indem so zwar europäische Cloudlösungen ermöglicht, jedoch gleichzeitig Unternehmen ausgeschlossen werden, die aufgrund des in Drittstaaten geltenden Rechts ggf. verpflichtet werden können, personenbezogene Daten an Behörden in Drittstaaten herauszugeben, wurde ein tragfähiger Kompromiss gefunden. Wir begrüßen es, dass die Regelung ausdrücklich vorsieht, dass die Verarbeitung nur durch Personen erfolgen darf, die nach dem für sie geltenden Recht einer dem deutschen Strafrecht entsprechenden Verschwiegenheitspflicht und einem Zeugnisverweigerungsrecht unterliegen.

Da Patient:innen meist keine Wahlmöglichkeit haben, ob sie in ein Krankenhaus gehen oder nicht, ist es notwendig, dass ihre Daten durch gesetzliche Regelungen ausreichend geschützt werden. Mit der Neufassung der Regelung für die Auftragsverarbeitung im LKG hat der Gesetzgeber die Bedingungen hierfür in einer Weise geregelt, die dem besonderen Schutzbedürfnis der Daten von Patient:innen Rechnung trägt. Wir werden die Umsetzung der Regelung in der Praxis beobachten.

5.2 Wo bleibt die Verantwortung? Umgang der Gesundheitsverwaltung mit Daten von in Impfzentren geimpften Personen

Für die Onlinebuchung von Terminen zur Schutzimpfung gegen SARS-CoV-2 in den vom Land Berlin eingerichteten Impfzentren nutzte die zuständige Senatsverwaltung für Wissenschaft, Gesundheit, Pflege und Gleichstellung auch im Jahr 2022 die Dienste eines Auftragsverarbeiters. Um online einen Impftermin zu vereinbaren, mussten die Bürger:innen ein Nutzerkonto bei dem Auftragsverarbeiter anlegen und

110 Siehe § 24 Abs. 7 LKG.

dafür ein Vertragsverhältnis mit diesem eingehen. Viele Bürger:innen wurden zudem nach der Impfung von einer E-Mail des Auftragsverarbeiters überrascht, in der ihnen mitgeteilt wurde, dass ihre persönlichen Impfdokumente (u. a. der ausgefüllte Anamnesebogen) in ihr Nutzerkonto hochgeladen worden seien. Beim Einsehen der im Nutzerkonto hochgeladenen Impfdokumente fanden einige Berliner:innen dann nicht ihre eigenen Dokumente, sondern die Dokumente anderer Personen vor.

Dass ein Auftragsverarbeiter die personenbezogenen Daten, die er für den Verantwortlichen verarbeiten soll, nicht zu eigenen Zwecken – konkret für ein zwischen ihm und den zu Impfenden einzugehendes Vertragsverhältnis – verarbeiten darf, haben wir der Gesundheitsverwaltung seit Ende des Jahres 2020 mehrfach dargelegt. Wir forderten sie wiederholt auf, Maßnahmen zu ergreifen, um einen datenschutzkonformen Zustand herzustellen. Dieser Aufforderung ist die Gesundheitsverwaltung nicht nachgekommen. Stattdessen hat sie den Vertrag mit dem Auftragsverarbeiter ohne die datenschutzrechtlich gebotene Anpassung verlängert. Folglich mussten Bürger:innen, die online einen Termin in einem Berliner Impfzentrum vereinbaren wollten, auch 2022 noch ein Nutzerkonto bei dem Auftragsverarbeiter einrichten und dafür ein Vertragsverhältnis mit diesem eingehen. Wir haben die Senatsverwaltung angehalten, dafür zu sorgen, dass die Vertragsverhältnisse mit dem Auftragsverarbeiter – sofern die Berliner:innen die Nutzerkonten nicht behalten möchten – automatisch beendet werden, sobald die Konten nicht mehr für die Vereinbarung von Terminen in Berliner Impfzentren erforderlich sind.

Zudem können wir keine Rechtsgrundlage dafür erkennen, dass die Gesundheitsverwaltung den geimpften Personen eine Kopie der Impfunterlagen in ihre für die Terminvereinbarung verwendeten Nutzerkonten hochladen lässt. Diese Verarbeitung ist im Zusammenhang mit der Impfung nicht zwingend erforderlich. Sofern den geimpften Personen ihre Gesundheitsdaten so zur Verfügung gestellt werden sollen, ist das nur mit deren ausdrücklicher Einwilligung und unter besonderen Sicherheitsvorkehrungen zulässig. Das sieht die Senatsverwaltung anders und hält an der von uns beanstandeten Datenverarbeitung fest. Die Risiken dieser nicht erforderlichen Datenverarbeitung haben sich in den uns vorliegenden Fällen, in denen die Dokumente falschen Personen zugeordnet waren, deutlich gezeigt.

Immerhin konnten wir erreichen, dass Daten von Personen, die einen vereinbarten Impftermin nicht wahrgenommen haben, nunmehr nach Aussage der Senatsverwaltung in regelmäßigen Abständen gelöscht werden. In Anbetracht der zuvor dargestellten Mängel bei der Gestaltung des Auftragsverarbeitungsverhältnisses, die die personenbezogenen Daten einschließlich der Gesundheitsdaten einer hohen Anzahl an Bürger:innen betreffen, wird uns das Thema weiterhin beschäftigen.

Personenbezogene Daten dürfen von Auftragsverarbeiter:innen nur auf Weisung der Verantwortlichen verarbeitet werden. Verstoßen Auftragsverarbeiter:innen hiergegen, müssen die Verantwortlichen sie dazu auffordern, einen datenschutzkonformen Zustand herzustellen, und nötigenfalls die Zusammenarbeit beenden. Wir haben die verantwortliche Gesundheitsverwaltung mehrfach auf dieses Erfordernis hingewiesen. Die Menschen erwarten gerade von der öffentlichen Hand, dass sie Daten sicherheitsorientiert, datensparsam und unter strenger Beachtung der Zweckbindung verarbeitet.

5.3 Erinnerung an den Termin – Ärztliche Praxen senden Nachrichten an falsche Personen

Auch in diesem Jahr erreichten uns viele Anfragen und Beschwerden von Patient:innen, die die Nutzung eines Terminverwaltungssystems eines Dienstleisters durch ärztliche Praxen betreffen. Der Dienstleister wird u. a. insofern als Auftragsverarbeiter für Ärzt:innen in der gesamten Bundesrepublik tätig, als er von den Praxen veranlasste Terminbestätigungen und -erinnerungen per SMS oder E-Mail an die Patient:innen versendet. In einigen Fällen kamen solche Nachrichten jedoch nicht bei den richtigen Patient:innen, sondern bei anderen Personen an.

Die Versendung von Terminnachrichten durch ärztliche Praxen an Patient:innen ist nur dann zulässig, wenn die Patient:innen ausdrücklich darin eingewilligt haben, dass ihre Telefonnummer oder E-Mail-Adresse für die Terminnachricht genutzt werden darf.[111] Neben der Einholung der Einwilligung der Patient:innen müssen die Praxismitarbeiter:innen darauf achten, dass sie die E-Mail-Adresse oder die Telefonnummer,

111 Siehe auch JB 2019, 6.3; JB 2021, 6.5.

an die die Terminnachricht geschickt werden soll, korrekt erfassen. Denn ein einziger kleiner Buchstaben- oder Zahlendreher kann dazu führen, dass eine Person, die weder mit der Praxis noch mit dem Termin etwas zu tun hat, an einen fremden Termin erinnert wird.

Da sich in den Nachrichten oft jedoch weder die Kontaktdaten der Praxis noch ein Link zur Abmeldung befanden, war es für die Empfänger:innen dieser Nachrichten nahezu unmöglich, bei der Praxis die Löschung ihrer E-Mail-Adresse oder ihrer Telefonnummer, die ohne ihre Einwilligung verarbeitet wurde, zu erreichen. Da einzig der Name des Dienstleisters aus den Nachrichten hervorging, wandten sich die betroffenen Personen mit der Bitte um Löschung ihrer E-Mail-Adresse bzw. Telefonnummer an dieses Unternehmen. Dieses teilte den betroffenen Personen – wie aus den bei uns eingereichten Beschwerden hervorgeht – jedoch weder die Kontaktdaten der tatsächlich verantwortlichen Praxis mit, noch informierte es die Praxis über die fehlgeleitete Terminnachricht und das entsprechende Löschungsersuchen der Empfänger:innen. Die betroffenen Personen, deren E-Mail-Adresse oder Telefonnummer unrechtmäßig verwendet wurde, werden durch diese Verfahrensweise sowohl von den ärztlichen Praxen, die solche Terminnachrichten veranlassen, als auch von dem als Auftragsverarbeiter eingesetzten Dienstleister schlicht im Regen stehen gelassen.

Ärztliche Praxen haben nicht nur die technischen und organisatorischen Maßnahmen zu treffen, die ein Versenden von Nachrichten an falsche Empfänger:innen verhindern. Sie sollten zudem einen Link zur Abmeldung in die Nachrichten integrieren, über den die Betroffenen die weitere Zusendung von Nachrichten ablehnen können.

5.4 Impfeinladungen der Gesundheitssenatorin an Minderjährige

Im Juli 2021 hatte die ehemalige Senatorin für Gesundheit, Pflege und Gleichstellung Einladungen zur Impfung gegen SARS-CoV-2 an minderjährige Berliner:innen versandt. Im Rahmen unserer Aufsichtstätigkeit erreichten uns zahlreiche Beschwerden von Personen, die sich gegen diese an ihre Kinder adressierten Einladungen richteten. Um eine Prüfung der Angelegenheit vornehmen zu können, baten wir die zuständige Senatsverwaltung um Beantwortung einer Reihe von Fragen. Die uns in

diesem Jahr schließlich mitgeteilten Antworten lassen erkennen, dass die inhaltlichen Anforderungen an gesetzlich vorgegebene Datenschutzinformationen nicht berücksichtigt wurden.

In dem Einladungsschreiben der Senatorin wurden die Vorgaben des Art. 14 DSGVO nicht beachtet. Da die personenbezogenen Daten (Namen und Anschriften der betroffenen Kinder und Jugendlichen), die der Senatsverwaltung vom Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) übermittelt worden waren,[112] zur Kommunikation mit den betroffenen Personen verwendet werden sollten, war die Gesundheitsverwaltung als Verantwortliche gehalten, spätestens zum Zeitpunkt der ersten Mitteilung ihren Informationspflichten gegenüber den betroffenen Personen nachzukommen.[113] Entsprechende Datenschutzinformationen sind den betroffenen Personen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.[114] Das gilt insbesondere für Informationen, die sich – wie hier – speziell an Kinder richten.[115]

In dem Schreiben der Senatorin wurden die adressierten Kinder und Jugendlichen weder präzise noch transparent noch in leicht zugänglicher Form über die Verarbeitung ihrer personenbezogenen Daten in Zusammenhang mit dem Schreiben informiert. Es gab vielmehr an keiner einzigen Stelle einen solchen Hinweis. Zudem waren keine Kontaktdaten des behördlichen Datenschutzbeauftragten der zuständigen Senatsverwaltung enthalten. Des Weiteren mangelte es auch an der Angabe der Rechtsgrundlage für die Datenverarbeitung, der Angabe zur Dauer der Speicherung der Daten, der Angabe der Quelle, aus der die Adressdaten stammen, sowie der Information über die Betroffenenrechte.

Wir erwarten, dass die Anforderungen an zu erteilende Datenschutzinformationen zukünftig beachtet werden. Dies haben wir der Senatsverwaltung mitgeteilt. Auf unsere Nachfrage, wann genau die Daten der betroffenen Personen gelöscht wurden, teilte uns diese mit, dass die Datensätze bereits nach der Einladungsaktion unter Berücksichtigung von Rückläufern gelöscht worden seien.

112 Gemäß § 34 des Bundesmeldegesetzes (BMG).
113 Siehe Art. 14 Abs. 3 lit. b DSGVO.
114 Art. 12 Abs. 1 Satz 1 1. Hs. DSGVO.
115 Art. 12 Abs. 1 Satz 1 2. Hs. DSGVO.

Werden personenbezogene Daten, die zur Kommunikation mit der betroffenen Person verwendet werden sollen, nicht bei der betroffenen Person selbst erhoben, sondern z. B. beim LABO, müssen die datenschutzrechtlichen Informationen spätestens zum Zeitpunkt der ersten Mitteilung an die betroffene Person erteilt werden. Insbesondere dann, wenn es sich bei der angeschriebenen Personengruppe um Minderjährige handelt, ist es erforderlich, dass besonders auf die Verständlichkeit der Informationen geachtet wird.

5.5 Offene Archivtüren im Krankenhaus

Durch eine nahe einer Klinik lebende Anwohnerin wurden wir darüber informiert, dass Unbekannte Patientenakten in ihren Briefkasten eingeworfen hätten. Parallel dazu erhielten wir eine Datenpannenmeldung der Klinik, wonach ca. 300 Patientenakten entwendet worden seien. Wir haben die Klinik dazu aufgefordert, die Sicherheit ihrer Akten sicherzustellen.

Jede medizinische Behandlung, ob ambulant oder stationär, muss dokumentiert werden. Diese Dokumentation dient sowohl als Informationsquelle für die laufende Behandlung als auch dem Nachweis des Vorgehens der behandelnden Ärzt:innen nach Abschluss der Behandlung. Akten aus der ambulanten Behandlung, um die es in diesem Vorfall ging, sind grundsätzlich für zehn Jahre aufzubewahren.[116] Im vorliegenden Fall hatte die Leitung der Klinik entschieden, die Akten länger aufzubewahren als vorgeschrieben – ein Vorgehen, das regelmäßig nicht als rechtmäßig einzustufen ist – und im Verlauf der Jahre anscheinend die Kontrolle über die Aktenarchivierung verloren. Weder wurden die Akten ausreichend geschützt aufbewahrt – die Türen zu den Archivräumen standen auch Unbefugten offen –, noch bestand eine Übersicht darüber, welche Akten sich konkret in welcher Anzahl an welchem Ort befanden.

So kam es zu einem unbefugten Zugriff unbekannten Ausmaßes. Eine unbefugte Person gelangte wiederholt in das Archiv und entnahm bündelweise Akten, die sie in Briefkästen und an mehreren Orten in der Nähe der Klinik verteilte. Die Akten wurden der Klinik vermutlich größtenteils wieder zurückgegeben. Genau beziffern kann die Klinik

116 § 630f Abs. 3 Bürgerliches Gesetzbuch (BGB).

jedoch nur die Anzahl der zurückgegebenen Akten. Wie viele Akten für immer verschwunden sind, ist ihr unbekannt. Für die betroffenen Personen ein unbefriedigender Zustand. Der Fall zeigt, welche Auswirkungen Missmanagement im Bereich der Archivierung von Akten haben kann. Wir haben die Klinik aufgefordert, die Sicherheit ihrer Akten zu gewährleisten, die Akten vollständig zu katalogisieren und Akten, für deren Aufbewahrung über die reguläre gesetzliche Frist hinaus kein konkreter Anlass besteht, zu vernichten.

Patientenakten sind wie alle Träger von Gesundheitsdaten besonders geschützt aufzubewahren. Die Aufbewahrung muss geordnet erfolgen, sodass stets nachvollzogen werden kann, welche Akten vorhanden und welche zu welchem Zeitpunkt zu vernichten sind. Die Frist zur Aufbewahrung soll sich, von begründeten Einzelfällen abgesehen, an den regulären gesetzlichen Aufbewahrungsfristen orientieren. Während der ganzen Aufbewahrungszeit ist die Vertraulichkeit der Akten durch effektive technische und organisatorische Maßnahmen sicherzustellen.

6 Integration und Soziales

6.1 Beratung zur Einwilligungs- und Schweigepflicht-entbindungserklärung bei Anträgen nach dem Schwerbehindertenrecht

Das Landesamt für Gesundheit und Soziales (LAGeSo) und die Senatsverwaltung für Integration, Arbeit und Soziales beabsichtigen, die Anträge nach dem Schwerbehindertenrecht zu überarbeiten. Hinsichtlich der Einwilligungs- und Schweigepflichtentbindungserklärung haben wir darauf hingewiesen, dass zu beachten ist, dass die Angaben im Antrag so präzise wie möglich sind, bevor entsprechende Auskünfte und Unterlagen bei Ärzt:innen und sonstigen Stellen eingeholt werden.

Beim Versorgungsamt gehen jährlich mehrere tausend Anträge nach dem Schwerbehindertenrecht[117] ein. Im Rahmen dieser Anträge, in denen es um die Feststellung des Vorliegens einer Behinderung und des Grads der Behinderung geht, werden besonders geschützte Gesundheitsdaten der Antragstellenden verarbeitet. Antragstellende müssen etwa Angaben zu gesundheitlichen Einschränkungen und Behandlungen machen. Wenn weitere Informationen zur Bearbeitung des Antrags notwendig sind, kann es erforderlich sein, Auskünfte und Unterlagen auch direkt bei den behandelnden Ärzt:innen anzufordern, um zu entscheiden, ob bzw. in welchem Umfang eine Schwerbehinderung vorliegt. Damit dies rechtlich möglich ist, holt das LAGeSo Einwilligungs- und Schweigepflichtentbindungserklärungen von den Antragstellenden ein.

Der Überarbeitung der Formulare war ein bereits 2018 begonnener Beratungsprozess mit unserer Behörde vorausgegangen. Es ging um die Frage, ob das LAGeSo der Ärzteschaft die Einwilligungs- und Schweigepflichtentbindungserklärungen ihrer Patient:innen vorzulegen hat. Dies ist im Regelfall nicht notwendig, es sei denn, die Ärzt:innen verlangen nach der Vorlage einer entsprechenden Erklärung.[118] Insbesondere wenn Unterlagen bei Krankenhäusern eingeholt werden, verlangen diese regelmäßig die Vorlage. Wichtig ist, dass das LAGeSo die Erklärungen dann auch zügig

117 Gemäß § 152 Sozialgesetzbuch Neuntes Buch (SGB IX).
118 Siehe JB 2018, 7.2.

zugänglich macht. Bei der Überarbeitung der derzeit verwendeten Formulare haben wir das LAGeSo beraten und darauf gedrängt, diese im Interesse der Transparenz möglichst präzise zu fassen.

Eine Einwilligung muss informiert, für den bestimmten Fall und freiwillig erteilt sowie die betroffene Person auf ihr Widerrufsrecht für die Zukunft hingewiesen werden.[119] Die betroffene Person muss sich darüber bewusst sein, welche Daten aufgrund ihrer Einwilligung verarbeitet werden dürfen und welche Personen und Stellen sie von der Schweigepflicht entbindet. Wird in der Schweigepflichtentbindungs- und Einwilligungserklärung auf eine namentliche Nennung aller Ärzt:innen verzichtet und insofern auf die getätigten Angaben im Antrag nach dem Schwerbehindertenrecht verwiesen, muss sichergestellt sein, dass die Angaben im Antrag so präzise wie möglich sind, bevor entsprechende Auskünfte bei den Ärzt:innen und Krankenhäusern eingeholt werden. Im Rahmen der Antragstellung ist daher von den zuständigen Sachbearbeiter:innen zu überprüfen, dass der Antrag von den Antragstellenden so genau und vollständig wie möglich ausgefüllt wurde. Pauschale Hinweise im Antrag auf einen Aufenthalt in einem bestimmten Krankenhaus ohne nähere Angaben reichen nicht aus, um von einer rechtswirksamen Einwilligungs- und Schweigepflichtentbindungserklärung auszugehen.

Damit das Versorgungsamt Auskünfte und Unterlagen bei den behandelnden Ärzt:innen und sonstigen Stellen im Rahmen eines Antrags nach dem Schwerbehindertenrecht erhalten kann, ist es erforderlich, von den Antragsteller:innen Einwilligungs- und Schweigepflichtentbindungserklärungen einzuholen. Dabei müssen die im Antrag getätigten Angaben zu behandelnden Ärzt:innen und Krankenhäusern so präzise wie möglich sein, damit klar ersichtlich ist, auf welche Auskünfte sich die Einwilligungs- und Schweigepflichtentbindungserklärung bezieht.

6.2 Berechtigungsnachweis statt Berlinpass

Wegen der Schließungen aufgrund der Corona-Pandemie konnten die Bezirksämter für einen gewissen Zeitraum keine Berlinpässe ausstellen, die den Empfänger:innen

119 Art. 7 Datenschutz-Grundverordnung (DSGVO) i. V. m. Art. 4 Nr. 11 DSGVO.

von Sozialleistungen die Inanspruchnahme von Vergünstigungen ermöglichen. Dies führte dazu, dass betroffene Personen bei Kontrollen im Öffentlichen Personennahverkehr (ÖPNV) und bei anderen Stellen ihren Leistungsbescheid zum Nachweis ihrer Berechtigung vorzeigen mussten. Nun soll der Berlinpass ganz abgeschafft und durch einen Berechtigungsnachweis sowie eine Trägerkarte der Berliner Verkehrsbetriebe (BVG) ersetzt werden.

Der Berlinpass ermöglicht Menschen mit geringem oder gar keinem Einkommen einen vergünstigten Zugang zu Bildung, Sport, Kultur und Nahverkehr. Dabei bildet der Berlinpass eine diskrete Möglichkeit des Berechtigungsnachweises, da ihm keine näheren Informationen zu den konkreten Berechtigungsgründen zu entnehmen sind. Solche Gründe müssen lediglich bei der Beantragung des Berlinpasses durch Vorlage der entsprechenden Sozialleistungsbescheide gegenüber den Bezirksämtern nachgewiesen werden.

Die Sozialleistungsbescheide enthalten besonders schützenswerte Daten wie den Berechtigungsgrund für Sozialleistungen, also bspw. Arbeitslosigkeit, den Asylbewerberstatus oder den Status als Opfer eines SED-Unrechts, und darüber hinaus eine Vielzahl personenbezogener Daten wie Name, Adresse, Geburtsdatum und Familienstand. Es ist nicht mit den Vorgaben des Datenschutzes zu vereinbaren, die berechtigten Personen dazu zu verpflichten, bei der Nutzung von vergünstigten Angeboten ihren Leistungsbescheid gegenüber Kontrollierenden im ÖPNV, Kassierenden an Theaterkassen etc. vorzulegen. Der Senat hatte im Jahr 2020 diejenigen Personen, die einen Berlinpass wegen der Pandemie nicht neu beantragen konnten, obwohl sie dazu berechtigt gewesen wären, darauf verwiesen, bei etwaigen Kontrollen den Leistungsbescheid vorzulegen. Betroffene beschwerten sich bei uns darüber und baten um datenschutzrechtliche Überprüfung.[120]

Wir sind diesen Beschwerden nachgegangen und haben uns an die BVG und die zuständige Senatsverwaltung für Integration, Arbeit und Soziales gewandt. Dabei sind wir insbesondere dem Argument der Senatsverwaltung entgegengetreten, dass betroffene Personen die Wahl hätten, zwischen dem Erwerb der regulären Angebote oder der Preisgabe ihrer Daten zu entscheiden, da diese auf die Vergünstigungen ja gerade

120 Siehe JB 2020, 12.1.

angewiesen sind. Datenschutz darf nicht vom Einkommen der betroffenen Personen abhängig sein.[121]

Im März wurden wir nun von der Senatsverwaltung über einen Beschluss des Senats informiert, nach dem der Berlinpass in seiner bisher bekannten Form abgeschafft und durch einen neuen Berechtigungsnachweis in Kombination mit einer BVG-Trägerkarte ersetzt werden soll. Wir wurden um Unterstützung bei der Entwicklung des neuen Berechtigungsnachweises gebeten. Dieser Bitte sind wir nachgekommen und haben die Senatsverwaltung im Laufe dieses Jahres beraten, wie der neue Nachweis diskret und datenschutzkonform ausgestaltet werden kann. Dieser soll künftig direkt durch die jeweils zuständigen Leistungsstellen ausgegeben werden und dabei nur den Namen, den Vornamen, das Geburtsdatum und die Dauer der Leistungsbewilligung aller anspruchsberechtigten Personen der jeweiligen Bedarfs- bzw. Haushaltsgemeinschaft enthalten. Aktenzeichen oder sonstige Kennnummern (wie etwa Wohngeldnummern) sollen nicht erkennbar sein. Schließlich soll der neue Berechtigungsnachweis mit Ausnahme des Jobcenters auch nicht die jeweilige Leistungsstelle, sondern lediglich das Land Berlin als zuständige Stelle ausweisen, sodass kein Rückschluss auf die Art der Leistung gezogen werden kann. Soweit das Jobcenter aufgrund bundesrechtlicher Regelungen ausgewiesen werden muss, soll dies in möglichst diskreter Form geschehen.

Zudem unterstützen wir die Senatsverwaltung und die BVG bei der Einführung der neuen BVG-Trägerkarte. Diese soll so gestaltet sein, dass sie nicht auf den ersten Blick von anderen Plastikkarten der BVG zu unterscheiden ist. Im Antragsprozess dürfen ausschließlich Daten erhoben werden, die zur Prüfung dessen erforderlich sind, ob die den Antrag stellende Person auch die auf dem Berechtigungsnachweis aufgeführte Person ist. Sowohl die Senatsverwaltung als auch die BVG haben darüber hinaus Sorge zu tragen, dass auch etwaig eingesetzte Dienstleister:innen datenschutzkonform handeln.

Angebote der öffentlichen und kulturellen Teilhabe für Sozialleistungsberechtigte müssen datenschutzkonform ausgestaltet sein. Da die Inanspruchnahme einer entsprechenden Berechtigung stets die Preisgabe besonders geschützter personen

121 Siehe auch unsere Pressemitteilung vom 1. März 2021, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210301-PM-berlinpass.pdf.

bezogener Daten voraussetzt, muss die Priorität auf dem Schutz eben dieser Daten liegen. Die Gefahr einer unter Umständen sogar öffentlichen Stigmatisierung der betroffenen Personen bei Inanspruchnahme der Angebote ist unter allen Umständen zu vermeiden.

6.3 Panne bei den Wahlen der Seniorenvertretung der Bezirke

Im Rahmen der Wahlen der Seniorenvertretung der Bezirke kam es in diesem Jahr zu einer erheblichen Panne, von der tausende Berliner:innen betroffenen waren. Uns erreichten dazu zahlreiche Beschwerden. Wir haben den Fall aufgeklärt und das verantwortliche Bezirksamt Reinickendorf verwarnt.

Das Gesetz zur Stärkung der Mitwirkungsrechte der Seniorinnen und Senioren am gesellschaftlichen Leben im Land Berlin[122] fördert die aktive Eigenbeteiligung der Senior:innen und zielt dabei auch auf eine Verbesserung der Solidargemeinschaft ab. Dazu werden als Gremien der Seniorenmitwirkung sog. Seniorenvertretungen auf bezirklicher Ebene gewählt. Dabei erlebten in diesem Jahr fast 70.000 Senior:innen in den Bezirken Friedrichshain-Kreuzberg, Pankow und Charlottenburg-Wilmersdorf eine Überraschung: Sie bekamen Anfang Januar Post aus dem Bezirk Reinickendorf, mit der sie zur dortigen Wahl der bezirklichen Seniorenvertretung eingeladen wurden. Viele der Betroffenen konnten dabei nicht nachvollziehen, aus welchen Gründen das Bezirksamt Reinickendorf im Besitz ihrer persönlichen Daten war und diese für das Einladungsschreiben nutzte, obwohl sie doch in einem ganz anderen Bezirk lebten.

Im Zuge der Verfolgung der bei uns eingereichten Beschwerden konnten wir den Fall aufklären: Auslöser der Panne war ein technischer Defekt an der Kuvertiermaschine des IT-Dienstleistungszentrums Berlin (ITDZ). Das ITDZ übernahm den Druck und den Versand der Wahlbenachrichtigungen zentral für die Bezirksämter und wurde dabei hinsichtlich der verwendeten personenbezogenen Daten als Auftragsverarbeiter für diese tätig. Am Abend des 6. Januar 2022 trat im ITDZ ein Problem mit der Kuvertiermaschine auf, sodass die Produktion unterbrochen werden musste. Beim Neustart

122 Berliner Seniorenmitwirkungsgesetz (BerlSenG).

der Produktion kam es dann zu einem Fehler in der Bedienung der Software zur Verknüpfung des Anschreibens mit den Adressdaten. Dies führte dazu, dass der Text des Bezirksamts Reinickendorf versehentlich mit den Adressdaten aus den Bezirken Friedrichshain-Kreuzberg, Pankow und Charlottenburg-Wilmersdorf verbunden wurde. Von insgesamt 910.000 versendeten Anschreiben waren so für den Bezirk Friedrichshain-Kreuzberg 19.123, für den Bezirk Pankow 25.000 und für den Bezirk Charlottenburg-Wilmersdorf 25.000 fehlerhaft. Zu einer Offenbarung der Daten gegenüber Dritten ist es nicht gekommen.

Wir haben gegenüber dem Fachbereich Senioren des Bezirksamts Reinickendorf, der die datenschutzrechtliche Verantwortlichkeit trägt, eine Verwarnung ausgesprochen. Grund hierfür war das Versäumnis, einen wirksamen Auftragsverarbeitungsvertrag mit dem ITDZ zu schließen. Der Fachbereich des Bezirks und das ITDZ haben zugesagt, dies nun unmittelbar nachzuholen und alle Maßnahmen zu ergreifen, um vergleichbare Fälle in Zukunft zu vermeiden.

Lassen öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung personenbezogene Daten durch IT-Dienstleister:innen wie das ITDZ verarbeiten, so ist hierin regelmäßig eine Auftragsverarbeitung zu sehen. Diese muss nach den Vorgaben der DSGVO zwingend rechtlich abgesichert werden,[123] was insbesondere durch einen Auftragsverarbeitungsvertrag erfolgen kann. Wird dies versäumt, liegt ein Datenschutzverstoß vor.

123 Art. 28 Abs. 3 DSGVO.

7 Wissenschaft und Forschung

7.1 Digitale Studieneignungstests – Wirklich eine Alternative zur Präsenz?

Auf den ersten Blick scheinen digitale Studieneignungstests eine unkomplizierte Lösung für die Auswahl von Bewerber:innen auf Studienplätze zu sein. Auf den zweiten Blick stellen sich bei der Durchführung solcher Tests mithilfe der eigenen Geräte der Bewerber:innen in deren Wohnungen jedoch erhebliche datenschutzrechtliche Fragen.

Wir haben die zuständige Senatsverwaltung für Wissenschaft, Gesundheit, Pflege und Gleichstellung sowie Vertreter:innen der Universitäten Anfang des Jahres zu den Anforderungen an digitale Studieneignungstests im Rahmen der Hochschulzulassung beraten. Die Idee einer der vertretenen Universitäten war, die ordnungsgemäße Durchführung eines Studieneignungstests mittels einer sog. Proctoring-Software zu überwachen, die auf den privaten Geräten der Bewerber:innen zu installieren ist. Zweck sollte es sein, Betrugsversuche frühzeitig zu erkennen; ein nachvollziehbares Anliegen.

Im Detail kamen allerdings erhebliche Datenschutzfragen auf: Während der Durchführung der digitalen Tests sollten im Rahmen einer Videoaufsicht Bild- und Tonaufnahmen der Testteilnehmer:innen angefertigt sowie eine automatisierte Überwachung der sonstigen auf den Geräten ausgeführten Programme vorgenommen werden. Die Software sollte hierfür u. a. den Browserverlauf auswerten und Konfigurationseinstellungen wie die Datenschutzeinstellungen im Browser verändern. In ihrem Funktionsumfang ähnelte die Software somit eher einer Schadsoftware (sog. Trojaner) als einer Software, die sich Nutzer:innen freiwillig installieren würden. Zudem stellte sich das Problem, dass mit dem Einsatz dieser Software auch biometrische Daten – wie Gesichtsmerkmale und Augenbewegungen – sowie weitere persönliche Daten – wie die Ausstattung der Wohnung oder die gespeicherten Dokumente auf den verwendeten Geräten – erfasst wurden. Wir haben thematisiert, dass der Einsatz einer solchen Software erhebliche Eingriffe in das Recht auf informationelle Selbstbestimmung mit sich bringt und deren rechtliche Zulässigkeit genau beleuchtet werden muss. Da eine entsprechende Rechts

grundlage in den hochschulrechtlichen Regelungen derzeit fehlt und im Übrigen aufgrund der erheblichen Eingriffstiefe auch mit den Anforderungen an Erforderlichkeit und Verhältnismäßigkeit einer solchen Datenverarbeitung nicht ohne Weiteres in Einklang zu bringen wäre, lässt sich die Durchführung entsprechender Tests unter Einsatz einer derartigen Software auf gesetzlicher Grundlage nicht abbilden.

Auch für die Einholung von Einwilligungen seitens der Studienbewerber:innen sahen wir ohne alternative Testangebote keine Möglichkeit. Einwilligungen können lediglich in Betracht kommen, wenn die Bewerber:innen konkret und transparent über die Datenverarbeitungen informiert werden. Dazu gehören auch die Kriterien der automatisierten Auswertungen, die sich aber ohne genaue Kenntnis der von der Software verwendeten Algorithmen nur schwer beschreiben lassen. Zudem kommt eine Einwilligung nur dann in Betracht, wenn diese freiwillig abgegeben wird. Neben der Möglichkeit zur Durchführung der Eignungstests unter Einsatz der Überwachungssoftware bedarf es daher einer alternativen Möglichkeit zur Präsenzabnahme der Tests auf hochschuleigenen Geräten.

Angesichts der erheblichen Eingriffe, die mit dem Einsatz solcher Softwareprodukte und der automatisierten Auswertungen verbunden wären, bedürfte es allerdings auch bei einer Einwilligungslösung zunächst einer gesetzlichen Regelung im Berliner Hochschulgesetz (BerlHG), die die rechtlichen Rahmenbedingungen der Datenverarbeitungsprozesse abbildet. Zudem ist davon auszugehen, dass die Regelungen des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) für einzelne Prozesse in jedem Fall eine Einwilligung erfordern werden, die nicht durch eine alternative Rechtsgrundlage im BerlHG ersetzt werden kann.[124] Wir haben der Senatsverwaltung für Wissenschaft, Gesundheit, Pflege und Gleichstellung und der betreffenden Universität vom Einsatz der Software bei der Durchführung von Studieneignungstests abgeraten. Die Beteiligten sind unserer Empfehlung gefolgt.

Sowohl in rechtlicher als auch in technischer Sicht wirft die Durchführung von Studieneignungstests, aber auch von digitalen Prüfungen unter Einsatz von Software zur Überwachung erhebliche Fragen auf. Angesichts der Anforderungen an ein datenschutzkonformes Verfahren ist es notwendig, genau auszuloten, inwieweit Bedarf

124 Siehe § 25 TTDSG.

in der Hochschulpraxis am Einsatz der Überwachungssoftware besteht, um dann die rechtlichen Rahmenbedingungen exakt zu definieren. Wir stehen hierfür gern beratend zur Verfügung.

7.2 Was wollte die Person genau? Und was nicht?

Viele Datenverarbeitungen werden damit gerechtfertigt, dass die betroffenen Personen (vermeintlich) in die Verarbeitung eingewilligt haben. Dabei prüfen die Verantwortlichen jedoch häufig nicht ausreichend, welche Verarbeitungen von einer Einwilligungserklärung wirklich erfasst und damit erlaubt sind und welche nicht.

Uns erreichte eine Beschwerde über eine Selbsthilfeorganisation, die Personen unterstützt, die in ihrer Kindheit problematischen Erziehungsmaßnahmen unterworfen waren. Neben Hilfsangeboten für diese Personen engagiert sich die Organisation auch im Bereich der wissenschaftlichen Erforschung dieser Erziehungsmaßnahmen und ihrer (psychischen) Folgen für die Betroffenen. Zu diesem Zweck führte die Organisation eine Liste mit Kontaktdaten betroffener Personen, die sich bereit erklärt hatten, für Befragungen zu Forschungszwecken zur Verfügung zu stehen.

Diese Kontaktdaten gab die Organisation an eine Universität weiter. Die Betroffenen sollten für die Erhebung von Daten im Rahmen einer Masterarbeit kontaktiert werden. Die Masterstudentin verschickte ihren Fragebogen dann an fast 200 Kontaktpersonen in einem offenen E-Mail-Verteiler. Damit hatten alle Empfänger:innen der E-Mail nicht nur Zugriff auf die E-Mail-Adressen der anderen, sie erhielten auch Kenntnis darüber, wer im Einzelnen ebenfalls von Erziehungsmaßnahmen betroffen war, wegen deren Folgen sich die Organisation engagiert. Die Masterstudentin legte damit besonders geschützte Daten der Betroffenen offen.

Einer der Betroffenen beschwerte sich bei uns über diesen Sachverhalt. Für die Offenlegung selbst war die Universität verantwortlich, die nicht in Berlin ansässig ist und damit nicht in unseren Zuständigkeitsbereich fällt. Wir haben jedoch überprüft, ob die Weitergabe der Kontaktdaten durch die Organisation rechtmäßig erfolgte. Hierfür bedarf es einer freiwilligen und unmissverständlichen Willensbekundung der betroffenen Personen. Diese hatten im Rahmen eines Fragebogens gegenüber

der Organisation folgende Erklärung abgegeben: „Ich bin einverstanden mit einer Kontaktaufnahme durch die Selbsthilfeorganisation und das Expertenteam zur wissenschaftlichen Aufarbeitung."

Diese Erklärung beinhaltet keine unmissverständliche Befugnis, dass die Daten auch an Personen oder Einrichtungen außerhalb der Organisation weitergegeben werden dürfen. Der Erklärung lässt sich diese Bedeutung auch nicht aus dem Zusammenhang entnehmen, denn im vorliegenden Fall stand in der Einleitung zu dem Fragebogen explizit, dass die Daten nicht an Dritte weitergegeben werden würden. Die Einwilligungserklärung bezog sich daher nur auf eine Kontaktierung durch die Organisation selbst. Damit lag der Organisation keine wirksame Einwilligung zur Weitergabe der Kontaktdaten an externe Einrichtungen vor. Schon die Weitergabe der Daten war folglich rechtswidrig. Wir haben gegenüber der Organisation deswegen eine Verwarnung ausgesprochen. Die Organisation reagierte auf unsere Ansprache und überarbeitete die Einwilligungserklärung.

Die Weitergabe von personenbezogenen Daten an Dritte birgt Risiken, da Verantwortliche damit die Kontrolle über die Daten aus der Hand geben und Betroffene nicht nachvollziehen können, an wen die Daten weitergegeben werden. Wenn die Weitergabe auf eine Einwilligung gestützt wird, müssen Verantwortliche prüfen, ob der Erklärung das Einverständnis der Betroffenen mit der Offenlegung ihrer Daten an Dritte tatsächlich unmissverständlich zu entnehmen ist.

8 Beschäftigtendatenschutz

8.1 Kameraüberwachung am Arbeitsplatz

Beschäftigte können einer Videoüberwachung am Arbeitsplatz kaum ausweichen, weshalb an das Betreiben derartiger Überwachung hohe Anforderungen zu stellen sind. Es darf in keinem Fall zu einer umfassenden Kontrolle der Tätigkeit der Beschäftigten kommen.

Grundsätzlich dürfen personenbezogene Daten von Beschäftigten nur verarbeitet werden, wenn dies unbedingt notwendig ist. Für die Rechtmäßigkeit einer Überwachung von Arbeitsplätzen mittels Videokameras müssen besondere Umstände vorliegen, wie bspw. eine hohe Gefahr für das Eigentum des Unternehmens. Zurückliegende Diebstähle oder Einbruchsversuche können dafür Anhaltspunkte sein. Doch selbst dann ist nicht jede Kameraüberwachung erlaubt: Grundsätzlich gilt, dass am Arbeitsplatz keine Totalüberwachung erfolgen darf. Insbesondere darf regelmäßig nicht der Produktionsbereich, an dem die Arbeit hauptsächlich ausgeübt wird, mittels Kameras dauerhaft überwacht werden. Auch Umkleiden, Pausenräume und Toiletten dürfen nicht videoüberwacht werden.

In einem von uns untersuchten Fall überwachte ein Unternehmen die Küche, die den zentralen Produktionsort darstellte, mit einer Kamera, die das Geschehen rund um die Uhr aufzeichnete. Das Unternehmen wurde auf das Verbot hingewiesen, woraufhin die Kamera tagsüber ausgeschaltet wurde und nun nur noch außerhalb der Betriebszeiten aktiv ist. In einem anderen Fall wurden zwar nicht die Arbeitsplätze selbst, dafür aber die Flure, über die die Büros der Beschäftigten zu erreichen waren, mit acht Kameras gefilmt. Begründet wurde die Kameraüberwachung mit zurückliegenden Einbruchsversuchen und Sachbeschädigungen. Es ist auch in Fällen wie diesen nicht ausreichend, wenn das Unternehmen lediglich über die Aufzeichnung mittels Videokameras informiert. Es muss zusätzlich überlegt werden, ob mildere Maßnahmen umgesetzt werden können, die den Sicherheitsinteressen des Unternehmens ebenso gerecht werden. Es wäre z. B. darüber nachzudenken, ob eine Alarmanlage ausreicht, um Einbrüche abzuwehren. Im vorliegenden Fall sollten die acht Kameras die

Nebeneingangstüren überwachen, die sich jeweils an den Enden der Flure befanden. Dadurch war es den Beschäftigten faktisch nicht möglich, den Kameras während der Arbeitszeit auszuweichen, denn der Zugang zum Arbeitsplatz wurde direkt überwacht. Hier empfahlen wir im Rahmen der Untersuchung, die Positionierung der Kameras und deren Einsatz an sich zu überdenken. Das Unternehmen entschied sich letztlich für ein neues Sicherheitskonzept, für das deutlich weniger Kameras notwendig sind, woraufhin ein Großteil der Kameras abgestellt und die nicht mehr benötigten Kameras abmontiert werden konnten.

Zu beachten ist, dass auch Kameraattrappen oder deaktivierte Kameras einen Eingriff in die Privatsphäre darstellen können. Die Rechtsprechung sieht insoweit aufgrund eines damit verbundenen Überwachungsdrucks einen Eingriff in die Persönlichkeitsrechte der betroffenen Person.[125] Auch wenn hier mangels Datenverarbeitung der Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) nicht eröffnet ist, kann ein zivilrechtliches Vorgehen gegen Kameranachbildungen oder inaktive Kameras möglicherweise zur Beseitigung führen.

Grundsätzlich muss über eine erforderliche Überwachung mittels Kameras umfangreich aufgeklärt werden. Eine Aufzeichnung sollte in der Regel nach 72 Stunden gelöscht werden. In Unternehmen, die einen Betriebs- oder Personalrat haben, ist dessen Zustimmung zu einer Kameraüberwachung erforderlich. Es muss zudem immer geprüft werden, ob geringere Eingriffe in die Persönlichkeitsrechte der Beschäftigten das Sicherheitsbedürfnis des Unternehmens ausreichend erfüllen. Zivilrechtlich können selbst bei deaktivierten Kameras oder Kameraattrappen Beseitigungs- bzw. Unterlassungsansprüche bestehen.

8.2 Löschung von Bewerbungsunterlagen

Bewerbungen für einen Arbeitsplatz beinhalten meist eine Menge persönlicher Daten. Verständlicherweise verlangen darum viele Bewerber:innen nach Abschluss des Bewerbungsverfahrens eine Löschung ihrer Daten bzw. die Vernichtung ihrer Unterlagen. Wird die Bewerbung zurückgezogen, ist die Situation einfach: Es besteht keine

125 Siehe Bundesgerichtshof (BGH), Urteil vom 16. März 2010, VI ZR 176/09; Landgericht (LG) Berlin, Urteil vom 14. August 2018, 67 S 73/18.

Rechtsgrundlage für eine weitere Verarbeitung der Daten, die Bewerbungsunterlagen sind unverzüglich zu löschen.

Im Fall einer Zurücknahme der Bewerbung empfiehlt es sich, die Löschung der Daten zu beantragen. Auf unserer Website befindet sich ein Musterformular mit der Aufforderung, die personenbezogenen Daten zu löschen.[126] Zu beachten ist dabei, dass die verantwortliche Stelle eine Frist von einem Monat zur Beantwortung des Löschauftrags hat.

Etwas komplizierter ist die Situation, wenn die Bewerbung nicht zurückgenommen, sondern von der Behörde oder dem Unternehmen abgelehnt wurde. Bewerber:innen könnten gegen die Ablehnung klagen. Der Behörde bzw. dem Unternehmen muss dann die Möglichkeit eingeräumt sein, sich mit rechtlichen Mitteln gegen eine solche Klage zu verteidigen. Dazu dürfen die Bewerbung und auch eine Dokumentation des Bewerbungsverfahrens einschließlich der Auswertung aufbewahrt werden. Es gilt dafür eine Frist von bis zu sechs Monaten. Diese ergibt sich aus den jeweils einschlägigen Rechtsmittelfristen des Allgemeinen Gleichbehandlungsgesetzes (AGG) und des Arbeitsgerichtsgesetzes (ArbGG) sowie etwaigen Verzögerungen durch die Zustellung einer Klage.

Teilweise wird aber auch seitens der Arbeitgeber:innen eine viel umfangreichere Speicherung beabsichtigt: In einem von uns geprüften Fall beauftragte ein Unternehmen eine Recruiting-Agentur mit der Durchführung des Bewerbungsprozesses. Das kann im Rahmen einer Auftragsverarbeitung grundsätzlich in Ordnung sein. In dieser Situation verlangte die Agentur von den Bewerber:innen jedoch, dass diese einer unbegrenzten Speicherung der Unterlagen für weitere Bewerbungsverfahren zustimmen, andernfalls könne ihre Bewerbung nicht berücksichtigt werden. Ein Bewerber zog daraufhin seine Bewerbung zurück und legte bei uns Beschwerde ein. Das beauftragende Unternehmen trennte sich aufgrund unserer Intervention sehr schnell von der Agentur, die rechtswidrig Beschäftigtendaten speichern wollte.

In einem anderen uns vorliegenden Fall wunderte sich ein Beschwerdeführer, warum er in einem Bewerbungsverfahren auf eine vermeintliche Gehaltsvorstellung angesprochen wurde, die er nicht übermittelt hatte. Nachdem Bekannte ihn darauf aufmerksam

126 Abrufbar unter https://www.datenschutz-berlin.de/buergerinnen-und-buerger/selbstdatenschutz/ueberpruefung-ihrer-daten.

gemacht hatten, dass seine Adresse inklusive Telefonnummer im Internet veröffentlicht sei, ging er der Sache auf den Grund: Über die Ergebnisanzeige mehrerer Suchmaschinen waren Bewerbungsunterlagen von ihm auf der Website eines Unternehmens vollständig einsehbar, bei dem er sich im Jahr 2019 beworben hatte. Das Unternehmen hat die Bewerbungsunterlagen nach unserem Einschreiten zwar von der eigenen Website entfernt, die Daten waren aber über den Zwischenspeicher der Suchmaschinen noch eine Weile abrufbar. In diesem Zusammenhang ist es hilfreich zu wissen, dass die verantwortliche Stelle laut Rechtsprechung des Kammergerichts (KG) Berlin auch für die Löschung der noch in den Suchmaschinen befindlichen Daten verantwortlich gemacht werden kann.[127]

Ist eine Speicherung von Bewerbungsdaten nicht mehr erforderlich, müssen diese gelöscht werden. Bei Löschbegehren der Bewerber:innen kommt es in der Praxis oft zu Problemen, weil Unternehmen die Monatsfrist zur Beantwortung des Löschauftrags überschreiten. Andererseits erreichen uns viele Eingaben, bei denen die Betroffenen die Monatsfrist nicht abgewartet haben, die das Unternehmen zur Beantwortung des Löschauftrags hat. Hier weisen wir darauf hin, dass die Frist zunächst abzuwarten ist.

8.3 Notwendigkeit eines neuen Beschäftigtendatenschutzgesetzes

Die gesellschaftlichen Veränderungen im Zusammenhang mit der zunehmenden Digitalisierung werfen auch im Umgang mit Beschäftigtendaten Fragen auf, die durch den Gesetzgeber beantwortet werden müssen.

Ein eigenes Beschäftigtendatenschutzgesetz ist bereits seit Jahrzehnten in der Diskussion. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat zu Beginn des Jahres die Forderung nach einem neuen Beschäftigtendatenschutzgesetz wiederholt.[128] Der gesellschaftliche Wandel durch die Digitalisierung beeinflusst die Beschäftigungsverhältnisse in vielen Punkten und legt

127 Siehe KG Berlin, Urteil vom 27. November 2009, 9 U 27/09.

128 Entschließung der DSK vom 29. April 2022: „Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt'!", abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk.

Schwachstellen beim Schutz personenbezogener Daten von Beschäftigen offen. Bei vielen der aktuell aufkommenden Problemstellungen besteht Rechtsunsicherheit; offene Fragen werden im Zweifelsfall nicht zugunsten der Beschäftigen ausgelegt. Problematisch ist, wenn Beschäftigte aus Angst vor beruflichen Nachteilen Verstöße gegen ihr informationelles Selbstbestimmungsrecht während des Arbeitsverhältnisses nicht geltend machen. Hinweise auf Verstöße erreichen uns oft erst nach Beendigung des Arbeitsverhältnisses und somit zeitlich stark verzögert.

Von großer praktischer Bedeutung für den Schutz von Beschäftigtendaten ist die Verlagerung der Arbeit ins Homeoffice. Diese Umstrukturierung hat jedoch nicht zur Folge, dass der Bedarf der Behörden und Unternehmen an einer Kontrolle der Arbeitsabläufe abnimmt. Vielmehr erreichen uns Beratungsanfragen, wonach das Interesse an Überwachung derart weit reicht, dass selbst eine umfassende Inspektion der Arbeitsplätze in den Wohnungen der Beschäftigten noch als angemessen erachtet wird. Zudem werden nicht allen Beschäftigten gesonderte Geräte für die Arbeit im Homeoffice zur Verfügung gestellt. Nicht selten wird dort an privaten Geräten gearbeitet, weshalb nicht nur der Datenbestand aus dem Arbeitsverhältnis, sondern ggf. auch die Privatsphäre der Beschäftigten jenseits des Beschäftigungsverhältnisses betroffen ist, selbst wenn die Kontrolle der Arbeitgeber:innen nur auf digitaler Ebene erfolgt.

Bei den Beschwerden von Beschäftigten, die wir erhielten, spielte immer wieder der Umgang mit personenbezogenen Daten auf Bewerbungsportalen im Internet eine Rolle, auf denen die Betroffenen ihre Daten zuvor veröffentlicht hatten. Auch der Einsatz von Künstlicher Intelligenz wird bei der Vermittlung von Beschäftigungsverhältnissen zukünftig an Bedeutung gewinnen. Dadurch wird ermöglicht, sehr viele Daten zur Anbahnung eines Arbeitsverhältnisses zu verarbeiten und personenbezogene Einschätzungen, Prognosen, Profile zu erstellen, die für die Betroffenen ggf. intransparent bzw. schwer nachvollziehbar sind, was zu tiefen Eingriffen in die Privatsphäre der potenziell Beschäftigten führen kann.

Gesellschaftlicher Wandel und Digitalisierung stellt die Arbeitswelt allgemein und besonders den Beschäftigtendatenschutz vor große Herausforderungen. Hier sind spezifische gesetzliche Regelungen in Form eines neuen Beschäftigtendatenschutzgesetzes notwendig.

8.4 Besonders schützenswerte Daten in Personalakten

Auch in Beschäftigungsverhältnissen gilt, dass besonders schützenswerte personenbezogene Daten nur in eng begrenzten Ausnahmefällen verarbeitet werden dürfen. Zu diesen Daten gehören Informationen, die bspw. Rückschlüsse auf den Gesundheitsstatus oder die politische Überzeugung von Beschäftigten zulassen oder Anhaltspunkte für religiöse Diffamierung oder rassistische Verfolgung bieten können. Auch Informationen über Gewerkschaftszugehörigkeiten unterliegen diesem besonderen Schutz.[129]

Beamt:innen des Landes Berlin können nach der Sonderurlaubsverordnung (SUrlV) für besondere Zwecke Urlaubstage beantragen. Als besondere Anlässe gelten u. a. staatspolitische, kirchliche, fachliche, gewerkschaftliche und sportliche Zwecke. Nach Beantragung des Sonderurlaubs beim Landesverwaltungsamt (LVwA) werden die Unterlagen der Personalakte der antragstellenden Person beigefügt. Dadurch können personenbezogene Daten zur Religions-, Partei- oder Gewerkschaftszugehörigkeit Eingang in die Personalakte finden.

Hierzu lag uns eine Beschwerde vor, die wir zum Anlass nahmen, die Praxis des LVwA zu überprüfen. Tatsächlich war es üblich, den Personalakten auch besonders geschützte personenbezogene Daten im Zusammenhang mit einem Sonderurlaub beizulegen. Die Verarbeitung dieser besonderen Kategorien personenbezogener Daten ist nur in engen Grenzen zulässig. Aus den Anforderungen der SUrlV, wonach Sonderurlaub nur in bestimmten Fällen zu gewähren ist, ergibt sich im Rahmen der Prüfung des Antrags zwar die Notwendigkeit, im Zweifelsfall auch besonders schützenswerte Daten der Beschäftigten zu verarbeiten. Daraus kann jedoch nicht geschlussfolgert werden, dass diese Daten auch dauerhaft in der Personalakte gespeichert werden dürfen.

Über die Prüfung der Voraussetzungen für den Sonderurlaub hinaus gibt es keine Rechtsgrundlage für die Speicherung von besonders geschützten Daten in der Personalakte. Wie auch sonst im Beschäftigtendatenschutz ist hier zu prüfen, ob die Datenverarbeitung erforderlich ist.[130] Aufgrund der zeitlichen Begrenzung des Sonderurlaubs ist es notwendig, die Bewilligung zur Akte zu speichern, um nachvollziehbar

129 Art. 9 Abs. 1 DSGVO.
130 Hier nach § 14 Berliner Datenschutzgesetz (BlnDSG) i. V. m. Art. 9 Abs. 2 DSGVO.

zu machen, in welchem Umfang bereits Sonderurlaub gewährt wurde. Nicht notwendig sind dafür jedoch die Begründungen bzw. die Nachweise für die Begründung des jeweiligen Sonderurlaubs, anhand derer Rückschlüsse auf die besonders geschützten Daten gezogen werden können.

Im Laufe unserer Prüfung hat die Senatsverwaltung für Finanzen in ihrer Funktion als Fachaufsicht für das LVwA angekündigt, zukünftig im Zusammenhang mit der Beantragung von Sonderurlaub keine besonders geschützten personenbezogenen Daten mehr in die Personalakten zu übernehmen und ein Löschungskonzept für bestehende Akten zu erarbeiten.

In der Personalakte dürfen Informationen über den zeitlichen Umfang des bewilligten Sonderurlaubs gespeichert werden, nicht jedoch Informationen über die Art des Urlaubs oder über die jeweilige Begründung, sofern diese Rückschlüsse auf besonders geschützte personenbezogene Daten ermöglicht.

9 Wohnen

9.1 Doppelter Gesundheitsdaten-Exzess bei der Versammlung einer Wohnungseigentümergemeinschaft

Eine Hausverwaltung hatte für die Versammlung einer Wohnungseigentümergemeinschaft eine Liste für die Teilnehmer:innen ausgelegt, auf der auch der Impfstatus angegeben werden sollte. Ein Teilnehmer hat diese Liste fotografiert.

Die aufgrund der pandemischen Situation eingeführten Maßnahmen zur Kontaktbeschränkung sahen in vielen Fällen auch eine Anwesenheitsdokumentation vor. Die Infektionsschutzmaßnahmenverordnung (heute Basisschutzmaßnahmenverordnung) des Landes Berlin enthielt zudem Einschränkungen für den Besuch von öffentlichen Orten oder Zusammentreffen in größeren Gruppen für Personen, die keinen hinreichenden Impfschutz gegen COVID-19 nachweisen konnten.

Die Einrichtungen, Gastronomiebetriebe und auf andere Weise für die Organisation von Menschenansammlungen verantwortlichen Stellen beschritten unterschiedliche Wege zur Dokumentation von Anwesenheiten. Zweck war jeweils, eine anschließende Nachverfolgung von ggf. auftretenden Infektionen zu ermöglichen. Aus dieser Motivation heraus entschied sich eine Hausverwaltung, die für die Durchführung einer Versammlung der Wohnungseigentümergemeinschaft ausliegende Liste der Teilnehmer:innen um ein Abfragefeld zum Impfstatus der teilnehmenden Personen zu erweitern. Dort sollte eingetragen werden, ob und in welchem Umfang Teilnehmer:innen gegen eine COVID-19-Infektion geimpft seien. Dem kamen die Teilnehmer:innen in Teilen auch nach. Eines der Mitglieder fotografierte diese Liste nach Ende der Versammlung.

Die Verarbeitung von personenbezogenen Daten mittels einer Liste der teilnehmenden Personen ist bei Versammlungen von Wohnungseigentümergemeinschaften üblich und dient dem Zweck, nachzuweisen, wer tatsächlich an einer Versammlung teilgenommen und ggf. welche Stimmrechte ausgeübt hat. Wie viele andere Datenverarbeitungen innerhalb von Wohnungseigentümergemeinschaften ist eine solche zweckgebundene

Dokumentation nicht zu beanstanden. Bei den Daten zum Impfstatus handelt es sich jedoch um Gesundheitsdaten. Diese Daten stehen in keinem Zusammenhang mit der Durchführung des Verwaltungsauftrags, den die Hausverwaltung von der Wohnungseigentümergemeinschaft erhalten hat, bzw. mit der Anwesenheitsdokumentation zur Nachverfolgung von Infektionen. Ihre Verarbeitung unterliegt zudem besonderen Hürden, da es sich um besonders schützenswerte Angaben über eine Person handelt.[131] Die Abfrage durch die Hausverwaltung fand also keine Rechtsgrundlage – weder im Gesetz noch in der Infektionsschutzmaßnahmenverordnung – und war mangels Einwilligung der betroffenen Personen in die Verarbeitung ihrer Gesundheitsdaten rechtswidrig.

Innerhalb einer Wohnungseigentümergemeinschaft bestehen für Mitglieder aufgrund der engen vertraglichen Bindung naturgemäß vergleichsweise weitreichende Einsichtsrechte in die Unterlagen der Gemeinschaft, die auch Auskunft über die anderen Mitglieder geben können. Insofern besteht häufig bei der Übermittlung von Kopien von Eigentumsanteilslisten, Abrechnungen o. Ä. ein Recht der Mitglieder auf Erhalt dieser Informationen. Das Abfotografieren einer Teilnehmendenliste durch eines der Mitglieder der Gemeinschaft kann so auch gerechtfertigt sein. Dies gilt allerdings nur, soweit die Liste ausschließlich Daten enthält, die für die Durchführung des Vertrags der Wohnungseigentümergemeinschaft erforderlich sind. Dies war bei der in Rede stehenden Liste nicht der Fall, sodass auch das Abfotografieren der Liste einen datenschutzrechtlichen Verstoß darstellte. Die handelnde Hausverwaltung und das betreffende Mitglied der Wohnungseigentümergemeinschaft wurden von uns über die Rechtslage aufgeklärt und auf ihr Fehlverhalten hingewiesen. Die Löschung der unrechtmäßig erhobenen bzw. abfotografierten Daten wurde veranlasst.

Auch umfangreiche Einsichtsrechte im Rahmen enger vertraglicher Bindungen einer Wohnungseigentümergemeinschaft rechtfertigen grundsätzlich nicht die Abfrage von Gesundheitsdaten durch eine Hausverwaltung und erst recht nicht die Verarbeitung von diesen Daten durch ein Mitglied der Gemeinschaft. Unrechtmäßig erlangte Daten sind umgehend zu löschen und diese Löschung ist den Betroffenen auch zu bestätigen.

131 Siehe Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO).

9.2 Wohneigentum vs. Privatsphäre – Was geht, was nicht?

Der Beitritt zu einer Wohnungseigentümergemeinschaft verursacht weitgehende Einsichtsrechte der anderen Gemeinschaftsmitglieder in die eigenen Daten. Wird eine Hausverwaltung mit den Geschäften der Gemeinschaft betraut, so ist sie eine eigenständige verantwortliche Stelle mit allen entsprechenden Rechten und Pflichten.

Wohnungseigentümergemeinschaften werden vertraglich zwischen den Mitgliedern begründet, häufig werden mit der Verwaltung des gemeinsamen Eigentums Dritte beauftragt. Viele Hausverwaltungen haben sich sogar auf die Verwaltung von Wohneigentum im Auftrag von Wohnungseigentümergemeinschaften spezialisiert. Die Vorschriften des Gesetzes über das Wohnungseigentum und das Dauerwohnrecht (WEG) enthalten zahlreiche spezifisch auf diese Wohnform ausgerichtete Regelungen.

Zunächst steht jedem Mitglied ein weit gefasster Anspruch auf Einsicht in die Unterlagen der anderen Mitglieder zu. Dies folgt in erster Linie aus dem WEG: Innerhalb von Wohnungseigentümergemeinschaften ist zur Überprüfung eigener Abrechnungen regelmäßig Einsicht auch in die Unterlagen der übrigen Mitglieder erforderlich.[132] Dieses Einsichtsrecht umfasst bspw. auch Teilnehmendenlisten von Versammlungen der Gemeinschaft, sämtliche Abrechnungsunterlagen mit Bezug auf die Gemeinschaftsangelegenheiten oder Angaben über Hausgeldrückstände einzelner Mitglieder. Über den gemeinsam geschlossenen Vertrag können auch noch weitergehende Einsichtsrechte vereinbart werden.

Mit der fortschreitenden Digitalisierung verlagern sich Akteneinsichten mehr und mehr ins Internet, Wohnungseigentümergemeinschaften sind da keine Ausnahme: Portale, über die die Hausverwaltungen ihre Informationspflichten hinsichtlich der Angelegenheiten der Gemeinschaft online erfüllen können, sind weit verbreitet. Auch das proaktive Bereitstellen von Unterlagen über den Postversand war schon Gegenstand von Eingaben; beides ist grundsätzlich datenschutzrechtlich nicht zu beanstanden. So verarbeitet eine Hausverwaltung personenbezogene Daten von Mieter:innen oder Eigentümer:innen auf Grundlage von Art. 6 Abs. 1 Satz 1 lit. b DSGVO. Hiernach dürfen diejenigen Daten verarbeitet werden, die zur Erfüllung bspw. eines Mietvertrags oder

132 Siehe § 28 WEG.

eines Vertrags von Wohnungseigentümergemeinschaften erforderlich sind. Betreiber:innen von Portalen für die Verwaltung und Kommunikation mit den Bewohner:innen der verwalteten Wohnungen sind als Auftragsverarbeiter:innen für die jeweilige Hausverwaltung einzubinden. Die digitale Bereitstellung oder auch der postalische Versand von Listen und Abrechnungen beinhalten grundsätzlich keinen weitergehenden Eingriff in die Rechte der betroffenen Personen, als ohnehin durch das Recht auf Einsicht der anderen Mitglieder der Gemeinschaft gesetzlich vorgesehen ist, vorausgesetzt die erforderlichen technisch-organisatorischen Maßnahmen zum Schutz der Daten werden eingehalten.

Mitglieder von Wohnungseigentümergemeinschaften haben hingegen keinen Anspruch auf den Erhalt personenbezogener Daten der übrigen Mitglieder, wenn hiermit nicht die Erfüllung des Vertrags der Gemeinschaft bezweckt ist. Wenn im Vertrag bspw. nicht explizit angegeben ist, dass E-Mail-Adressen auch von Personen, die nicht der Hausverwaltung bzw. dem Gemeinschaftsbeirat angehören, genutzt werden dürfen, besteht auch für die übrigen Mitglieder kein Anspruch auf den Erhalt der E-Mail-Adressen. Auch Beiratsmitglieder dürfen die Adressen ausschließlich zur Erfüllung ihrer Aufgaben innerhalb dieses Gremiums nutzen. Gleiches gilt bspw. für die Telefonnummern anderer Mitglieder; es existiert kein Recht auf Kommunikation mit allen Mitgliedern außerhalb der hierfür gesetzlich und vertraglich vorgesehenen Gremien.

Häufig wird unterschätzt, wie weit die Verpflichtung zur Offenlegung eigener Verbrauchs- oder Abrechnungsdaten innerhalb einer Wohnungseigentümergemeinschaft reicht. Der Einsatz von Onlineportalen zur Verwaltung von Wohneigentum ist grundsätzlich nicht zu beanstanden, wenn die erforderliche Datensicherheit gewährleistet ist.

10 Wirtschaft

10.1 Benutzungsfreundliche Datenauskunft: Bitte vollständig und verständlich!

Regelmäßig wenden sich Menschen an uns, deren Auskunftsersuchen unvollständig oder unverständlich beantwortet wurden. Dabei ist das Recht auf Datenauskunft das Herzstück der Betroffenenrechte: Durch die Auskunft sollen betroffene Personen in die Lage versetzt werden, die Verarbeitung der sie betreffenden Daten nachvollziehen und die Rechtmäßigkeit der Datenverarbeitung überprüfen zu können.[133] Das Recht auf Datenauskunft ist auch deshalb von zentraler Bedeutung, weil es die gezielte Ausübung weiterer Betroffenenrechte ermöglicht, etwa den Anspruch auf Berichtigung oder Löschung der Daten.[134] Umso wichtiger ist es, dass die Datenauskunft vollständig erteilt wird und dabei präzise, transparent, verständlich und leicht zugänglich ist.

Eine vollständige Auskunft enthält nicht etwa nur die Stammdaten aus der Kundendatenbank, also Name, Adressdaten und Geburtsdatum, sondern sämtliche zur Person gespeicherte Daten, wie u. a. Bestellhistorie, Bonitätskennzahlen, Log-in-, Klick- und Browserdaten oder die Kommunikation mit der betroffenen Person. Darüber hinaus sind der betroffenen Person weitere Informationen (sog. Metainformationen) mitzuteilen, also z. B. woher die Daten stammen, an wen sie weitergegeben wurden oder wie lange sie gespeichert werden.[135] Sollten einzelne Punkte im konkreten Fall nicht einschlägig sein, etwa weil keine Weitergabe der Daten erfolgt ist, dürfen die Verantwortlichen nicht einfach dazu schweigen, sondern müssen eine entsprechende Negativauskunft erteilen.[136] Anderenfalls wäre für die betroffene Person nicht erkennbar, ob tatsächlich keine entsprechende Datenverarbeitung stattfand oder die Datenauskunft lediglich unvollständig ist.

133 Siehe Erwägungsgrund (EG) 63 Datenschutz-Grundverordnung (DSGVO).
134 Siehe Art. 16, 17 DSGVO.
135 Siehe Art. 15 Abs. 1 lit. a bis h DSGVO; Art. 15 Abs. 2 DSGVO.
136 Bspw. in Form von: „Ihre Daten wurden nicht weitergegeben."

Manche Unternehmen verweisen bei der Erteilung der Datenauskunft einfach auf die Ausführungen in ihrer Datenschutzerklärung. Ein solcher Verweis kann die individuelle Auskunft allerdings nicht ersetzen. Während die Datenschutzerklärung der Erfüllung allgemeiner Informationspflichten vor einer Datenverarbeitung dient,[137] müssen die Angaben bei einem Auskunftsersuchen auf die betroffenen Personen zugeschnitten sein. Die unveränderte Übernahme von Textteilen aus der Datenschutzerklärung in eine Datenauskunft ist nur dann möglich, wenn die Informationen gleich bleiben, wie dies etwa im Hinblick auf das Beschwerderecht bei einer Aufsichtsbehörde der Fall ist.[138]

Eine Datenauskunft ist in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.[139] Für Verantwortliche, die zahlreiche personenbezogene Daten verarbeiten, ist dies nicht immer leicht umzusetzen. Bei einer unübersichtlich großen Datenmenge können Verantwortliche im Einzelfall abgestuft vorgehen, d. h. zunächst die für ihre Durchschnittsadressat:innen relevantesten Daten mitteilen und zugleich anfragen, welcher inhaltliche Detaillierungsgrad der weiteren Daten gewünscht ist. Diese Form der Auskunftserteilung darf jedoch nicht zu einer Beschränkung oder Erschwerung des Auskunftsrechts führen.

Wenn die Datenauskunft interne Abkürzungen oder Codes enthält, kann es schwierig sein, diese zu verstehen. Hier müssen die Verantwortlichen mindestens ergänzende Informationen bereitstellen. Diese dürfen allerdings nicht dazu führen, dass die betroffene Person erst mühsame Übersetzungsarbeit leisten muss, um die Datenauskunft verstehen und überprüfen zu können. Zur Verständlichkeit gehört auch die visuelle Form der Darstellung einer Datenauskunft. Bei einem von uns geprüften Verantwortlichen konnten die Informationen in der Datenauskunft aufgrund der gewählten Darstellungsweise mit vielen Tabellenspalten und einer minimalen Schriftgröße weder digital als Ganzes lesbar betrachtet noch im regulären DIN A4-Format ausgedruckt werden. In diesem Fall konnten wir das Unternehmen davon überzeugen, eine alternative Form der Darstellung zu wählen.

137 Siehe Art. 13 bzw. Art. 14 DSGVO.
138 Siehe Art. 15 Abs. 1 lit. f DSGVO.
139 Art. 12 Abs. 1 Satz 1 DSGVO.

Datenauskünfte müssen vollständig sein und für die betroffene Person verständlich aufbereitet werden. Der Europäische Datenschutzausschuss (EDSA) hat einen Entwurf zu Leitlinien zum Recht auf Auskunft veröffentlicht, die nach ihrer Fertigstellung zusätzliche Klarheit für Unternehmen und Betroffene bieten.[140]

10.2 Einwand des rechtsmissbräuchlichen Auskunftsersuchens

Einige Unternehmen verweigern die Auskunftserteilung gegenüber betroffenen Personen. Sie argumentieren, dass keine Pflicht zur Auskunftserteilung und auf Herausgabe von Datenkopien, bspw. in Form von Telefonaufzeichnungen, bestehe, wenn die betroffene Person mit der Geltendmachung ihres Rechts auf Auskunft datenschutzfremde Zwecke verfolge. Uns erreichten mehrere Beschwerden, in denen Unternehmen den Einwand des rechtsmissbräuchlichen Verhaltens[141] geltend gemacht und vorgebracht haben, dass eine Auskunftserteilung nicht erfolgen müsse.

In einem uns vorliegenden Fall bestand zwischen einer Beschwerdeführerin und einem Unternehmen eine Streitigkeit darüber, ob ein telefonisch vereinbarter Vertrag wirksam zustande gekommen bzw. gekündigt worden sei. Die Beschwerdeführerin machte das Recht auf Auskunft gegenüber dem Unternehmen geltend und verlangte in diesem Zusammenhang auch die Aushändigung einer Kopie der Telefonaufzeichnung. Das Unternehmen verweigerte der Beschwerdeführerin die entsprechende Auskunft und erklärte, dass diese mit dem Auskunftsersuchen datenschutzfremde Zwecke verfolgen würde. Sie wolle lediglich Beweise für eine zivilrechtliche Auseinandersetzung sichern.

Zur Reichweite des Auskunftsanspruchs nach der DSGVO hat der Bundesgerichtshof (BGH) dem Europäischen Gerichtshof (EuGH) Fragen vorgelegt.[142] Der BGH bezweifelt, dass das mit dem Auskunftsersuchen verbundene Verfolgen von anderen als daten

140 Siehe Leitlinien 01/2022 des EDSA vom 18. Januar 2022: „On Data Subject Rights - Right of Access (Version 1.0)“, abrufbar unter https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en.

141 Art. 12 Abs. 5 Satz 2 lit. b DSGVO.

142 Siehe BGH, Beschluss vom 29. März 2022, VI ZR 1352/20.

schutzrechtlichen Zwecken automatisch zu einem Ausschluss des Auskunftsanspruchs führt.[143] Nach dem Wortlaut der DSGVO[144] sei das Bestehen des Auskunftsrechts nicht an die Motivation der betroffenen Person gekoppelt, entsprechend müsse das Auskunftsersuchen auch nicht begründet werden. Dies spreche dafür, dass der Unionsgesetzgeber es grundsätzlich der betroffenen Person überlassen wollte, ob und aus welchen Gründen sie das Auskunftsersuchen stellt. Daher dürfe nicht allein aufgrund des Umstands, dass ein Auskunftsbegehren auf Übermittlung einer Datenkopie auf datenschutzfremde Gründe gestützt wird, darauf geschlossen werden, dass dieser offenkundig unbegründet oder exzessiv[145] sei.[146]

Unter Berücksichtigung dieser Ansichten des BGH lag in unserem Fall kein offenkundig unbegründeter oder exzessiver Antrag vor. Weder wurde das Auskunftsersuchen häufig wiederholt, noch lagen andere Gründe für ein rechtsmissbräuchliches Verhalten vor. Eine Schädigungsabsicht seitens der Beschwerdeführerin war vorliegend nicht erkennbar. Dem Unternehmen haben wir unter Verweis auf den Vorlagebeschluss des BGH mitgeteilt, dass die Auskunft gegenüber der Beschwerdeführerin zu erteilen ist und der Anspruch auf Übermittlung einer Datenkopie besteht.

Verantwortliche sind verpflichtet, betroffenen Personen die gewünschte Auskunft zu erteilen und Datenkopien, wie bspw. Telefonaufzeichnungen, zu übermitteln. Ein Auskunftsersuchen kann nicht mit dem Einwand, es diene datenschutzfremden Zwecken, verweigert werden, wenn kein offenkundig unbegründeter oder exzessiver Antrag oder rechtsmissbräuchliches Verhalten vorliegt.

143 Ebd., Rn. 16 ff.
144 Siehe Art. 15 DSGVO.
145 I. S. v. Art. 12 Abs. 5 Satz 2 DSGVO.
146 Siehe BGH, Beschluss vom 29. März 2022, VI ZR 1352/20, Rn. 18.

10.3 Ich will's wissen! Informationspflichten beim Datenabruf aus dem Handelsregister

Immer wieder erhalten wir Beschwerden von Personen, die ihre personenbezogenen Daten überraschend in kommerziell betriebenen öffentlichen Plattformen wiederfinden. Als Quelle der Daten stellt sich dann häufig das Handelsregister heraus. Kaufleute und Handelsgesellschaften sind verpflichtet, bestimmte Informationen in das Handelsregister eintragen zu lassen. Dies betrifft auch personenbezogene Daten von natürlichen Personen, wie bspw. das Geburtsdatum oder die private Anschrift von Firmengründer:innen. Die Einträge im Handelsregister sind – seit August dieses Jahres kostenlos – im Internet öffentlich einsehbar.[147] Kommerzielle Plattformen greifen die Daten ab und nutzen sie für eigene Zwecke. In keinem der uns bekannten Vorgänge wurden die betroffenen Personen hierüber von den Plattformbetreiber:innen informiert.

Ob ein Datenabruf aus dem Handelsregister zum Zweck der kommerziellen Veröffentlichung auf einem anderen Portal rechtmäßig ist, ist im Rahmen einer Interessenabwägung zu bewerten.[148] Dabei ist einerseits zu berücksichtigen, dass die Daten auf Grundlage gesetzlicher Regelungen im Handelsregister veröffentlicht werden müssen. Mit jeder weiteren Veröffentlichung ist die Gefahr verbunden, dass die Daten unkontrollierbar vervielfältigt und dadurch auch verfälscht werden können. Andererseits handelt es sich um Daten, die über das Handelsregister schon öffentlich zugänglich sind, d. h. ein Abruf ist grundsätzlich nicht auf bestimmte Zwecke beschränkt. Die Verarbeitung in manchen Portalen dient zudem der Transparenz über mögliche Verflechtungen von Unternehmen. Die Interessenabwägung ist daher in jedem Einzelfall vorzunehmen. Dabei ist auch entscheidend, ob die Verantwortlichen sicherstellen können, dass die Daten unverfälscht übernommen wurden und auch langfristig aktuell gehalten werden.

Nicht verhandelbar ist hingegen regelmäßig die Pflicht der Verantwortlichen, die betroffenen Personen über die Erhebung und die geplante Veröffentlichung ihrer personenbezogenen Daten zu informieren.[149] Verantwortliche kommen diesen Informationspflichten gegenüber den betroffenen Personen oft nicht nach, sondern berufen

147 Siehe 3.2.
148 Siehe Art. 6 Abs. 1 Satz 1 lit. f DSGVO.
149 Siehe Art. 14 DSGVO.

sich auf den Ausnahmetatbestand des „unverhältnismäßigen Aufwands“.[150] Dafür wird u. a. auf die große Anzahl der zu informierenden Personen hingewiesen oder im Fall nur postalisch vorliegender Adressdaten auch darauf, dass die Information per Post umständlicher und teurer sei als per E-Mail. Die Beweislast für die Unverhältnismäßigkeit des Aufwands liegt bei den Verantwortlichen. Diese müssen ihre Abläufe darlegen und erklären, warum der Aufwand für die Benachrichtigungen gegenüber dem Erkenntnisgewinn bei den Betroffenen nicht verhältnismäßig wäre. Der Aspekt, dass der postalische Versand aufwändiger und kostspieliger ist als ein Versand per E-Mail, kann nicht geltend gemacht werden. Für die Berechnung des Aufwands für ihre Informationspflichten können sich Verantwortliche nicht auf die für sie günstigste Möglichkeit als mutmaßlichen Regelfall berufen. Außerdem erfolgt die Datenerfassung und Datenverarbeitung im Rahmen eines solchen Geschäftsmodells digital, sodass ein postalischer Sammelversand auch an eine große Anzahl von Adressen regelmäßig ohne größeren Aufwand möglich ist.

Wer sich für das Geschäftsmodell der Massendatenveröffentlichung entscheidet, muss auch die daraus resultierenden Pflichten erfüllen. Ein solches Unternehmen kann sich in der Regel nicht auf die Ausnahme des unverhältnismäßigen Aufwands berufen. Gegen die Anwendung der Ausnahmevorschrift auf solche kommerziellen Verarbeitungszwecke sprechen auch die aufgeführten Regelbeispiele, die Verarbeitungszwecke im öffentlichen Interesse zum Gegenstand haben. Entscheidend ist letztlich die Ermöglichung der Kontrolle der betroffenen Personen über ihre personenbezogenen Daten: Wenn die Betreiber:innen von Plattformen die betroffenen Personen nicht benachrichtigen, erfahren diese nicht oder nur zufällig von der Verbreitung ihrer personenbezogenen Daten. So bleibt ihnen auch die Möglichkeit verwehrt, ihre Betroffenenrechte, insbesondere das Recht auf Auskunft, Widerspruch und Löschung, gegenüber den Verantwortlichen auszuüben.

Der Abruf personenbezogener Daten aus dem Handelsregister durch kommerzielle Plattformen kann im Einzelfall rechtmäßig sein. Die betroffenen Personen sind hierüber regelmäßig zu informieren.

150 Art. 14 Abs. 5 lit. b DSGVO.

10.4 Onlinehandel aufgepasst: Gastbestellungen müssen grundsätzlich angeboten werden!

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat mit ihrem Beschluss vom 24. März dieses Jahres Hinweise zum datenschutzkonformen Onlinehandel mittels Gastzugang veröffentlicht.[151] Kernaussage des Beschlusses ist, dass Verantwortliche, die Waren oder Dienstleistungen im Onlinehandel anbieten, ihren Kund:innen grundsätzlich einen Gastzugang für die Bestellung bereitstellen müssen, unabhängig davon, ob sie ihnen daneben auch ein Kundenkonto zur Verfügung stellen. Hintergrund ist, dass Verantwortliche nicht per se unterstellen können, dass Kund:innen in jedem Fall über ein fortlaufendes Kundenkonto verfügen wollen, vielmehr ist hierfür eine bewusste Willenserklärung erforderlich.

Bislang war es im Onlinehandel gängige Praxis, dass die Einrichtung eines Kundenkontos verlangt wurde, um eine Bestellung tätigen zu können. Diese Kundenkonten können dazu dienen, neue Bestellungen bei demselben Onlineshop zu vereinfachen. Auch eine Bestellhistorie kann im Konto oftmals eingesehen werden. Darüber hinaus nutzen Onlineshops die im Konto gespeicherten Daten aber häufig auch zur Profilbildung und zu Werbezwecken.

Im Datenschutzrecht gilt der Grundsatz der Datenminimierung.[152] Daraus ergibt sich, dass die Datenverarbeitung – auch im Onlinehandel – auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Erfolgt die Datenverarbeitung zur Vertragserfüllung,[153] muss die Verarbeitung auf das beschränkt sein, was zur Vertragserfüllung bzw. Vertragsabwicklung erforderlich ist, wobei der Begriff der Erforderlichkeit eng auszulegen ist.[154] Die Einrichtung eines Kundenkontos sowie die damit einhergehenden weiteren Datenverarbeitungen sind zur Vertragserfüllung regelmäßig nicht erforderlich. In der Regel darf ein Unternehmen daher nur dann ein Konto ein

151 Beschluss der DSK vom 24. März 2022: „Datenschutzkonformer Online-Handel mittels Gastzugang“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk.
152 Art. 5 Abs. 1 lit. c DSGVO.
153 Art. 6 Abs. 1 Satz 1 lit. b DSGVO.
154 Siehe EG 39 Satz 9 DSGVO.

richten, wenn die betroffene Person wirksam, also insbesondere freiwillig und informiert, einwilligt.[155]

Damit das Kriterium der Freiwilligkeit gewährleistet ist, darf die Erfüllung eines Vertrags nicht mit einem Ersuchen um Einwilligung in eine Datenverarbeitung verknüpft werden, die für die Erfüllung des Vertrags nicht erforderlich ist.[156] Von der Freiwilligkeit der Einwilligung in die Einrichtung eines Kundenkontos kann nicht ausgegangen werden, wenn den Kund:innen keine Möglichkeit einer Gastbestellung bzw. keine gleichwertige Bestelloption angeboten wird. Eine Bestelloption ist dann als gleichwertig anzusehen, wenn sie für die Kund:innen keinerlei Nachteile mit sich bringt, also insbesondere Bestellaufwand und Zugang zu diesen Möglichkeiten einer Bestellung mit Kundenkonto entsprechen. Erfreulicherweise bieten bundesweit und auch in Berlin immer mehr Unternehmen ihren Kund:innen die Alternative in Form eines Gastzugangs an.

Wenn personenbezogene Daten aus dem Kundenkonto für Werbezwecke ausgewertet oder verarbeitet werden sollen, sollten Unternehmen außerdem beachten, dass eine eigene auf diese Zwecke bezogene Einwilligung einzuholen ist. Werbung stellt eine Datenverarbeitung dar, die über die bloße Einrichtung und Führung eines fortlaufenden Kundenkontos hinausgeht und von der diesbezüglichen Einwilligung nicht abgedeckt ist.

10.5 Sichere Authentisierung

In einer bei uns eingegangenen Datenpannenmeldung teilte uns ein Unternehmen mit, dass Passwörter seiner Beschäftigten im Klartext offengelegt wurden, die zur Anmeldung zu IT-Systemen des Unternehmens dienten, mit denen auch personenbezogene Daten verarbeitet werden.

Wer personenbezogene Daten verarbeitet, muss sicherstellen, dass nur berechtigte Personen auf die Daten zugreifen können. Voraussetzung dafür ist, dass sich diese Personen gegenüber den Systemen und Diensten ausweisen. Der Prozess dafür nennt sich

155 Art. 6 Abs. 1 Satz 1 lit. a DSGVO i.V.m. Art. 4 Nr. 11, Art. 7 DSGVO.
156 Siehe Art. 7 Abs. 4 DSGVO.

Authentisierung.[157] Klassisch erfolgt diese über die Eingabe eines Benutzernamens und eines Passworts. Das Passwort darf nur derjenigen Person bekannt sein, die es nutzt. Der Schutz ist nicht mehr gewährleistet, wenn Passwörter anderen Personen bekannt werden. Eine essenzielle Schutzmaßnahme ist daher u. a., Passwörter nicht im Klartext zu speichern. Eine Überprüfung der korrekten Eingabe durch die sich anmeldende Person ist auch anders möglich: Dazu lässt sich ein kryptografisches Verfahren verwenden, das aus jedem Passwort eindeutig einen Wert ableitet, der statt des Passworts gespeichert wird. Das Verfahren wird dabei so gewählt, dass es aufwändig ist, aus dem abgeleiteten Wert auf das Passwort zurückzuschließen.

Ein Teil der Berechnung sollte dabei auf das Gerät ausgelagert werden, das die sich anmeldende Person nutzt. So wird das Passwort auch nicht im Klartext über die Verbindung zum Server geschickt. Dies ist ein zusätzlicher Schutz für den Fall, dass die Verschlüsselung der Verbindung, die natürlich trotzdem nötig ist, versagt oder sich eine andere Person Zugang zu dem IT-System verschafft, das die Eingaben der Nutzer:innen für deren Authentifizierung entgegennimmt. Dieses IT-System ist oft notwendigerweise über das Internet erreichbar und damit besonders gefährdet. Die Überprüfung der Nutzer:innen sollte einem weiteren IT-System vorbehalten sein, das selbst vor einem direkten Zugriff aus dem Internet geschützt ist. Dadurch werden einige Schwächen der Authentisierung mit Passwörtern abgemildert. Insbesondere ist damit die Wahrscheinlichkeit wesentlich gesenkt, dass Vorfälle – wie die eingangs erwähnte Datenpanne – zu unangenehmen Folgen für die Nutzer:innen und diejenigen Personen führen, deren Daten verarbeitet werden.

Trotzdem bleiben Restrisiken. Sicherere Verfahren sind verfügbar und verursachen generell keinen großen Aufwand. Sie basieren darauf, dass die Person, die sich als berechtigt ausweisen möchte, ein Gerät (wie z. B. ein Smartphone) besitzt, das ein komplexes kryptografisches Geheimnis verwahrt.[158] Dieses Geheimnis verbleibt ausschließlich in dem Gerät und wird dafür genutzt, um auf Anforderung des Servers des

157 Die Begriffe „Authentisierung“ und „Authentifizierung“ werden im allgemeinen Sprachgebrauch oft synonym verwendet, beschreiben aber verschiedene Teilprozesse eines Anmeldevorgangs: Benutzer:innen „authentisieren“ sich an einem System mittels eindeutiger Anmeldeinformationen (etwa per Passwort oder Chipkarte). Das System überprüft daraufhin die Gültigkeit der verwendeten Daten, es „authentifiziert“ die Nutzer:innen. Siehe https://www.bsi.bund.de/dok/11693908.

158 Ein gängiges Verfahren wird im FIDO2-Standard beschrieben.

Verantwortlichen eine Berechnung auszuführen, deren Ergebnis nur mit Kenntnis des Geheimnisses ermittelbar ist, das aber durch den Server auch ohne dieses Geheimnis überprüft werden kann. Daher müssen Unternehmen prüfen, ob ein derart passwortloses Authentisierungsverfahren unter den Umständen der konkreten Verarbeitung umsetzbar ist und sich der Aufwand hierfür unter Berücksichtigung des Risikos unbefugter Kenntnisnahme von Passwortdaten im verhältnismäßigen Rahmen bewegt. Sind diese beiden Faktoren gegeben, ist eine rein passwortbasierte Authentifizierung nicht mehr zulässig.

Wer personenbezogene Daten verarbeitet, muss sicherstellen, dass nur berechtigte Personen auf die Daten zugreifen können. Die Verifikation der Berechtigung mit Benutzername und Passwort entspricht nicht mehr dem Stand der Technik. Wer das Verfahren trotzdem nutzt, weil Alternativen nicht umgesetzt werden können, muss ausschließen, dass dafür Passwörter im Klartext gespeichert werden. Vorzuziehen und ggf. verpflichtend einzusetzen sind passwortlose Verfahren.

10.6 Hilfe, mein Kundenkonto wurde gehackt! Was tun gegen Identitätsdiebstahl und Accountübernahme?

Identitätsmissbrauch im Onlinehandel ist ein großes Ärgernis für die betroffenen Personen. Auch in diesem Jahr haben wir wieder einige Beschwerden zu diesem Thema erhalten. Die gute Nachricht ist, dass betroffene Personen selbst etwas tun können, um sich vor Identitätsmissbrauch zu schützen. Aber auch die Unternehmen sind in der Pflicht, Maßnahmen zum Schutz ihrer Kund:innen zu ergreifen.

In diesem Jahr war vor allem die unbefugte Übernahme von bestehenden Kundenkonten vermehrt Gegenstand von Beschwerdeverfahren. Die Übernahme eines Kundenkontos durch unbefugte Dritte, auch Account Takeover genannt, erfolgt typischerweise unter Verwendung der tatsächlichen Log-in-Daten, die die oder der Inhaber:in des betroffenen Kundenkontos festgelegt hat.[159] Hinter der Accountübernahme steckt häufig sog. Credential Stuffing. Darunter versteht man eine Cyberangriffsmethode,

159 Dies meint in der Regel E-Mail-Adresse bzw. Benutzername und Passwort.

bei der Zugangsdaten, die bei anderen Datenschutzverletzungen bzw. Datenpannen abgeschöpft wurden, automatisiert bei weiteren Diensten ausprobiert werden. Die Angriffsmethode basiert darauf, dass viele Nutzer:innen von Onlinediensten dieselben Zugangsdaten (Credentials) bei mehreren Diensten verwenden. Darauf spekulieren die Angreifer:innen – leider nicht selten mit Erfolg. Angreifer:innen können Listen mit etlichen Log-in-Daten bspw. im Darknet erwerben. Die Zugangsdaten können aus einer einzelnen, aber auch aus unterschiedlichen Quellen stammen. Entgegen der üblichen Erwartungen müssen die Passwörter dabei nicht schlecht oder schwach sein, auch als stark geltende Zugangsdaten können betroffen sein, wenn diese bei einer vorangegangenen Datenpanne offengelegt wurden.

Für die betroffenen Kontoinhaber:innen ist die Übernahme ihres Kundenkontos mit unangenehmen Folgen verbunden. Nicht nur können die im Konto gespeicherten Daten eingesehen werden, also bspw. die Anschrift, das Geburtsdatum oder die Kaufhistorie. In einigen von uns bearbeiteten Fällen konnte auch die im Konto hinterlegte E-Mail-Adresse mithilfe der Log-in-Daten geändert werden, sodass die Kontoinhaber:innen keinen Zugang mehr zu ihrem Konto hatten. Kommt es dann auch noch zu einer Warenbestellung, wird für die Kontoinhaber:innen zumeist ein intensiver Schriftwechsel mit dem Unternehmen erforderlich, um den Sachverhalt aufzuklären und eventuelle Kaufpreisforderungen abzuwehren. Wurde vor der Bestellung die im Kundenkonto hinterlegte E-Mail-Adresse ausgetauscht, kommt hinzu, dass die Kontoinhaber:innen ggf. erst mit erheblichem Zeitverzug von der Bestellung erfahren, weil etwaige per E-Mail versendete Bestellbestätigungen an die neu hinterlegte E-Mail-Adresse versandt wurden.

Unternehmen sind dazu verpflichtet, unter Berücksichtigung verschiedener Faktoren wie dem Stand der Technik, den Implementierungskosten und der Schwere des Risikos für betroffene Personen geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit der Verarbeitung zu gewährleisten und eine gegen die DSGVO verstoßende Datenverarbeitung zu verhindern.[160] Eine Maßnahme, um Credential Stuffing zu vereiteln, besteht darin, auf die Verwendung von Passwörtern bei der Authentisierung zu verzichten und stattdessen auf die Nutzung kryptografischer

160 Siehe Art. 32 DSGVO; siehe dazu auch die Orientierungshilfe der DSK vom 29. März 2019: „Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk.

Schlüssel zu setzen[161] oder zusätzlich zur Verwendung eines Passworts die Authentisierung mit einem zweiten Faktor zu verlangen. Angreifer:innen erlangen mit den derzeit verbreiteten Angriffsmethoden in der Regel nur Passwörter, nicht jedoch die kryptografischen Schlüssel der Anwender:innen oder andere (zweite) Faktoren.[162] Als zweiter Faktor dient meist der Besitz eines Geräts, das eine nur kurze Zeit gültige Buchstaben- oder Zahlenkombination anzeigt, die die Kund:innen zusätzlich zu ihrem Passwort angeben. Die Kombination wird dabei entweder auf dem Gerät erzeugt oder durch das Unternehmen über einen gesonderten Übermittlungsweg an das Gerät und damit an die Kund:innen übermittelt, wobei die Erzeugung auf einem eigens dafür bereitstehenden Gerät vorzuziehen ist.

Zumindest bei Datenverarbeitungen mit einem hohen Risiko, wie bspw. beim Onlinebanking, ist eine Zwei-Faktor-Authentisierung keine reine Empfehlung, sondern zur Erreichung eines angemessenen Schutzniveaus notwendig. Im Bereich des herkömmlichen Onlineshoppings ist die Zwei-Faktor-Authentisierung bisher nicht branchenüblich, zum Log-in genügen meist Benutzername bzw. E-Mail-Adresse und Passwort. Kommt es zu Credential Stuffing, können die Unternehmen die Accountübernahme als solche nur schwer verhindern. Wenn der Log-in in die Kundenkonten unter Verwendung der tatsächlichen Zugangsdaten erfolgt, können Unternehmen in der Regel nicht erkennen, ob der Log-in durch die wahren Kontoinhaber:innen oder durch unbefugte Personen erfolgt. Ein höheres Gesamtvolumen an Anmeldeversuchen kann für Unternehmen zwar ein Hinweis auf Credential Stuffing sein, aber selbst wenn ein erhöhtes Anmeldevolumen erkannt wird, können Unternehmen einen Angriff nur schwer unterbinden, ohne den Anmeldeprozess insgesamt, d.h. für sämtliche Kund:innen, zu beeinträchtigen.

Daher müssen Unternehmen prüfen, ob ein passwortloses oder Zwei-Faktor-Authentisierungsverfahren unter den Umständen der konkreten Verarbeitung umsetzbar ist und sich der Aufwand hierfür unter Berücksichtigung der Folgerisiken unberechtigter Anmeldungen im verhältnismäßigen Rahmen hält. Sind diese beiden Faktoren gegeben, dann ist eine rein passwortbasierte Authentifizierung nicht mehr zulässig.[163] Darüber hinaus müssen Unternehmen Maßnahmen ergreifen, um die Auswirkungen erfolgreicher Angriffe für betroffene Personen einzudämmen. Unternehmen haben insoweit zu prüfen,

161 Siehe 10.5.
162 Zur Zwei-Faktor-Authentisierung siehe auch https://www.bsi.bund.de/dok/11693908.
163 Siehe 10.5.

welche Maßnahmen im konkreten Fall geeignet und angemessen sind, um weiteren Schaden abzuwenden. So kann bspw. die Sperrung eines (mutmaßlich) betroffenen Kundenkontos eine wirksame Maßnahme darstellen. Unabhängig vom etwaigen Bestehen einer Benachrichtigungspflicht nach einem Angriff[164] sollen Unternehmen die betroffenen Kund:innen zudem über wichtige Ereignisse im Kundenkonto benachrichtigen, dazu zählt etwa die Änderung der im Kundenkonto hinterlegten E-Mail-Adresse.[165] Es bleibt jedoch das Risiko, dass die Kund:innen Benachrichtigungs-E-Mails nicht erhalten, etwa aufgrund eines überfüllten Posteingangs, oder sie die E-Mail nicht bzw. nicht sofort lesen und somit nicht umgehend reagieren. Ob eine Benachrichtigung für sich genommen bereits eine ausreichende Schutzmaßnahme darstellt, ist daher im Einzelfall zu prüfen.

Sofern über das Kundenkonto Bestellungen aufgegeben werden können, welche vonseiten der Kund:innen keine weitere Interaktion zur Auslösung einer Zahlungsverpflichtung verlangen, sollte die Änderung der E-Mail-Adresse von der Bestätigung der Kontoinhaber:innen abhängig gemacht werden. Dies kann z. B. durch Versenden eines Bestätigungslinks an die ursprünglich im Kundenkonto hinterlegte E-Mail-Adresse erfolgen. Auf diese Weise kann sichergestellt werden, dass die Änderung der E-Mail-Adresse von den tatsächlichen Kontoinhaber:innen vorgenommen wird. Zudem werden etwaige per E-Mail versendete Bestellbestätigungen so an die tatsächlichen Kontoinhaber:innen versandt, was diesen im Fall einer Bestellung wiederum ein unmittelbares Eingreifen ermöglicht. Diese Maßnahme versagt nur dort, wo die Angreifer:innen auch über die Zugangsdaten für das E-Mail-Konto verfügen.

Die gute Nachricht ist, dass Kontoinhaber:innen das Risiko von Angriffen wie Credential Stuffing verringern können, indem sie die Mehrfachverwendung von Passwörtern konsequent vermeiden. Wir empfehlen Kontoinhaber:innen daher nachdrücklich, für jeden Dienst ein eigenes, ausreichend langes Passwort anzulegen. Für die Nutzbarkeit empfehlen wir die Verwendung eines sicheren Passwortmanagers. Außerdem sollten die Kontoinhaber:innen überall dort, wo dies möglich ist, insbesondere aber bei besonders schützenswerten Konten wie E-Mail-Konten oder Kundenkonten bei Onlineshops, eine passwortlose bzw. eine Zwei-Faktor-Authentisierung aktivieren.

164 Art. 34 DSGVO.

165 Siehe auch Punkt 2.5 der Orientierungshilfe der DSK vom 29. März 2019: „Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk.

10.7 Veröffentlichung von Unterschriften auf der Website einer Aktiengesellschaft

Ein Aktionär beschwerte sich bei unser Behörde über die vollständige Veröffentlichung seiner handschriftlichen Gegenanträge zur Hauptversammlung einschließlich seiner Unterschrift auf der Website einer Aktiengesellschaft.

Nach der DSGVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden.[166] Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[167] Dazu zählt auch die Unterschrift einer Person. Die Verarbeitung der Daten ist u. a. rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher die verantwortliche Stelle unterliegt.[168] Sie muss ihrem Zweck angemessen und erheblich sein sowie auf das notwendige Maß beschränkt werden.[169] Personenbezogene Daten sollen folglich nur soweit erhoben und verarbeitet werden, wie dies für die Erreichung der Zwecke der Datenverarbeitung notwendig ist und im Hinblick auf den Verarbeitungszweck Relevanz besitzt. Außerdem sollten personenbezogene Daten nur verarbeitet werden, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere, mildere, das informationelle Selbstbestimmungsrecht der betroffenen Personen weniger belastende Mittel erreicht werden kann.

Der Vorstand einer Aktiengesellschaft ist nach Maßgabe des Aktiengesetzes (AktG) verpflichtet, Anträge von Aktionär:innen zugänglich zu machen.[170] Gegenstand dieser sog. Publizitätspflicht sind neben der Antragsbegründung und einer etwaigen Stellungnahme der Verwaltung der Aktiengesellschaft aber lediglich die Namen der Aktionär:innen einschließlich der Vornamen, nicht jedoch deren Unterschrift. Zwar können von Aktionär:innen übersandte Texte in eingescannter Form zum Abruf bereitgehalten werden. Sofern Gegenanträge jedoch über die gesetzlichen Pflichtangaben hinausgehende personenbezogene Daten enthalten, sind diese jeweils unkenntlich zu machen.

166 Art. 5 Abs. 1 lit. a DSGVO.
167 Art. 4 Nr. 1 DSGVO.
168 Art. 6 Abs. 1 Satz 1 lit. c DSGVO.
169 Art. 5 Abs. 1 lit. c DSGVO.
170 Siehe § 126 Abs. 1 Satz 1 AktG.

Im vorliegenden Fall war die Veröffentlichung der Originalunterschrift des Aktionärs auf dessen Gegenanträgen zur Hauptversammlung der Aktiengesellschaft durch Einstellen auf deren Website nicht zur Erfüllung der vorgenannten Publizitätspflicht erforderlich. Eine Schwärzung seiner Unterschrift hätte erfolgen können. Gleichfalls wäre eine Abschrift seiner Gegenanträge und deren Zugänglichmachung beschränkt auf die gesetzlich vorgeschriebenen Inhalte der verantwortlichen Stelle möglich und auch zumutbar gewesen. Den festgestellten Rechtsverstoß der Aktiengesellschaft haben wir mit einer Verwarnung sanktioniert.

Die Veröffentlichung der Originalunterschrift von Aktionär:innen auf Gegenanträgen zur Hauptversammlung einer Aktiengesellschaft ist nicht erforderlich und verstößt damit gegen die DSGVO.

10.8 Alte Kontoauszüge und das Auskunftsrecht

Ein Beschwerdeführer hatte seine Bank um kostenfreie Vorlage der Umsatzdaten seines Kreditkartenkontos aus den Jahren 2010 bis 2016 im Rahmen eines datenschutzrechtlichen Auskunftsersuchens gebeten. Die Bank lehnte dies zunächst unter Verweis auf die Archivierungsfunktion im Onlinekontoführungsbereich ab und verwies nach Rückfrage des Beschwerdeführers, der die fraglichen Kontoauszüge nicht archiviert hatte, auf eine Regelung in ihren Allgemeinen Geschäftsbedingungen. Sie bot dem Beschwerdeführer an, ihm eine kostenpflichtige Kopie seiner Kontoauszüge gegen Zahlung eines bestimmten Entgelts zukommen zu lassen.

Nach Auffassung des Amtsgerichts (AG) Bonn haben Bankkund:innen gegenüber ihrer Bank einen datenschutzrechtlichen Anspruch auf Auskunft[171] über sämtliche Kontobewegungen auf ihrem Bankkonto. Die Bank erfülle den Auskunftsanspruch der Kund:innen allerdings noch nicht, wenn sie nur die Kontoauszüge zur Verfügung stellt. Damit seien lediglich ihre Pflichten aus dem Zahlungsdienstvertrag erfüllt. Die Datenauskunft solle zwar primär die Rechtmäßigkeitskontrolle im Hinblick auf die Verarbeitung der personenbezogenen Daten ermöglichen,[172] die Verfolgung eines darüber hinausgehenden oder anders gelagerten Zwecks (z. B. die Vorbereitung eines Gerichtsverfahrens

171 Art. 15 Abs. 1 DSGVO.
172 Siehe EG 63 Satz 1 DSGVO.

oder die Stärkung der eigenen Position gegenüber Dritten) begründe aber noch nicht den Einwand des Rechtsmissbrauchs.[173]

Das Auskunftsrecht nach der DSGVO umfasst alle Daten, die bei Verantwortlichen vorhanden sind. Eine Ausnahme für nur einen Teil der Daten ist nicht vorgesehen.[174] Für den Umfang des Auskunftsanspruchs ist daher der Datenbestand zum Zeitpunkt des Auskunftsverlangens maßgeblich. Die betroffene Person hat dabei stets einen Anspruch auf vollständige und inhaltlich richtige Auskunft über die konkret zu ihr verarbeiteten Daten. Die Leitlinien des EDSA zum Auskunftsrecht nach Art. 15 DSGVO sehen vor, dass sich der Begriff der Kopie lediglich auf diejenigen Informationen bezieht, die nach den Bestimmungen der DSGVO zu erteilen sind.[175] Diese geben den verantwortlichen Stellen einen Spielraum, wie die Auskunft im konkreten Einzelfall am zweckmäßigsten umgesetzt werden kann. Insofern besteht für betroffene Personen kein pauschaler Anspruch auf Übersendung einer kompletten Kontoauszugskopie. Dennoch besteht ein Recht auf vollständige Auskunft. Praktisch lässt sich das Auskunftsrecht in vielen Fällen am einfachsten durch eine Auflistung der Umsätze (Buchungen) des jeweiligen Kontos erfüllen. Wir haben die verantwortliche Bank im Gespräch darauf hingewiesen, um zukünftig auf einen veränderten und datenschutzkonformen Auskunftsprozess hinzuwirken.

Bankinstitute sind verpflichtet, betroffenen Personen im Rahmen eines Auskunftsverlangens zumindest die Umsatzdaten eines Bankkontos kostenfrei zur Verfügung zu stellen.

173 Siehe AG Bonn, Urteil vom 30. Juli 2020, 118 C 315/19, Rn. 33 Satz 3, 4 und 5, abrufbar unter https://openjur.de/u/2271642.html.

174 Siehe Art. 15 DSGVO.

175 Siehe Leitlinien 01/2022 des EDSA vom 18. Januar 2022: „On Data Subject Rights – Right of Access (Version 1.0)“, Ziffern 22 und 23, abrufbar unter https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en (im Konsultationsprozess).

10.9 Kein Rechtsmissbrauch bei Auskunftsverlangen zur Vorbereitung von Zivilprozessen

Ein Versicherungsunternehmen weigerte sich, den datenschutzrechtlichen Auskunftsanspruch einer betroffenen Person zu erfüllen, da diese ihrer Auffassung nach die Auskunft rechtsmissbräuchlich zur Vorbereitung eines gegen die Versicherung laufenden Zivilprozesses verlange.

Die DSGVO ermöglicht verantwortlichen Stellen, sich gegen die missbräuchliche Ausübung von Betroffenenrechten wie dem Auskunftsrecht zur Wehr zu setzen.[176] Dabei können zwei Fallkonstellationen unterschieden werden, in denen ein Missbrauch vorliegen kann: Zum einen liegt ein Missbrauchsfall bei einem offensichtlich unbegründeten Antrag vor.[177] Allerdings bedürfen unbegründete Anträge regelmäßig ohnehin lediglich einer Negativantwort,[178] die den verantwortlichen Stellen in der Regel keinen besonderen Aufwand abverlangt. Ein Missbrauchsfall in solchen Fallkonstellationen liegt daher erst dann vor, wenn die Bearbeitung des Antrags einen weit überdurchschnittlichen Aufwand erfordern würde, obwohl seine Erfolglosigkeit von vornherein unzweifelhaft feststeht. Zum anderen kann ein Missbrauchsfall im Falle eines exzessiven Antrags vorliegen.[179] Ein Antrag ist nicht schon allein deshalb exzessiv, weil er einen hohen Bearbeitungsaufwand bei den verantwortlichen Stellen auslöst. Erforderlich ist vielmehr ein rechtsmissbräuchliches Verhalten der antragstellenden Person. Für die Auslegung ist das hinter dem jeweiligen Recht stehende Ziel von Bedeutung.[180]

Die Leitlinien des EDSA zum Auskunftsrecht nach Art. 15 DSGVO sehen insoweit eine entsprechende Festlegung vor, dass Motive von betroffenen Personen zur Geltendmachung von datenschutzrechtlichen Auskunftsersuchen grundsätzlich für verantwortliche Stellen nicht abfragbar sind und darüber hinaus auch die Absicht, die erhaltenen Informationen

176 Siehe Art. 12 Abs. 5 Satz 2 DSGVO.
177 Siehe Art. 12 Abs. 5 Satz 2 Alt. 1 DSGVO.
178 Art. 12 Abs. 4 DSGVO.
179 Siehe Art. 12 Abs. 5 Satz 2 Alt. 2 DSGVO.
180 So beim Auskunftsrecht entsprechend EG 63 Satz 1 DSGVO: „Eine betroffene Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können."

zur Geltendmachung von Rechtsansprüchen gegenüber der verantwortlichen Stelle zu nutzen, keine rechtsmissbräuchliche Ausübung durch betroffene Personen darstellt.[181]

Motive von betroffenen Personen zur Geltendmachung von datenschutzrechtlichen Auskunftsersuchen sind durch verantwortliche Stellen nicht abfragbar. Auskunftsverlangen sind zu erfüllen, unabhängig davon, ob sie auch zur Vorbereitung von Zivilprozessen gegen die verantwortlichen Stellen dienen können.

10.10 Pseudonymisierung für den Datenexport

Ein Handelsunternehmen wandte sich an uns mit der Bitte um Einschätzung eines Verfahrens, das ihm ermöglichen sollte, ohne Risiken für seine Kund:innen Daten zur Verarbeitung in die USA zu exportieren. Die USA bieten nach Feststellung des EuGH keinen adäquaten Schutz der Persönlichkeitsrechte bei der Verarbeitung personenbezogener Daten. Die vorgeschlagene Lösung erwies sich leider als nicht tragfähig.

Im Jahr 2020 stellte der EuGH fest, dass in den USA kein angemessenes Niveau des Schutzes personenbezogener Daten besteht.[182] Dies liegt vornehmlich an den Möglichkeiten von US-amerikanischen Behörden, auf dort verarbeitete Daten zuzugreifen, ohne dass betroffenen Personen ausreichende Rechtsmittel dagegen zur Verfügung stehen. Der EDSA reagierte auf dieses Urteil mit Empfehlungen, mit welchen zusätzlichen Maßnahmen rechtlicher und technischer Art dennoch ein ausreichender Schutz bei Datenexporten in ein unsicheres Drittland wie den USA gewährleistet werden kann.[183] Eines der empfohlenen Mittel besteht in der Pseudonymisierung der Daten vor ihrem Export.

181 Siehe Leitlinien 01/2022 des EDSA vom 18. Januar 2022: „On Data Subject Rights - Right of Access (Version 1.0)“, Ziffern 13 und 187, abrufbar unter https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en (im Konsultationsprozess); siehe hierzu auch 10.2.

182 Siehe EuGH, Urteil vom 16. Juli 2020, C-311/18 („Schrems II“); siehe hierzu ausführlich JB 2020, 1.2.

183 Empfehlungen 01/2020 des EDSA vom 18. Juli 2021: „Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten (Version 2.0)“, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

Durch eine Pseudonymisierung werden personenbezogene Daten so verändert, dass sie ohne Hinzuziehung von zusätzlichen Informationen nicht mehr einzelnen Personen zugeordnet werden können.[184] Das setzt voraus, dass alles aus den ursprünglichen Daten entfernt werden muss, was die Personen eindeutig identifiziert. Dabei spielen zunächst eindeutig identifizierende Angaben wie der Name der Person, ihr Geburtsdatum oder ihre Adresse eine Rolle. So sah dies auch das Handelsunternehmen vor, das sich an uns gewandt hatte. Es wollte einen Dienstleister für die Abwicklung der Geschäfte seines Onlineshops einsetzen. Dieser Dienstleister hat seinen Sitz in den USA und verarbeitet dort auch vornehmlich die Daten, die ihm anvertraut werden. Auf dem Weg von den Kund:innen über den Onlineshop zum Dienstleister sollten die Daten so verändert werden, dass die Kund:innen weder für den Dienstleister noch für Behörden, die die Aushändigung der Daten des Dienstleisters hätten verlangen können, erkennbar sind.

Dabei sind die Möglichkeiten, die US-amerikanischen Behörden zur Erkennung von Personen in Datenbeständen zur Verfügung stehen und von denen vermutet werden kann, dass sie auch tatsächlich eingesetzt werden, nicht zu unterschätzen. Es ist nicht unwahrscheinlich, dass die Strategie einiger dieser Behörden darin besteht, sich Daten aus vielen Quellen zunächst auf Vorrat anzueignen und bei Bedarf miteinander zu vernetzen. Hierfür kommen etwa die Datenströme in Betracht, die aus Bezahlvorgängen stammen. Viele Bezahldienstleister:innen haben ihren Sitz in den USA. Die von ihnen verarbeiteten Daten unterliegen dem Zugriff US-amerikanischer Behörden. Auch die Society for Worldwide Interbank Financial Telecommunication (SWIFT) mit Sitz in Belgien, die weltweit besonders viele Transaktionen abwickelt, ist zur Herausgabe von Daten verpflichtet.[185] Handelsgeschäfte, die elektronisch bezahlt werden, wie die aus dem Geschäft des von uns beratenen Unternehmens, lassen sich mit derart aufgezeichneten Transaktionen abgleichen und damit die Identität zumindest eines Teils der Kund:innen aufdecken.

Der EDSA stellt daher in seinen Empfehlungen die Anforderung auf, dass keine der zusätzlichen Informationen, die der Zuordnung von pseudonymisierten Daten zu ein

184 Siehe Art. 4 Nr. 5 DSGVO.

185 In Bezug auf Daten, die durch SWIFT in der Europäischen Union (EU) verarbeitet werden, wird die Anforderung der Daten durch ein Abkommen zwischen der EU und den USA geregelt, siehe https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22010A0727(01).

zelnen Personen dienen können, in dem Land verfügbar sein dürfen, in das diese exportiert werden. Anderenfalls bestünde kein wirksamer Schutz für die Daten. Wir mussten die von dem Unternehmen vorgesehene Maßnahme daher als unzureichend zurückweisen.

Um Daten in ein Land zu exportieren, das keinen ausreichenden Schutz der Persönlichkeitsrechte bietet, sind tiefgreifende technische Maßnahmen nötig, die einen Missbrauch exportierter Daten ausschließen. Pseudonymisierung kann dies leisten. Doch müssen alle Möglichkeiten berücksichtigt werden, pseudonymisierte Daten wieder Einzelpersonen zuzuordnen.

10.11 Datenpannen bei Apps und Webdiensten

Ein nicht unerheblicher Anteil der bei uns gemeldeten Datenpannen ist darauf zurückzuführen, dass Datenschutz und IT-Sicherheit nicht bereits bei der Konzeption von Apps und Webanwendungen konsequent mitgedacht werden.

Wenn Menschen mit mobilen Anwendungen (Apps) und Webanwendungen umgehen, fällt eine Vielzahl von personenbezogenen Daten an, u. a. Daten über die Art und Weise der Nutzung der Anwendung sowie persönliche, zum Teil besonders schützenswerte Daten, die in der Anwendung hinterlegt werden. Sofern Nutzer:innen sich bei der Anmeldung gegenüber der Anwendung identifizieren müssen, wird als Benutzername häufig die eigene E-Mail-Adresse verwendet. Sicherheitslücken können diese Daten offenlegen, mit teils lästigen, teils ausgesprochen unangenehmen Folgen für die Betroffenen. Daher sind die Betreiber:innen verpflichtet, die Anwendungen und die dahinterstehenden Dienste sicher auszugestalten. Pannen sind an die zuständige Datenschutzaufsichtsbehörde zu melden. Bei hohen Risiken für die Betroffenen müssen auch diese informiert werden. Am besten ist es, wenn es gar nicht erst zu einer solchen Datenpanne kommt.

Uns erreichen dennoch oft Meldungen von Sicherheitslücken, sei es von den Unternehmen selbst, sei es, dass Sicherheitsforscher:innen Schwachstellen gefunden haben. Die gemeldeten Sicherheitslücken betreffen meistens eine der typischen Klassen von Schwachstellen, die vom Open Web Application Security Project (OWASP), einer

gemeinnützigen Stiftung, die sich für die Verbesserung der Sicherheit von Software einsetzt, regelmäßig in einer Liste der häufigsten und riskantesten Schwachstellen aufgelistet werden.[186] In der im Jahr 2021 herausgegebenen Liste steht erstmals die unzulängliche Zugangskontrolle auf dem ersten Platz. Gemeint ist damit, dass für bestimmte Zugriffe auf Daten eigentlich eine Identifizierung und Authentifizierung der Abfragenden erfolgen müsste, diese aber entweder gar nicht erfolgt oder fehlschlägt, sodass zu schützende Daten an unberechtigte Personen ausgeliefert werden. Auch in unserer Arbeit machen diese Fälle neben den Angriffen durch Schadsoftware einen wesentlichen Anteil der Sicherheitsvorfälle aus, die schwerwiegende Folgen für eine große Anzahl von betroffenen Personen haben können.

In verschiedenen uns bekannt gewordenen Fällen wurde bspw. die Kommunikation einer Smartphone-App mit den dazugehörigen Serversystemen nicht ausreichend abgesichert. Die Einschätzung der Entwickler:innen war dabei anscheinend: Da die App von uns stammt und nur diese mit den Servern spricht, genügt es, die Kommunikationsverbindung zu verschlüsseln. Eine Prüfung der Zulässigkeit der jeweiligen Abfrage erfolgte dann nur noch eingeschränkt, denn man ging davon aus, dass die eigene App nur berechtigte Anfragen stellen würde. Anfragen aus anderen Quellen fielen gänzlich aus dem Blickfeld. Diese Ansicht geht fehl: Auch die Anwendung kann Fehler enthalten und die Abfrage solcher Daten ermöglichen, auf die die jeweils nutzende Person eigentlich keinen Zugriff haben sollte. Zudem besteht auch die schwerwiegendere Möglichkeit, dass Dritte die Kommunikationsschnittstelle ohne die Anwendung nutzen und direkt den Server kontaktieren. Die Verschlüsselung hilft hier nur sehr eingeschränkt. Sie erschwert es zwar, zu ermitteln, auf welche Weise und über welche Schnittstellen die Anwendung mit den Servern des Hintergrundsystems interagiert. Doch kann sie meist leicht umgangen werden, wenn die Angreifenden das Endsystem kontrollieren, auf dem die Anwendung läuft. Es ist daher nur eine Frage der Zeit, bis bekannt ist, welche Befehle der Server über die Anwendungsschnittstelle entgegennimmt und ausführt, ohne die Berechtigung der Anfragenden zu überprüfen. Dabei können personenbezogene Daten preisgegeben werden. Durch geschickte Variation der Anfragen lässt sich die Datenbeute zudem oft maximieren.

186 Siehe https://owasp.org.

Konkrete Datenpannen, die auf dem beschriebenen Problem basierten, waren u. a. folgende Vorfälle:

- Die Serverschnittstelle einer App zur Wahlkampfunterstützung[187] gab nicht nur wie vorgesehen die 15 Top-Wahlhelfenden in einer Gegend aus, sondern so viele, wie angefordert wurden. Da zudem weit mehr Daten pro Datensatz als notwendig geliefert wurden, konnten umfangreiche Daten aller Wahlhelfenden eingesehen werden. In einer später aufgetretenen Schwachstelle ließen sich sogar sämtliche Daten des Straßenwahlkampfs abrufen. Die Anonymisierung der betroffenen Personen war dabei so unzureichend, dass zumindest in Einzelfällen ihre Identifizierung möglich sein konnte.

- Ein Apothekenlieferdienst ermöglichte über die Schnittstelle, die dessen Bestell-App verwendete, den Abruf der gesamten Bestelldaten aller Kund:innen.

- Eine Praxisverwaltungssoftware lieferte über die Schnittstelle eine Liste der betreuten Praxen. Die Datensätze enthielten Zugangsdaten zu weiteren Systemen. Patient:innen konnten Daten anderer Patient:innen inklusive Rechnungen, Laborergebnissen und Krankschreibungen abrufen, da nur die grundsätzliche Zugangsberechtigung geprüft wurde, nicht aber, ob auf Daten des eigenen oder eines fremden Accounts zugegriffen wurde.

Andere Datenpannen basierten darauf, dass Zugangsschlüssel zu Schnittstellen von weiteren Diensten (z. B. für den E-Mail-Versand) im Programmcode einer Website abgelegt waren, der ungeschützt von Dritten abgerufen werden konnte. Solche Pannen traten bspw. bei einer Anwendung für Buchung und Ergebnisversand bei Corona-Schnelltestzentren und einem Webshop auf.

Häufig auftretende Fehler bei Webanwendungen sind zudem unzureichend abgesicherte Links, die zum Abrufen von Rechnungen, Bestellbestätigungen oder Corona-Testergebnissen[188] genutzt werden. Oft existieren fortlaufende Kunden- oder Bestellnummern, die in einem vorliegenden Link verändert werden können, um die jeweiligen Dokumente anderer Personen abzurufen. Eine sichere Implementierung würde das ent

187 Siehe JB 2021, 15.1.
188 Siehe JB 2021, 1.4.

sprechende Dokument nur dann ausgeben, wenn weitere Prüfungen erfolgreich verlaufen. Mögliche Bedingungen können darin bestehen, dass die betreffende Person in der Anwendung eingeloggt sein oder sie weitere das Dokument identifizierende Parameter angeben muss, die Dritten nicht bekannt sind und auch nicht erraten werden können.

Werden wir auf Sicherheitslücken wie die beschriebenen hingewiesen, wenden wir uns unverzüglich an das verantwortliche Unternehmen und fordern zur Beseitigung der Sicherheitslücke auf. Wir fordern weitere Informationen an, um zu beurteilen, ob die ergriffenen Maßnahmen ausreichen, die Datenverarbeitung zukünftig sicherer zu gestalten. Ist den Verantwortlichen eine Verletzung ihrer Pflichten nachzuweisen, können auch Sanktionsmaßnahmen die Folge sein.

Wer Apps und Webanwendungen betreibt, muss für die Sicherheit der mit ihnen verarbeiteten Daten sorgen. Um Sicherheitslücken zu finden, müssen Anwendung und dahinterstehende Serverdienste detailliert auf Schwachstellen untersucht werden. Schutzmaßnahmen, die unabhängig von der konkreten Anwendung arbeiten – wie z. B. Verschlüsselung, Firewalls, Proxyserver oder automatisierte Untersuchungen von Quellcodes auf eher formale Fehler – reichen nicht aus.

11 Verkehr und Tourismus

11.1 Der Wächter-Modus von Tesla

In diesem Jahr haben wir eine Vielzahl von Beschwerden in Bezug auf den sog. Wächter-Modus (Sentry Mode) erhalten, den Tesla in seinen Fahrzeugen zur Verfügung stellt. Auch Presseanfragen erreichen uns immer wieder zu diesem Thema.

Seitdem Tesla Ende 2021 seine deutsche Hauptniederlassung von Bayern nach Berlin verlegt hat, sind wir innerhalb Deutschlands als Datenschutzaufsichtsbehörde für die Entgegennahme von Beschwerden zuständig, die sich gegen die Verarbeitung personenbezogener Daten durch Tesla zu eigenen Zwecken richten. Die europaweite Hauptniederlassung von Tesla liegt allerdings in den Niederlanden. Daher reichen wir die bei uns eingehenden Beschwerden gegen Tesla im Rahmen des europäischen Kooperationsverfahrens[189] an die zuständige niederländische Aufsichtsbehörde zur Bearbeitung weiter.

Der überwiegende Teil der bei uns eingehenden Beschwerden hat sich aber nicht gegen das Unternehmen Tesla selbst gerichtet, sondern gegen den in Tesla-Fahrzeugen eingebauten Wächter-Modus, mit dem sich die Umgebung videotechnisch überwachen lässt. War der Wächter-Modus in seiner früheren Form aktiviert, haben mehrere Kameras das Geschehen um das Fahrzeug permanent aufgezeichnet. Die Aufzeichnungen wurden erst nach einer Stunde überschrieben. Erkannte dann das Fahrzeug eine Bedrohung, wurden die letzten zehn Minuten der Aufzeichnung dauerhaft auf einem USB-Stick gespeichert, falls dieser im Fahrzeug angeschlossen war. Im Fall einer erheblichen Bedrohung aktivierte sich zudem die Alarmanlage und die Halter:innen wurden über eine Benachrichtigung per Mobiltelefon verständigt. Eine erhebliche Bedrohung wurde etwa erkannt, wenn eine Scheibe eingeschlagen wurde. Es gibt allerdings Hinweise, dass bereits als Bedrohung eingeschätzt wurde, wenn sich eine Person lediglich am Fahrzeug vorbeibewegte.

189 Art. 60 Datenschutz-Grundverordnung (DSGVO).

Der Einsatz des Wächter-Modus war in dieser Form in aller Regel nicht datenschutzkonform: Die Anfertigung und Speicherung von Videoaufnahmen von Personen oder Kennzeichen im öffentlichen Raum ist generell nur zulässig, wenn sie aus einem hinreichenden Anlass erfolgt. Dies ist jedenfalls ohne konkretes Bedrohungsszenario, etwa wenn sich Personen oder andere Fahrzeuge lediglich an einem Fahrzeug vorbeibewegen, nicht der Fall. Die Interessen der betroffenen Personen überwiegen dann in der Regel jenen der Halterin bzw. des Halters.[190]

Seit Ende 2022 ist der Wächter-Modus nach einem Software-Update wesentlich datenschutzfreundlicher gestaltet. Insbesondere sind die Kameras nun standardmäßig deaktiviert. Die Halter:innen können selbst einstellen, ob permanent Videoaufnahmen erfolgen sollen. Sind die Kameras deaktiviert, werden Bedrohungen lediglich durch Sensoren erkannt, die nur bei Berührungen des Fahrzeugs, nicht mehr bei Aktivitäten um das Fahrzeug herum – etwa bei bloßem Vorbeigehen – reagieren. Wird eine Bedrohung festgestellt, werden die Kameras ebenfalls nicht mehr automatisch aktiviert, vielmehr empfangen die Halter:innen eine Benachrichtigung per Mobiltelefon, ob Videoaufnahmen angefertigt werden sollen. Zudem hat Tesla die Dauer der Videoaufnahmen auf ein bis zehn Minuten – je nach den Einstellungen der Halter:innen – reduziert.

Sowohl die Kameras als auch der Wächter-Modus insgesamt sind standardmäßig ausgeschaltet und müssen manuell aktiviert werden. Die Videoaufnahmen erfolgen zu eigenen Zwecken der Halter:innen, bspw. zum Diebstahlschutz. Halter:innen von Tesla-Fahrzeugen sind daher zunächst selbst für den Betrieb des Wächter-Modus verantwortlich und haben die Voraussetzungen für die Anfertigung und Speicherung von Videoaufnahmen zu beachten. In jedem Fall sind sie ebenso wie Unternehmen, die Videoüberwachungstechnik betreiben, verpflichtet, den betroffenen Personen auf geeignetem Wege Datenschutzinformationen zu erteilen.[191] Wird eine Videoüberwachung mittels eines Fahrzeugs durchgeführt, bietet sich hier regelmäßig ein Aufdruck auf dem Fahrzeug an. Dieser sollte darauf aufmerksam machen, dass und durch wen eine Videoüberwachung erfolgt, sowie einen Link oder QR-Code enthalten, der auf eine Website mit weiteren Datenschutzinformationen verweist. Uns ist kein Fall bekannt, in dem Halter:innen von Tesla-Fahrzeugen tatsächlich die bei Betrieb des Wächter-Modus erforderlichen Datenschutzinformationen erteilt haben.

190 Art. 6 Abs. 1 Satz 1 lit. f DSGVO.
191 Art. 13, 14 DSGVO.

Sollten wir auf eine nicht rechtmäßige Videoüberwachung durch ein Fahrzeug mit aktiviertem Wächter-Modus oder mangelnde Informationen über die Videoüberwachung aufmerksam gemacht werden, besteht für uns insbesondere bei wiederholten Verstößen die Möglichkeit, Aufsichtsmaßnahmen bis hin zur Verhängung eines Bußgelds zu ergreifen. Dies kann insbesondere Halter:innen betreffen, die das genannte Software-Update nicht installiert haben, d. h. den Wächter-Modus in seiner früheren Form nutzen. Tesla-Fahrzeuge sind auch ohne aktivierten Wächter-Modus grundsätzlich vor Diebstählen geschützt, etwa durch die ebenfalls in den Fahrzeugen verbauten Alarmanlagen.

Für Tesla sind wir innerhalb Deutschlands die zuständige Aufsichtsbehörde. Ebenso sind wir für alle Halter:innen von Tesla-Fahrzeugen zuständig, die in Berlin ansässig sind. Werden der in Tesla-Fahrzeugen verbaute Wächter-Modus bzw. dessen Kameras aktiviert, muss sichergestellt sein, dass andere Personen und Fahrzeuge nur mit hinreichendem Anlass aufgezeichnet werden. Zudem müssen den betroffenen Personen die erforderlichen Datenschutzinformationen bereitgestellt werden.

11.2 Vorlage von Ausweiskopien zur Buchung von Ferienunterkünften

Ferienunterkünfte über Onlineplattformen bzw. per App zu buchen, ist bequem. Weniger bequem ist es, sich auf einer solchen Plattform zu registrieren oder Ansprüche auf Datenauskunft bzw. -löschung geltend zu machen, wenn hierfür ungeschwärzte Ausweiskopien angefordert werden. Hierzu liegt nunmehr eine Entscheidung der irischen Datenschutzaufsichtsbehörde (DPC) vor.

Eine Onlineplattform zur Buchung von Ferienunterkünften hat ihre deutsche Niederlassung in Berlin. Diese hat über Jahre hinweg sowohl für die Registrierung als auch für Fälle, in denen Kund:innen Auskunft über die zu ihnen verarbeiteten Daten einholen oder diese löschen lassen wollten,[192] pauschal ungeschwärzte Ausweiskopien angefordert. Wegen dieser Praxis sind seit 2018 viele Beschwerden gegen das Unternehmen bei unserer Behörde eingegangen. Wir haben bereits früher darüber berichtet und

192 Siehe Art. 15, 17 DSGVO.

dargelegt, welche Voraussetzungen für die Anforderung von Ausweiskopien gelten. In der Folge haben wir den betroffenen Personen empfohlen, sich gegen die pauschale Anforderung von ungeschwärzten Ausweiskopien zu wehren.[193]

Die europäische Hauptniederlassung des Unternehmens liegt in Irland. Letztlich zuständig für die inhaltliche Bearbeitung der bei uns eingehenden Beschwerden ist daher die DPC. Zu einer bereits im Herbst 2019 eingereichten Beschwerde liegt nunmehr die erste abschließende Entscheidung der DPC vor. Die Beschwerde führende Person wünschte die Löschung ihrer Daten durch das Unternehmen. Das Unternehmen forderte hierfür zunächst eine Ausweiskopie an, woraufhin sich die Person weigerte, diese zu übermitteln, und Beschwerde bei uns einreichte. Die DPC hat der Person in ihrem Kernanliegen Recht gegeben und entschieden, dass das Unternehmen rechtswidrig gehandelt hat. Das Unternehmen habe mehr Daten angefordert, als zur Identifizierung erforderlich gewesen wäre.[194] Zudem habe das Unternehmen keine hinreichenden Zweifel an der Identität der Person dargelegt und wohl auch nicht gehabt.[195] Die DPC hat dementsprechend Maßnahmen gegen das Unternehmen ergriffen.

Es ist regelmäßig rechtswidrig, wenn Unternehmen pauschal ungeschwärzte Ausweiskopien anfordern, wenn betroffene Personen die ihnen nach der DSGVO zustehenden Rechte geltend machen wollen. Die Zukunft wird zeigen, ob die irische Datenschutzaufsichtsbehörde ihre diesbezügliche Entscheidung auch auf den Registrierungsprozess der Onlineplattform überträgt.

193 Siehe JB 2020, 12.4.
194 Siehe das Datenminimierungsgebot i. S. v. Art. 5 Abs. 1 lit. c DSGVO.
195 Siehe Art. 12 Abs. 6 DSGVO.

12 Sanktionen

12.1 Kontaktverfolgung der unerwünschten Art

Auch im zweiten Pandemiejahr mussten wir zweckfremde Nutzungen von Kontaktdaten, die in Geschäften oder Restaurants zum Zwecke der Anwesenheitsdokumentation erhoben wurden, sanktionieren.

Zur Eindämmung der Corona-Pandemie regelten die verschiedenen SARS-CoV-2-Infektionsschutzmaßnahmenverordnungen die Erhebung von Kontaktdaten wie Name, Telefonnummer, Anschrift oder E-Mail-Adresse. In einem uns vorliegenden Fall wurden solche Daten durch einen Mitarbeiter eines Sportgeschäfts verwendet, um eine Kundin mehrmals privat zu kontaktieren und sie u. a. zu einem Treffen aufzufordern. Die wiederholte unerwünschte Kontaktaufnahme per E-Mail wurde mit einem Bußgeld durch uns sanktioniert. In einem weiteren Fall erhielt ein Restaurantgast unerwünschte Werbe-E-Mails, nachdem er seine Kontaktdaten in eine Anwesenheitsliste eingetragen hatte. Das Restaurant verwendete die von ihm allein zur Kontaktnachverfolgung im Fall einer Corona-Infektion angegebene E-Mail-Adresse ohne seine Einwilligung für die Versendung von Newslettern. Auch als er dem Restaurant bereits mitgeteilt hatte, dass er keine Werbung mehr wünsche, erhielt er einen weiteren unerwünschten Newsletter. Gegen das Restaurant haben wir ebenfalls einen Bußgeldbescheid erlassen.

Inzwischen ist eine Anwesenheitsdokumentation zum Zwecke der Kontaktnachverfolgung zu Infektionsschutzgründen gesetzlich nicht mehr vorgesehen.

12.2 Datenschutz für die Tonne

Wer einen Corona-Test in einem Testzentrum machen möchte, muss regelmäßig eine Reihe von personenbezogenen Daten angeben. Dabei erfolgt die Erhebung der Daten entweder analog in Papierform oder digital über eine Webanwendung. Die vier von uns gegen Betreiber:innen von Testzentren erlassenen Bußgeldbescheide

zeigen, dass Verstöße gegen das Datenschutzrecht abhängig vom gewählten Format in unterschiedlicher Ausprägung auftreten können.

Ein Unternehmen, das mehrere Corona-Teststationen betreibt und eine digitale Datenerhebung über das eigene Internetportal vorsah, hatte sein Anmeldeformular nicht datenschutzkonform gestaltet. Als Pflichtangabe war in dem Formular der Impfstatus vorgesehen. Weder gab es eine gesetzliche Verpflichtung, diese Information für die Durchführung eines Corona-Tests zu erheben, noch wurden entsprechende Einwilligungen eingeholt. Zudem sah das Onlineformular zur Angabe der Staatsangehörigkeit eine standardmäßige Voreinstellung in Form einer Deutschlandflagge vor, obwohl auch diese Information für den Zweck der Tests nicht erforderlich war.

Bei optionalen Angaben in Onlineformularen sollte die Voreinstellung grundsätzlich ein leeres Feld sein. Vorausgewählte Einstellungen (in diesem Fall die deutsche Staatsangehörigkeit) verstoßen bei optionalen Feldern in der Regel gegen den Datenschutz durch datenschutzfreundliche Voreinstellungen (sog. Privacy by Default).[196] Die betroffenen Personen werden durch diese Vorauswahl nämlich im Sinne eines sog. Opt-out gezwungen, die Voreinstellung zu korrigieren. Mit einem leeren Standardfeld als technische Voreinstellung wäre dafür gesorgt, dass die optionale Angabe der Kund:innen nur dann erhoben wird, wenn die Kund:innen diese auch tatsächlich machen wollen. Ein Opt-out kann hingegen dazu führen, dass Kund:innen die Voreinstellung aus Bequemlichkeit, oder weil sie es übersehen, nicht ändern.

In einem ähnlich gelagerten Fall haben wir gegen ein Unternehmen, das ebenfalls Corona-Teststationen betreibt, einen Bußgeldbescheid erlassen, weil dieses u. a. die Ausweis- bzw. Passnummer, den Impfstatus und die Staatsangehörigkeit bei der Onlineanmeldung für einen Corona-Test als Pflichtangaben erhob. Ein weiteres Unternehmen, das Corona-Teststationen betreibt, hatte zu einer Beschwerdeführerin, die sich zunächst für einen Test angemeldet, diesen jedoch nicht wahrgenommen hatte, diverse Informationen im eigenen Webportal fortlaufend gespeichert. Dies wurde trotz eines Löschungsantrags der Beschwerdeführerin und unserer Intervention als Aufsichtsbehörde nicht geändert. In einem weiteren Fall wurden Daten der Kund:innen in Papierform erhoben. Das von uns sanktionierte Unternehmen entsorgte die Anmel

196 Siehe Art. 25 Abs. 2 Satz 1 Datenschutz-Grundverordnung (DSGVO).

debögen allerdings nicht ordnungsgemäß. Stattdessen wurden ausgefüllte Anmeldebögen – in Müllsäcken gemeinsam mit benutzten Corona-Tests – auf offener Straße gefunden. Ebenso unterblieb eine entsprechende Datenpannenmeldung durch das Unternehmen bei unserer Behörde, was wir mit einem rechtskräftigen Bußgeld sanktioniert haben.

Die Inanspruchnahme der Dienstleistungen von Testzentren war während der Pandemie die Voraussetzung für die Teilhabe an vielen Bereichen des gesellschaftlichen Lebens. Dabei haben wir eine große Bandbreite von Datenschutzverstößen festgestellt, bei denen oftmals die Sanktionierung mit Bußgeldern geboten war.

12.3 Bußgelder wegen unbefugter Nutzung der Polizeidatenbank und von Kontaktdaten aus dem Polizeidienst

Auch in diesem Jahr führten wir viele Bußgeldverfahren gegen Polizeibedienstete, die unbefugt, d. h. ohne dienstlichen Anlass, personenbezogene Daten aus der polizeiinternen Datenbank POLIKS abriefen oder anderweitig dienstlich erlangte Kontaktdaten für private Zwecke nutzten.

POLIKS ist eines der wichtigsten elektronischen Informationssysteme der Berliner Polizei und enthält dementsprechend umfangreiche Datensätze. In POLIKS werden insbesondere Daten von Beschuldigten, Straftäter:innen, Opfern und Zeug:innen gespeichert. Dazu gehören Informationen wie Namen, Geburtsdaten, Anschriften, aber auch Vorstrafen und Zeugenaussagen. Die Polizei nutzt POLIKS als Informationssystem für ihre gesetzlichen Aufgaben im Bereich der Strafverfolgung und Gefahrenabwehr. Polizeibedienstete werden in regelmäßigen Abständen über datenschutzrechtliche Vorschriften informiert und darüber belehrt, dass es ihnen ausdrücklich untersagt ist, Daten aus POLIKS und anderen polizeilichen Informationssystemen für private Zwecke zu nutzen. Dennoch wird der Zugang zu POLIKS immer wieder dazu missbraucht, Personen – etwa aus dem persönlichen Umfeld – ohne dienstlich veranlassten Grund abzufragen und so insbesondere Informationen über deren Lebensumstände zu erfahren. Beispielsweise fragte eine Polizeibeamtin Informationen zu

ihrem neuen Lebenspartner ab, um zu prüfen, ob dieser polizeilich in Erscheinung getreten war.

Im Rahmen ihrer täglichen Arbeit – etwa bei Einsätzen oder der Vernehmung von Zeug:innen – erlangen Polizeibedienstete regelmäßig Kenntnis von den Kontaktdaten von Personen. Wir haben mehrere Fälle sanktioniert, in denen diese dienstlich erlangten Informationen anschließend zu privaten Zwecken durch die Polizeibediensteten verwendet wurden. In einem uns vorliegenden Fall hat ein Polizeibeamter die Telefonnummer eines Einbruchsopfers, die er im Rahmen eines Polizeieinsatzes dienstlich in Erfahrung gebracht hatte, in sein privates Mobiltelefon gespeichert, um die Frau danach sexuell motiviert zu kontaktieren. In einem anderen Fall hat ein Polizeibeamter die Handynummer einer Frau, die ihm im Rahmen seines Notrufdiensts bekannt geworden war, ebenfalls zur privaten Kontaktaufnahme genutzt.

Wir haben in diesem Jahr 18 Verfahren gegen Polizeibedienstete eingeleitet und 16 Bußgeldbescheide mit insgesamt 124 Bußgeldern gegen Polizeibedienstete erlassen. Obwohl wir seit vielen Jahren die unbefugte Nutzung dienstlich erlangter personenbezogener Daten sanktionieren, beobachten wir leider weiterhin rechtswidrige Abrufe bei Polizeibediensteten.

12.4 Unbefugte Datenbankabfragen durch Mitarbeiter:innen der Jobcenter

Regelmäßig führen wir Bußgeldverfahren gegen Beschäftigte der Jobcenter, die im Rahmen ihrer Tätigkeit auf verschiedene Datenbanken Zugriff haben, diese Zugriffsmöglichkeit aber für zweckfremde Abfragen nutzen.

In einem Fall hat eine Mitarbeiterin wiederholt und unbefugt Informationen zu ihrer Nachbarin in den elektronischen Informationssystemen des Jobcenters abgefragt. In einem weiteren Fall haben wir ein Bußgeld erlassen, weil ein Mitarbeiter in dem zur zentralen Verfahrensbetreuung verwendeten Portal zur Onlinemelderegisterauskunft (OLMERA) Informationen über eine Kollegin zu privaten Zwecken abfragte.

In diesem Jahr haben wir insgesamt 6 Verfahren gegen Mitarbeitende von Jobcentern, Landes- und Bezirksämtern eingeleitet und 4 Bußgeldbescheide mit 171 Bußgeldern erlassen.

12.5 Das Zwei-Augen-Prinzip: Interessenkonflikt eines betrieblichen Datenschutzbeauftragten innerhalb einer Konzernstruktur

Wir haben gegen die Tochtergesellschaft eines Handelskonzerns ein Bußgeld in Höhe von 525.000 Euro wegen eines Interessenkonflikts des betrieblichen Datenschutzbeauftragten verhängt. Das Unternehmen hatte einen Datenschutzbeauftragten benannt, der Entscheidungen unabhängig kontrollieren sollte, die er selbst in einer anderen Funktion getroffen hatte. Das Bußgeld ist noch nicht rechtskräftig.

Betriebliche Datenschutzbeauftragte haben eine wichtige Aufgabe: Sie beraten das Unternehmen hinsichtlich der datenschutzrechtlichen Pflichten und kontrollieren die Einhaltung der Datenschutzvorschriften. Diese Funktion dürfen ausschließlich Personen ausüben, die keinem Interessenkonflikt durch andere Aufgaben unterliegen.[197] Ein Interessenkonflikt bestünde bspw. bei Personen mit leitender Funktion, die selber maßgebliche Entscheidungen über die Verarbeitung von personenbezogenen Daten im Unternehmen treffen. Die Aufgabe darf demnach nicht von Personen wahrgenommen werden, die sich dadurch selbst überwachen würden.

Ein solcher Interessenkonflikt lag im Falle eines Datenschutzbeauftragten einer Tochtergesellschaft eines E-Commerce-Konzerns vor. Die Person war zugleich Geschäftsführer von zwei Dienstleistungsgesellschaften, die im Auftrag desjenigen Unternehmens personenbezogene Daten verarbeiteten, für das er als Datenschutzbeauftragter benannt war. Die von ihm geführten Dienstleistungsgesellschaften sind ebenfalls Teil des Konzerns, umfassen den Kundenservice und führen Bestellungen aus. Der Datenschutzbeauftragte musste somit die Einhaltung des Datenschutzrechts durch die im Rahmen der Auftragsverarbeitung tätigen Dienstleistungsgesellschaften überwachen,

197 Art. 38 Abs. 6 Satz 2 DSGVO.

die von ihm selbst als Geschäftsführer geleitet wurden. Damit bestand ein Interessenkonflikt und folglich ein Verstoß gegen die DSGVO.

Als Aufsichtsbehörde erteilten wir daher im Jahr 2021 zunächst eine Verwarnung gegen das Unternehmen. Nachdem eine erneute Überprüfung in diesem Jahr ergab, dass der Verstoß trotz der Verwarnung weiterhin bestand, verhängten wir das Bußgeld. Bei der Bußgeldzumessung berücksichtigten wir den dreistelligen Millionenumsatz des E-Commerce-Konzerns im vorangegangenen Geschäftsjahr und die Rolle des Datenschutzbeauftragten als Ansprechpartner für eine hohe Zahl an Beschäftigten und Kund:innen. Berücksichtigung fand auch die vorsätzliche Weiterbenennung des Datenschutzbeauftragten über den Zeitraum von fast einem Jahr trotz der bereits durch uns erteilten Verwarnung. Als bußgeldmindernd wurde u. a. eingestuft, dass das Unternehmen umfangreich mit uns zusammengearbeitet und den Verstoß während des laufenden Bußgeldverfahrens abgestellt hat.

Dieses Bußgeld unterstreicht die wichtige Funktion von Datenschutzbeauftragten in Unternehmen. Datenschutzbeauftragte können nicht einerseits die Einhaltung des Datenschutzrechts überwachen und andererseits darüber mitentscheiden. Eine solche Selbstkontrolle widerspricht der Stellung von Datenschutzbeauftragten als unabhängige Instanz, die im Unternehmen auf die Einhaltung des Datenschutzes hinwirken soll. Zur Vermeidung von Datenschutzverstößen sollten Unternehmen etwaige Doppelrollen der betrieblichen Datenschutzbeauftragten in Konzernstrukturen auf mögliche Interessenkonflikte hin prüfen. Das gilt insbesondere dann, wenn Auftragsverarbeitungen oder gemeinsame Verantwortlichkeiten zwischen den Konzerngesellschaften bestehen.

12.6 Der Mann mit den 13 Geburtstagen

Falsche Einträge und eine verspätete Auskunft führten für den Betreiber einer Wirtschaftsauskunftei zu zwei Bußgeldern in Höhe von insgesamt 46.500 Euro.

Entgegen der gesetzlichen Vorgaben[198] waren in der betreffenden Wirtschaftsauskunftei mehr als zwei Jahre lang insgesamt 27 falsche Anschriften und 13 falsche Geburtsdaten zu einem unserer Beschwerdeführer gespeichert. Die Speicherung eines solchen „Datencocktails" in einer Auskunftei stellt eine erhebliche Gefährdungslage für die betroffenen Personen hinsichtlich ihrer wirtschaftlichen Leistungsfähigkeit dar. Der große Umfang falscher Daten suggerierte im konkreten Fall, dass der Beschwerdeführer bereits an über zwei Dutzend Adressen gewohnt hat, wodurch bei Dritten, die den Eintrag in der Wirtschaftsauskunftei übermittelt bekommen, ein negativer Eindruck entstehen kann.

Erst im Rahmen des Antrags der betroffenen Person auf Erteilung einer Auskunft über die vom Betreiber der Wirtschaftsauskunftei zu ihm verarbeiteten Daten wurden die falschen Angaben korrigiert. Zusätzlich erfolgte die Auskunftserteilung aufgrund interner Zuordnungsprobleme zunächst falsch als Negativauskunft und dann auch noch verspätet mit einer Verzögerung von mehr als drei Monaten. Da das Unternehmen von uns bereits vorher wiederholt wegen einschlägiger Verstöße verwarnt worden war, entschieden wir uns in diesem Fall zur Verhängung von Bußgeldern, die bereits rechtskräftig sind.

Es ist essenziell, dass die von einer Wirtschaftsauskunftei gesammelten personenbezogenen Daten richtig und klar einer Person zuzuordnen sind. Gerade durch Auskunfteien müssen insofern auch interne Strukturen im Unternehmen geschaffen werden, die dafür sorgen, dass Auskünfte[199] wahrheitsgemäß und fristgerecht[200] erteilt werden können.

198 Nach Art. 6 Abs. 1 Satz 1 DSGVO i. V. m. Art. 5 Abs. 1 lit. d DSGVO.
199 Nach Art. 15 Abs. 1 DSGVO.
200 Im Rahmen der einmonatigen Frist gemäß Art. 12 Abs. 3 Satz 1 DSGVO.

12.7 Veröffentlichung von Sportfotos Minderjähriger zum Onlineverkauf

In einem schwerwiegenden Bußgeldfall veröffentlichte ein Sportfotograf über 16.000 Fotos von Minderjährigen, die in Badekleidung an einem Schwimmwettbewerb teilgenommen hatten, auf einer frei zugänglichen Website zum Verkauf. Die Minderjährigen konnten nach Land und Altersklassen kategorisiert werden.[201]

Das Unternehmen, das die betreffende Website betreibt, bietet EU-weit Sportfotografie von Wettkämpfen an. Es konnte allerdings weder wirksame Einwilligungen der fotografierten Minderjährigen noch ihrer Eltern für die Aufnahme und Veröffentlichung der Fotos nachweisen. Auch eine Berufung auf das Presseprivileg vonseiten des Unternehmens scheiterte, da die Bilder weder redaktionell bearbeitet worden waren, noch eine Beschränkung ihrer Weiterverwendung für journalistische Zwecke erkennbar gewesen ist. Der von uns verhängte Bußgeldbescheid ist noch nicht rechtskräftig.

Für die kommerzielle Verwertung von Fotos ohne redaktionell-journalistischen Bezug bedarf es der Einwilligung der fotografierten Personen bzw. für den Fall, dass diese minderjährig sind, der Einwilligung ihrer Erziehungsberechtigten.

201 Siehe auch die Ausführungen zum zugehörigen Verwaltungsfall in JB 2021, 3.7.

13 Telekommunikation und Medien

13.1 Fonts in aller Munde

Ausgelöst durch ein Urteil des Landgerichts (LG) München zu Google Fonts haben Schriftarten auf Websites jüngst große Aufmerksamkeit erfahren. Für Unmut sorgten eine Fülle zivilrechtlicher Abmahnversuche. Viele Betreiber:innen haben den Aufruhr zum Anlass genommen, ihre Websites zu überarbeiten. Dabei sind nicht nur extern eingebundene Schriftarten in den Blick zu nehmen, sondern auch die übrigen eingesetzten Drittdienste kritisch zu überprüfen.

Für die optische und funktionale Gestaltung von Websites binden die Betreiber:innen häufig vorgefertigte Elemente ein, die von externen Dienstleister:innen zur Verfügung gestellt werden. Gängig ist dies insbesondere bei Fotos, Videos, Logos oder Landkarten. In den Fokus ist in diesem Jahr ein Dienst gerückt, der unscheinbar wirkt, für viele jedoch unverzichtbar ist: Schriftarten (Fonts). Ebenso wie andere externe Elemente können Schriftarten dynamisch oder lokal genutzt werden. Bei der dynamischen Einbindung werden die Schriftarten bei jedem Aufruf der Website simultan von Servern der Dienstleister:innen in den Browser der Nutzer:innen geladen. Hierbei wird mindestens die IP-Adresse an die externen Dienstleister:innen übermittelt, die ggf. außerhalb der Europäischen Union (EU) sitzen.

Um diese rechtfertigungsbedürftigen Datenströme auszusparen, können Schriftarten stattdessen auf eigenen Servern der Website-Betreiber:innen gespeichert und sodann lokal ausgeliefert werden. Die Umsetzung einer solchen lokalen Lösung können Betreiber:innen mithilfe von online frei verfügbaren Anleitungen und ohne großen Aufwand selbst vornehmen. Allerdings stellen wir fest, dass vielen Betreiber:innen gar nicht bewusst ist, welche Elemente in ihre Website eingebunden sind – gerade bei Website-Baukästen sind viele Dienste standardmäßig vorinstalliert. Auch dies können Website-Betreiber:innen anhand einer Netzwerkanalyse selbst überprüfen, die mithilfe der in allen Webbrowsern enthaltenen Entwicklerwerkzeuge durchgeführt werden kann.

Im Januar hat sich das LG München mit Schriftarten beschäftigt und mit einem Google Fonts betreffenden Urteil Aufmerksamkeit auf das Thema gelenkt.[202] Das Gericht stellte eine Verletzung des Rechts auf informationelle Selbstbestimmung und des Persönlichkeitsrechts fest, wenn Website-Betreiber:innen die dynamischen IP-Adressen von Dritten automatisiert und ohne deren Zustimmung an Google weiterleiten, sobald die Website aufgerufen wird. Eine Rechtsgrundlage für die Weitergabe der IP-Adressen liege nicht vor, da das Angebot von Google Fonts auch genutzt werden könne, ohne dass beim Aufruf der Website eine Verbindung zu einem Google-Server hergestellt wird und eine Übertragung der IP-Adressen der Website-Nutzer:innen an Google stattfindet. Kernkritik des Gerichts war demnach der Transfer von Daten in die USA ohne Rechtsgrundlage, obwohl dies ohne Not und Aufwand vermeidbar wäre. Dem Kläger wurde vom Gericht sodann ein Schadensersatz von 100 Euro zuerkannt.

In der Folge gingen bei uns nicht nur viele Beschwerden über den Einsatz von Google Fonts auf Websites ein, sondern auch Beratungsersuchen stiegen deutlich an. Ursache hierfür war eine Fülle kampagnenartiger Abmahnversuche. Zehntausende Website-Betreiber:innen wurden wegen des Einsatzes von Google Fonts zivilrechtlich abgemahnt, zudem wurde Schadensersatz von ihnen verlangt. Aufgrund unserer originären Aufgabenzuweisung der Kontrolle datenschutzrechtlicher Vorgaben kann durch uns keine Rechtsberatung zum Umgang mit solchen Abmahnschreiben erfolgen. Um Website-Betreiber:innen bei der Gestaltung ihrer Website aber datenschutzrechtlich zu unterstützen, haben die deutschen Aufsichtsbehörden bereits in der Vergangenheit Leitlinien zum Thema veröffentlicht. Hierzu zählt u. a. die Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) für Anbieter:innen von Telemedien, die alle potenziellen Probleme rund um den Einsatz von Drittdiensten auf Websites adressiert.[203]

202 Siehe LG München I, Urteil vom 20. Januar 2022, 3 O 17493/20.

203 Siehe DSK: „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021“, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2022_OH_Telemedien.pdf; zur Aktualisierung der Orientierungshilfe nach Durchführung eines Konsultationsverfahrens siehe 13.2.

Bei allem Aufruhr rund um das Thema Fonts sollte nicht aus dem Blick geraten, dass bei den meisten Websites umfangreichere Aspekte für einen datenschutzkonformen Betrieb zu klären sind als die Nutzung eines einzelnen Schriftartendiensts. Unabhängig von potenziellen Abmahnungen sollten Website-Betreiber:innen das aktuelle Aufsehen zum Anlass nehmen, um in Erfahrung zu bringen, welche Drittdienste tatsächlich in ihre Websites eingebunden sind. Die kritische Überprüfung sollte sich nicht auf die Nutzung von Schriftarten beschränken, sondern stets auch die übrigen eingesetzten Drittdienste umfassen.

13.2 Ergebnisse des ersten DSK-Konsultationsverfahrens zur Orientierungshilfe für Anbieter:innen von Telemedien

Im Dezember 2021 hatte die DSK eine neue Orientierungshilfe für Anbieter:innen von Telemedien verabschiedet.[204] Im Anschluss an die Veröffentlichung wurde betroffenen Akteur:innen im Rahmen eines Konsultationsverfahrens Gelegenheit gegeben, zu den Inhalten der Orientierungshilfe Stellung zu nehmen. Alle eingegangenen Stellungnahmen wurden zwischenzeitlich ausgewertet und eine aktualisierte Version der Orientierungshilfe veröffentlicht. Im Ergebnis wurden einzelne Rechtsansichten präzisiert und zwei Kapitel mit praktischen Ergänzungen eingefügt.

In Anlehnung an die Praxis des Europäischen Datenschutzausschusses (EDSA) hat sich die DSK dazu entschieden, hinsichtlich der Orientierungshilfe auch interessierte Kreise einzubeziehen. Das Konsultationsverfahren dient der Überprüfung und ggf. der Fortentwicklung der Orientierungshilfe, soll aber nicht ihre Geltung und Anwendung in der Praxis berühren.

Innerhalb der zweimonatigen Konsultationsfrist sind insgesamt 14 Stellungnahmen eingegangen.[205] Diese wurden gesichtet und ausgewertet sowie daraufhin überprüft, ob sich Änderungsbedarf für die Veröffentlichung ergibt. Die Auswertung wurde in einem umfassenden Bericht festgehalten, der von der DSK am 5. Dezember dieses Jahres

204 Siehe JB 2021, 14.2.

205 Diese sind über die Website der DSK unter https://www.datenschutzkonferenz-online.de/konsultationsverfahren.html abrufbar.

zusammen mit der aktualisierten Version der Orientierungshilfe veröffentlicht wurde.[206] Die vorgenommenen Änderungen präzisieren oder konkretisieren im Wesentlichen einige Aussagen zu den Rechtsansichten und Bewertungen der Aufsichtsbehörden. Darüber hinaus wurden zwei neue Kapitel zur Gestaltung von Einwilligungsbannern sowie zu den Betroffenenrechten im Zusammenhang mit dem Einsatz von Cookies ergänzt. Beide Kapitel haben große Praxisrelevanz, da sich Beschwerden bei den Aufsichtsbehörden vielfach gegen die Gestaltung von Bannern und – neuerdings deutlich zunehmend – gegen unerfüllte Auskunftsersuchen im Zusammenhang mit Cookies richten.

Wir empfehlen Website-Betreiber:innen, sich insbesondere mit den beiden neuen Kapiteln der „Orientierungshilfe für Anbieter:innen von Telemedien“ vertraut zu machen. Diese behandeln die konkrete Gestaltung von Einwilligungsbannern sowie die Einhaltung von Betroffenenrechten im Zusammenhang mit dem Einsatz von Cookies.

13.3 Onlinespiele: Rechtmäßige Adressänderung oder heimliche Kontoübertragung?

Uns erreichen viele Beschwerden zu Onlinespielen. In der Praxis stehen häufig die berechtigten Interessen der Anbieter:innen an einer effektiven Durchsetzung der Spielregeln den Interessen von Spieler:innen bei der Geltendmachung ihrer Betroffenenrechte gegenüber.

In einem Fall wollte ein Spieler die E-Mail-Adresse seines Spielerkontos ändern. Der Spieler machte geltend, er habe ein Recht auf Berichtigung seiner Daten. Das anbietende Unternehmen vermutete allerdings, dass der Spieler sein Konto mit dieser Änderung einem anderen Spieler übertragen wolle. Dies war nach den Spielregeln verboten. Hintergrund dieser Regeln ist, dass Spieler:innen ihren Spielfortschritt selbst erreichen sollen, um einen ehrlichen Wettkampf zu ermöglichen. Das Unternehmen verwehrte dem Spieler die Änderung zunächst mit der Begründung, diese sei technisch nicht möglich, räumte dann aber im Rahmen des Verfahrens ein, dass die Änderung

206 Abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2022_OH_Telemedien.pdf.

der E-Mail-Adresse zwar möglich, aber mit einem hohen Aufwand verbunden sei. Es müsse sichergestellt werden, dass die neue E-Mail-Adresse tatsächlich derselben Person gehöre. Das Unternehmen war der Ansicht, es handele sich bei der Änderung einer E-Mail-Adresse nicht um eine Berichtigung der Daten, da die alte E-Mail-Adresse weiter gültig und somit nicht falsch sei.

Dieser Einwand konnte nicht greifen: Es steht grundsätzlich jeder Person frei, zu entscheiden, welche E-Mail-Adresse sie für welchen Kommunikationszweck oder für welche Kommunikationspartner:innen nutzen möchte. Insbesondere muss es jeder Person gestattet sein, eine bestimmte E-Mail-Adresse nach und nach aus dem Verkehr zu ziehen, um sie irgendwann abschalten zu können, z. B. weil die Person den E-Mail-Provider wechseln möchte oder weil sie zu viele unerwünschte E-Mails über eine bestimmte Adresse erreichen. Die Richtigkeit einer E-Mail-Adresse setzt demnach nicht nur voraus, dass sie der betroffenen Person objektiv zugeordnet werden kann. Erforderlich ist auch, dass eine E-Mail-Adresse von der betroffenen Person für den spezifischen Kommunikationszweck bestimmt worden ist. Diese Bestimmung kann die betroffene Person im Lauf der Zeit auch ändern. So kann eine ehemals richtige E-Mail-Adresse unrichtig werden. Ein Unternehmen ist dann grundsätzlich verpflichtet, diese auf Antrag zu ändern. Dabei darf das Unternehmen jedoch Maßnahmen ergreifen, um sicherzustellen, dass die neue E-Mail-Adresse tatsächlich derselben Person gehört. Wir haben gegen das Unternehmen eine Verwarnung ausgesprochen, da dieses den Berichtigungsantrag ohne weitere Prüfung abgelehnt und dem Spieler zunächst eine falsche Begründung für die Ablehnung genannt hat.

Wenn eine Person ihre E-Mail-Adresse in einem Onlinekonto ändern möchte, stellt dies regelmäßig einen Antrag auf Berichtigung der personenbezogenen Daten dar. Bei Zweifeln an der Rechtmäßigkeit der Berichtigung kann das Unternehmen Maßnahmen zur Überprüfung ergreifen.

13.4 Erhebung der Telefonnummer als Pflichtfeld

Ein Unternehmen bietet die Nutzung digitaler Medieninhalte über das Internet im Rahmen eines kostenpflichtigen Abonnements an. Uns erreichte eine Beschwerde, dass das Unternehmen von Kund:innen, die die kostenpflichtige Variante des Angebots wählten, eine Telefonnummer als Pflichtangabe erhob.

Nach Ansicht des Unternehmens war die Erhebung der Telefonnummer für die Vertragserfüllung[207] erforderlich: Falls Kund:innen ein Problem bei der Nutzung des Angebots haben, das nicht per E-Mail oder Chat zu lösen sei, würden die Mitarbeiter:innen des Unternehmens die Kund:innen persönlich am Telefon unterstützen. Zudem sei die Kenntnis und Nutzung der Telefonnummer auch zur Missbrauchs- und Betrugsprävention notwendig: So könnten bei einem vermuteten Fremdzugriff auf das Kundenkonto oder bei fehlerhaften Abbuchungen und entsprechender Sperrung des Kontos die Kund:innen per SMS benachrichtigt werden. Hilfsweise könne die zwangsweise Erhebung der Telefonnummer und deren Nutzung für die o. g. Zwecke auch auf berechtigte Interessen des Unternehmens gestützt werden.[208]

Die verpflichtende Angabe der Telefonnummer zu Servicezwecken bzw. zur Missbrauchs- und Betrugsprävention ist für den Abschluss und die Durchführung von Nutzungsverträgen mit dem Unternehmen im Sinne der DSGVO nicht erforderlich. Für die Durchführung des Kundenservice reichen die übrigen dem Unternehmen zur Verfügung stehenden Kommunikationskanäle aus, insbesondere durch die Möglichkeit der Nutzung der vorliegenden E-Mail-Adresse und durch das Angebot an betroffene Personen, sich selbst telefonisch an den Kundenservice des Unternehmens zu wenden. Für die Betrugs- und Missbrauchsprävention stehen andere Optionen als die Nutzung der Telefonnummer zur Verfügung, wie bspw. die E-Mail-Benachrichtigung bei Log-in-Versuchen oder die Verwendung einer eigens dafür eingerichteten App.

Die zwangsweise Erhebung der Telefonnummer kann auch nicht auf berechtigte Interessen des Unternehmens gestützt werden:[209] Zwar hat dieses grundsätzlich ein berechtigtes (wirtschaftliches) Interesse an der Erhebung und Verarbeitung der Daten

207 Art. 6 Abs. 1 Satz 1 lit. b Datenschutz-Grundverordnung (DSGVO).
208 Siehe Art. 6 Abs. 1 Satz 1 lit. f DSGVO.
209 Siehe ebd.

der Kund:innen. Jedoch fehlt es für eine zwangsweise Erhebung der Telefonnummer auch hier an der vom Gesetz vorausgesetzten Erforderlichkeit: Die Kundenzufriedenheit und eine wirksame Missbrauchs- oder Betrugsprävention können ebenso gut dadurch sichergestellt werden, dass das Unternehmen seinen Kund:innen die Angabe einer Telefonnummer für die genannten Zwecke freistellt, sodass diejenigen Kund:innen, die von dem Serviceangebot Gebrauch machen wollen, ihre Telefonnummer angeben können, während diejenigen Kund:innen, die darauf verzichten wollen, keine Angabe leisten müssen. Im Ergebnis ist die zwangsweise Erhebung und weitere Verarbeitung der Telefonnummer der betroffenen Personen nicht erforderlich, um berechtigte Interessen des Unternehmens zu wahren.

Im Rahmen einer Interessenabwägung mit den Interessen der betroffenen Personen wäre zudem der entgegenstehende Wille jener Personen beachtlich, die die Nutzung ihrer Telefonnummer für die genannten Zwecke nicht wünschen. Zugleich verstößt eine zwangsweise Erhebung der Telefonnummer gegen die Verpflichtung zur Datenminimierung.[210] Für die Erhebung der Telefonnummer ist überdies die Einholung einer Einwilligung notwendig.[211] Bei der Einwilligung im Sinne der DSGVO muss es sich um eine freiwillig „für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung“ handeln.[212] Freiwilligkeit liegt aber nicht vor, wenn die Telefonnummer als Pflichtangabe ausgestaltet ist. Aufgrund unserer Intervention hat das Unternehmen die Telefonnummer des Beschwerdeführers gelöscht und uns außerdem mitgeteilt, zukünftig auf die Erhebung von Telefonnummern als Pflichtfeld zu verzichten. Wir haben eine Verwarnung ausgesprochen.

Die Erhebung von Telefonnummern als Pflichtfeld in Internetangeboten muss entweder für die Vertragserfüllung mit den betroffenen Personen oder für berechtigte Interessen der Verantwortlichen erforderlich sein. Wo dies nicht der Fall ist, müssen die Verantwortlichen eine (freiwillige) Einwilligung ihrer Kund:innen in die Erhebung und die beabsichtigte Nutzung einholen.

210 Art. 5 Abs. 1 lit. c DSGVO.
211 Art. 6 Abs. 1 Satz 1 lit. a DSGVO.
212 Art. 4 Nr. 11 DSGVO.

13.5 Novellierung des RBB-Staatsvertrags

Die Staatskanzlei des Landes Brandenburg und die Berliner Senatskanzlei arbeiten gegenwärtig an der Novellierung des Staatsvertrags über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg (RBB-Staatsvertrag). Dabei ist nach dem derzeit bekannten Entwurfsstand u. a. geplant, die Kontrolle der Einhaltung von Datenschutzbestimmungen auch im sog. wirtschaftlich-administrativen Bereich der oder dem Datenschutzbeauftragten des RBB zu übertragen.

Bisher unterliegt die Kontrolle der Einhaltung von Datenschutzbestimmungen bei der Verarbeitung personenbezogener Daten für journalistische Zwecke der Datenschutzbeauftragten des RBB, während die Kontrolle im wirtschaftlich-administrativen Bereich – dies betrifft vor allem die Daten von Rundfunkteilnehmer:innen zum Einzug des Rundfunkbeitrags sowie die Daten von Beschäftigten des RBB und seiner Hilfs- und Beteiligungsunternehmen – unserer Behörde zugewiesen ist. Diese Aufteilung wird auch in Brandenburg, Bremen und Hessen praktiziert. In den übrigen Bundesländern obliegt die Kontrolle für beide Bereiche den Datenschutzbeauftragten der jeweiligen Rundfunkanstalt. Der derzeitige Entwurf zur Änderung des RBB-Staatsvertrags sieht vor, dass zukünftig auch in Berlin und Brandenburg die Kontrolle für beide Bereiche durch die oder den Datenschutzbeauftragte:n des RBB erfolgen soll.

In einer gemeinsamen Stellungnahme mit der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA) Brandenburg haben wir insbesondere darauf hingewiesen, dass die vorgeschlagene vollständige Übertragung der Datenschutzkontrolle auf die oder den Datenschutzbeauftragte:n des RBB nicht mit den Bestimmungen der DSGVO vereinbar ist: Abweichungen von Kapitel VI der DSGVO, das Regelungen zu den unabhängigen Aufsichtsbehörden enthält, sind nur zulässig, wenn dies bei der Verarbeitung personenbezogener Daten für journalistische Zwecke erforderlich ist, „um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen“.[213] Dies gilt nicht für die Verarbeitung personenbezogener Daten im wirtschaftlich-administrativen Bereich und insbesondere nicht für die Verarbeitung personenbezogener Daten von Rundfunkbeitragszahler:innen und von Beschäftigten des RBB und

213 Art. 85 Abs. 2 DSGVO.

dessen Hilfs- und Beteiligungsunternehmen. Die im Entwurf vorgesehene Übertragung der Kontrolle der Einhaltung von Datenschutzbestimmungen auf eine oder einen internen Rundfunkdatenschutzbeauftragte:n auch für die Verarbeitung personenbezogener Daten im wirtschaftlich-administrativen Bereich verstößt daher gegen die Vorschriften der DSGVO und ist somit europarechtswidrig.

Auch das im Entwurf vorgesehene Verfahren zur Ernennung einer oder eines Rundfunkdatenschutzbeauftragten für die Kontrolle der Verarbeitung personenbezogener Daten außerhalb der Datenverarbeitung für journalistische Zwecke halten wir für europarechtswidrig: Nach der uns bei Redaktionsschluss vorliegenden Fassung des neuen Staatsvertrags sollen bei der Ernennung lediglich der Rundfunkrat bzw. die Intendantin oder der Intendant des RBB mit Zustimmung des Verwaltungsrats mitwirken. Nach der DSGVO obliegt die Ernennung aber dem Parlament, der Regierung, dem Staatsoberhaupt oder einer unabhängigen Stelle, die nach dem Recht des EU-Mitgliedstaats mit der Ernennung betraut wird.[214] Die Ernennung durch eine unabhängige Stelle, wie z. B. eine Wahlkommission, kann nur dann zulässig sein, wenn diese Stelle ihrerseits über eine ausreichende demokratische Legitimation verfügt. Der Rundfunk- und der Verwaltungsrat des RBB sind aufgrund des im Entwurf vorgesehenen (und bisher auch schon so praktizierten) Benennungsverfahren für ihre Mitglieder jedoch keine unabhängigen Stellen im Sinne dieser Vorschrift. Von den dann 33 Mitgliedern des Rundfunkrats werden nur sieben Mitglieder vom Landtag Brandenburg und vom Abgeordnetenhaus entsandt, die auf Vorschlag der jeweiligen Fraktionen gewählt werden.[215] Mehrheitlich werden die Mitglieder des Rundfunkrats dagegen nicht gewählt, sondern von den zahlreichen im Staatsvertrag genannten Institutionen und Einrichtungen (z. B. Kirchen, Unternehmensverbände, Gewerkschaften und andere gesellschaftliche Gruppen) entsandt.[216] Der Verwaltungsrat wiederum besteht aus sieben vom Rundfunkrat gewählten Mitgliedern und einem vom Personalrat entsandten Mitglied.[217] Rundfunkrat und Verwaltungsrat verfügen damit nicht über eine ausreichende demokratische Legitimation im Sinne von Art. 53 Abs. 1 DSGVO für die Ernennung von Mitgliedern einer unabhängigen Aufsichtsbehörde für den Datenschutz. Auch geht der Ernennung kein Vorschlag der Regierung oder eines ihrer Mit

214 Art. 53 Abs. 1 DSGVO.
215 Dies entspricht der bisherigen Regelung in § 14 Abs. 1 Nr. 24 RBB-Staatsvertrag.
216 Siehe § 14 Abs. 1 RBB-Staatsvertrag.
217 Siehe § 19 Abs. 1 RBB-Staatsvertrag.

glieder, des Parlaments oder einer Parlamentskammer voraus, wie dies in der DSGVO vorgesehen ist.[218]

Die bislang in Berlin und Brandenburg praktizierte Aufsichtsstruktur hat sich bewährt, nach der unsere Behörde im Benehmen mit der LDA Brandenburg für die Aufsicht über die Verarbeitung personenbezogener Daten im wirtschaftlich-administrativen Bereich zuständig ist, während die Aufsicht über die Verarbeitung personenbezogener Daten für journalistische Zwecke durch die bzw. den Datenschutzbeauftragte:n des RBB erfolgt. Zu einer Veränderung besteht aus unserer Sicht keine Veranlassung.

Die Kontrolle der Einhaltung von Datenschutzbestimmungen im wirtschaftlich-administrativen Bereich des RBB sollte wie bisher durch unsere Behörde im Benehmen mit der LDA Brandenburg wahrgenommen werden. Eine Übertragung auf die oder den Datenschutzbeauftragte:n des RBB ist europarechtlich nicht möglich.

218 Siehe Erwägungsgrund (EG) 121 Satz 1 DSGVO.

14 Politische Parteien

14.1 Der Zukauf von Adressen befreit nicht von Pflichten

Bei uns beschwerte sich ein Bürger, der persönlich adressierte Wahlwerbung des Landesverbands einer politischen Partei in seinem Briefkasten fand. Er hatte der werbenden Partei weder seine Adresse genannt, noch sonst mit ihr in Verbindung gestanden. Die Angaben im Impressum der Werbebroschüre brachten ihn nicht weiter, denn sie führten lediglich zu einem Adresshändler.

Unser Beschwerdeführer schrieb daher die Partei an und fragte dort nach. Man sah sich zunächst als nicht zuständig und stellte sich auf den Standpunkt, dass man die Adressen zugekauft und die Werbung über einen sog. Lettershop vom Adressdienstleister versenden habe lassen. Selber habe man die Adressen nie in der Hand gehabt, sondern nur Inhalte beigesteuert. Im Rahmen unserer Prüfung stellte sich heraus, dass die Partei den Listeneigner insbesondere damit beauftragt hatte, Adressen zu übermitteln, die bestimmten Selektionskategorien entsprachen: So sollten die Angeschriebenen bspw. „Performer-ähnliche Merkmale“ aufweisen, „[Partei-]affin und jünger als 60 Jahre“ sein. Aus den Datensätzen sollten zudem bestimmte politische Einstellungen und die Zugehörigkeit zu bestimmten sozialen Milieus ersichtlich werden.

Wir haben den Landesverband der Partei aus mehreren Gründen verwarnt: Adresshändler und Partei waren vorliegend gemeinsam Verantwortliche, da weder der Adresshändler noch die Partei ohne den jeweils anderen Teil über die Auswahl der Adressen abschließend entscheiden konnte. Dafür spielt es keine Rolle, ob die Partei unmittelbaren Zugriff auf die Daten hatte.[219] Die Daten waren ohne Rechtsgrundlage verarbeitet worden, da keine Einwilligung des Angeschriebenen in den Empfang von

219 Siehe Europäischer Gerichtshof (EuGH), Urteil vom 10. Juli 2018, C 25/17, Rn. 68 f.

Parteiwerbung vorlag.[220] Gleichzeitig war die Partei ihren Informations- und Auskunftspflichten nicht nachgekommen.[221] Die Partei hat gegen unsere Verwarnung Klage beim Verwaltungsgericht erhoben, über die noch nicht entschieden wurde.

14.2 Fake-Testimonials im Wahlkampf?

Im September 2021 erhielten Bürger:innen personalisierte Schreiben, in denen sie von Persönlichkeiten aus Politik und Wirtschaft dazu aufgerufen wurden, einen bestimmten Bundestagskandidaten zu wählen. Die Schreiben vermitteln mangels weiterer Informationen den Eindruck, sie wären direkt von den Personen versandt, die werbend für den Kandidaten eintreten.

Selbst wenn die Schreiben inhaltlich in Abstimmung mit den vermeintlichen Absender:innen gestaltet wurden, so stammten die Adressen der Angeschriebenen aus dem Melderegister und waren dort vom Bezirksverband der Partei, für die geworben wurde, abgerufen worden. Der Abruf erfolgte auf der Grundlage der spezifisch für Parteien geregelten Befugnis im Bundesmeldegesetz (BMG).[222] Der Bezirksverband übermittelte die Adressen sodann einem Werbeanbieter[223] und beauftragte diesen mit dem massenhaften Versand der Empfehlungen (Testimonials). Trotz entsprechender Auskunftsersuchen unsererseits konnte der Bezirksverband der Partei keinen Auftragsverarbeitungsvertrag[224] vorlegen, womit bereits die Weitergabe der Adressen an den Werbeanbieter unzulässig war. Auch besteht kein berechtigtes Interesse an der Verarbeitung der Daten durch den Bezirksverband, wenn die Betroffenen im Unklaren darüber gelassen werden, wer Urheber:in der Wahlwerbung ist. Weiterhin hat der Bezirksverband der Partei durch die Gestaltung der Schreiben gegen seine Informations- und Transparenzpflichten verstoßen. Für die Empfänger:innen sind dies aber wichtige Informationen – wie etwa: Woher hat die Partei

220 Grundsätzlich dürfen Parteien nach § 50 Bundesmeldegesetz (BMG) Adressen aus dem Melderegister erhalten. Dagegen besteht ein Widerspruchsrecht, allerdings nicht hinsichtlich des Zukaufs von Adressen. Zudem erlaubt § 50 Abs. 1 BMG auch nur sehr begrenzte Auswahlkriterien (etwa die Altersgruppe). Werbung, die über das nach § 50 BMG Zulässige hinausgeht, ist nur mit Einwilligung erlaubt.
221 Siehe Art. 14, 15 Datenschutz-Grundverordnung (DSGVO).
222 Siehe § 50 Abs. 1 BMG.
223 Im sog. Lettershop-Verfahren; siehe 14.1.
224 Gemäß Art. 28 Abs. 3 DSGVO.

meine Daten? Wer hat meine Daten verarbeitet? Welche Rechtsbehelfe stehen mir zur Verfügung?

Angesichts der hohen Zahl an Betroffenen und der Schwere der Verstöße haben wir den Vorgang unserer Sanktionsstelle zur weiteren Bearbeitung übergeben.

15 Europa und Internationales

15.1 Einheitliche Leitlinien zur Bußgeldbemessung

Im Mai hat der Europäische Datenschutzausschuss (EDSA) neue Leitlinien zur Bemessung von Bußgeldern beschlossen.[225] Damit haben sich die europäischen Datenschutzaufsichtsbehörden auf eine einheitliche Bußgeldpraxis geeinigt.

Unsere Behörde hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in der EDSA-Arbeitsgruppe „Bußgelder" vertreten und die Leitlinien maßgeblich mitentwickelt. Die Leitlinien sehen ein aus fünf Schritten bestehendes Bemessungsverfahren vor, das die Art und Schwere der Verstöße sowie den Umsatz der betreffenden Unternehmen berücksichtigt:

Im ersten Schritt des Bemessungsverfahrens wird festgestellt, ob der betreffende Fall sanktionierbare Handlungen umfasst und inwieweit diese zu Verstößen geführt haben. Dabei wird geklärt, ob sämtliche oder nur einige Verstöße mit einer Geldbuße geahndet werden können. Im zweiten Schritt wird ein Ausgangsbetrag zur Berechnung der Geldbuße festgelegt, was nun nach einheitlichem Modell erfolgt. Im dritten Schritt werden erschwerende bzw. mildernde Faktoren geprüft, durch die sich der Betrag der Geldbuße erhöhen oder verringern kann. Hierfür sehen die Leitlinien eine einheitliche Auslegung vor. Im vierten Schritt wird der gesetzliche Höchstbetrag der Geldbuße gemäß Art. 83 Abs. 4 bis 6 Datenschutz-Grundverordnung (DSGVO) bestimmt und sichergestellt, dass der Betrag nicht überschritten wird. Im fünften Schritt wird schließlich geprüft, ob der berechnete Endbetrag den Anforderungen in Bezug auf Verhältnismäßigkeit und Wirksamkeit genügt oder weitere Anpassungen des Betrags erforderlich sind.

Nach Verabschiedung der Leitlinien unterlagen diese einer sechswöchigen öffentlichen Konsultation. In der endgültigen Fassung wurden die Rückmeldungen berücksichtigt und die Leitlinien um eine Referenztabelle mit Ausgangspunkten zur Berechnung der

225 Leitlinien 04/2022 des EDSA vom 12. Mai 2022: „On the Calculation of Administrative Fines under the GDPR", abrufbar unter https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en.

Geldbuße ergänzt, welche die Schwere eines Verstoßes mit dem Umsatz eines Unternehmens in Beziehung setzt.

Durch die Leitlinien erhöht sich die Transparenz des Vorgehens der Datenschutzaufsichtsbehörden bei der Verhängung von Geldbußen. Seit ihrer Verabschiedung liegen die Leitlinien den Bußgeldbemessungen unserer Behörde zugrunde.

15.2 Datenschutz-Zertifizierung

In diesem Jahr hat die Zertifizierung nach Art. 42 DSGVO deutlich an Dynamik gewonnen. Das erste deutsche Zertifizierungsprogramm für Auftragsverarbeitung namens EuroPriSe wurde von der Aufsichtsbehörde in Nordrhein-Westfalen genehmigt, nachdem es einen Prozess der innerdeutschen und europäischen Abstimmung durchlaufen hatte, an dem auch unsere Behörde aktiv beteiligt war. Bei drei weiteren Zertifizierungsprogrammen, die bei anderen deutschen Aufsichtsbehörden eingereicht wurden, haben wir uns ebenfalls in die innerdeutsche Abstimmung eingebracht. Darunter war ein Zertifizierungsprogramm für Auftragsverarbeitungen durch Clouddienstleister:innen. Ein weiteres, generisches Zertifizierungsprogramm für Verantwortliche und Auftragsverarbeiter:innen werden wir auch künftig in der Rolle als Co-Reviewer vor dem EDSA begleiten.

Ziel der Zertifizierungen ist es, die Transparenz zu erhöhen und die Einhaltung der DSGVO zu erleichtern, indem ein rascher Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglicht wird. Im Rahmen von Zertifizierungsverfahren prüft eine akkreditierte Zertifizierungsstelle einen bestimmten Datenverarbeitungsprozess auf die Einhaltung von vorher festgelegten Zertifizierungskriterien. Wenn die Prüfung positiv ausfällt, wird das Zertifikat für drei Jahre erteilt und kann im Anschluss erneuert werden. Innerhalb des Drei-Jahres-Zeitraums ist die Zertifizierungsstelle auch zu stichprobenartiger Kontrolle verpflichtet.

Anhand von Datenschutz-Zertifikaten können Bürger:innen einfacher datenschutzfreundliche Services für die private Nutzung identifizieren, Unternehmen wird z. B. die Auswahl von Auftragsverarbeiter:innen erleichtert. Die Pflicht der Verantwortli

chen zur sorgfältigen Auswahl zuverlässiger Auftragsverarbeiter:innen[226] kann in der Praxis erheblichen Prüfungsaufwand bedeuten und stellt vor allem kleinere und mittlere Unternehmen mitunter vor Herausforderungen. Zertifikate können die Auswahl geeigneter Dienstleistungen für die Auftragsverarbeitung vereinfachen. Zu beachten bleibt, dass nicht das Unternehmen als solches, sondern ein bestimmter Verarbeitungsprozess zertifiziert wird. Es muss also durch die Verantwortlichen auch immer geprüft werden, ob der konkret geplante Einsatz der jeweiligen Anbieter:innen dem zertifizierten Verarbeitungsprozess entspricht.

Die Zertifizierungskriterien, die die Vorgaben der DSGVO weiter konkretisieren, sind ein wesentlicher Teil der Zertifizierungsprogramme und müssen vor ihrem Einsatz in der Praxis von der zuständigen Aufsichtsbehörde geprüft und genehmigt werden. Zudem enthalten die Zertifizierungsprogramme Anwendungshinweise und Prüfmethoden, die ebenfalls im Rahmen der Programmprüfung von der Aufsichtsbehörde begutachtet werden. In diesem Jahr waren wir aktiv daran beteiligt, die bei der Prüfung der Zertifizierungsprogramme gewonnenen Erfahrungen im Rahmen des DSK-Arbeitskreises „Zertifizierung“ in die neue Version (2.0) der „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ einzubringen, die im Juni verabschiedet wurde.[227] Dabei haben wir gemeinsam mit den anderen deutschen Aufsichtsbehörden auch die innerdeutschen Abstimmungsprozesse verbessert. Ebenso wurde in diesem Jahr die Arbeit an den beiden bei unserer Behörde eingereichten Prüfprogrammen fortgesetzt. Insgesamt hat die innerdeutsche Zusammenarbeit in diesem Jahr einen enormen Zuwachs an praktischer Erfahrung mit datenschutzrechtlichen Zertifizierungsprogrammen gebracht, was künftige Programmprüfungen erleichtern wird. Nachdem EuroPriSe, das erste deutsche Zertifizierungsprogramm für Auftragsverarbeitung, nach einem Prozess der innerdeutschen und europäischen Abstimmung von der Aufsichtsbehörde in Nordrhein-Westfalen 2022 genehmigt wurde, gehen wir davon aus, dass bald eine Zertifizierungsstelle akkreditiert und die ersten Zertifikate erteilt werden können.

Das erste deutsche Datenschutz-Zertifizierungsprogramm (EuroPriSe) wurde nach innerdeutscher und europäischer Abstimmung von der Aufsichtsbehörde in

226 Art. 28 Abs. 1 DSGVO.

227 Abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/DSK_Zertifizierungskriterien_V2_0_Stand_21062022.pdf.

Nordrhein-Westfalen genehmigt. Wir gehen davon aus, dass bald eine Zertifizierungsstelle akkreditiert wird, sodass sich Auftragsverarbeiter:innen in Deutschland für alle Arten von Verarbeitungen nach diesem Programm zertifizieren lassen können, um gegenüber Verantwortlichen zu zeigen, dass die Verarbeitung DSGVO-konform erfolgt. Auf Basis der Erfahrung dieses und anderer Zertifizierungsprogramme hat die DSK die Anforderungen an datenschutzrechtliche Zertifizierungsprogramme weiter präzisiert.

15.3 Internationaler Datenverkehr: Geplanter Angemessenheitsbeschluss für die USA

Das Bewusstsein und die Aufmerksamkeit für die Übermittlung personenbezogener Daten in Drittländer haben im zweiten Jahr nach dem „Schrems II"-Urteil des Europäischen Gerichtshofs (EuGH) stark zugenommen. Wir erhalten immer mehr Beschwerden gegen Unternehmen aus diversen Branchen, in denen Beschwerdeführende die Übermittlungen ihrer Daten in Länder außerhalb des Europäischen Wirtschaftsraums (EWR) rügen.

Nachdem der EuGH am 16. Juli 2020 den Angemessenheitsbeschluss der Europäischen Kommission für die USA für ungültig erklärt hatte,[228] bestanden für Unternehmen und Betroffene große Unsicherheiten bei der Übermittlung personenbezogener Daten in die USA.[229] Am 7. Oktober dieses Jahres hat US-Präsident Joe Biden nun eine neue Executive Order erlassen, die die Kritikpunkte des EuGH am US-amerikanischen Überwachungsrecht entkräften soll. Die Europäische Kommission plant, auf dieser Grundlage einen neuen Angemessenheitsbeschluss[230] für die USA zu verabschieden.

Mit einem derartigen Beschluss attestiert die Europäische Kommission einem Drittland außerhalb des EWR ein angemessenes Datenschutzniveau, wodurch es Unternehmen aus dem EWR ermöglicht wird, personenbezogene Daten ohne die Ergreifung weiterer Maßnahmen[231] in dieses Drittland zu übermitteln. Ein neuer Angemessen

228 EuGH, Urteil vom 16. Juli 2020, C-311/18 („Schrems II").
229 Siehe JB 2020, 1.2.
230 Siehe Art. 45 DSGVO.
231 Siehe Kapitel V DSGVO.

heitsbeschluss für die USA muss daher in jedem Fall die Kritik des EuGH aus dem „Schrems II"-Urteil ausräumen. Konkret bedeutet dies, dass für staatliche Zugriffe auf Daten aus dem EWR klare und dem Grundsatz der Verhältnismäßigkeit entsprechende Regeln sowie effektive Rechtsschutzmöglichkeiten gegen behördliche Zugriffe für Betroffene aus dem EWR geschaffen werden müssen. Nach der Vorstellung eines konkreten Entwurfs für einen Angemessenheitsbeschluss durch die Europäische Kommission wird der EDSA den Entwurf sorgfältig analysieren und eine Stellungnahme abgeben. Wir begleiten diese Entwicklung intensiv und bringen uns auch über die Arbeit in den Arbeitsgruppen des EDSA bei der Bewertung eines solchen Beschlusses und seiner Konsequenzen ein. Erst mit der vollständigen Umsetzung der von US-Seite geplanten Änderungen sowie der Verabschiedung und dem Wirksamwerden eines Angemessenheitsbeschlusses für die USA ändert sich die konkrete Rechtslage bezüglich transatlantischer Übermittlungen. Bis dahin müssen Unternehmen die Vorgaben aus dem „Schrems II"-Urteil weiterhin vollumfänglich beachten.

Wir beobachten, dass die Aufmerksamkeit und das Bewusstsein für Themen des Internationalen Datenverkehrs bei Unternehmen und Beschwerdeführenden stark zugenommen haben. Dies wird auch an der wachsenden Anzahl von Beschwerden sichtbar, die mutmaßlich rechtswidrige Datenübermittlung in Drittländer zum Inhalt haben oder in denen die Übermittlungen neben anderen Verstößen als ergänzender Beschwerdepunkt gerügt werden. Die entsprechenden Beschwerden richten sich dabei gegen Unternehmen und Institutionen diverser Branchen wie bspw. Medizin, Finanzprodukte, Lieferdienste, Rechtsberatung, Therapie, Bildung und öffentliche Datenbanken. Dem Internationalen Datenverkehr kommt damit zunehmend die Rolle eines Querschnittsthemas zu, da es bei Hosting, Auftragsverarbeitung und kommerziellem Datenaustausch in vielen Fällen zu Übermittlungen in Drittländer kommt.

Diejenigen Unternehmen, die Datenexporte im eigenen Verantwortungsbereich erkennen, stützen ihre Datenübermittlungen in die USA inzwischen zum allergrößten Teil auf sog. Standardvertragsklauseln (SCC) als geeignete Garantien.[232] Durch die Hilfestellungen der deutschen und der übrigen europäischen Datenschutzaufsichtsbehörden[233]

232 Siehe Art. 46 Abs. 2 lit. c DSGVO.
233 Siehe JB 2021, 1.1.

konnten die zentralen Vorgaben des EuGH in diesem Bereich konkretisiert werden.[234] In vielen Fällen ergreifen die Unternehmen jedoch immer noch keine ausreichenden, vom EuGH geforderten ergänzenden Maßnahmen. Daher führen wir unsere Prüfungen der Datenexporte von etwa 80 Unternehmen im Rahmen von Website- und E-Mail-Hosting weiter.[235] Ein großer Teil der Verfahren konnte inzwischen abgeschlossen werden, da die Verantwortlichen die in Rede stehende Verarbeitung beendet oder eine rechtssicherere Lösung zum Hosting ihrer Website oder ihres E-Mail-Servers gewählt haben. Einige wenige Verantwortliche setzen jedoch weiterhin auf die Übermittlung in Drittstaaten, ohne die Vorgaben aus Kapitel V der DSGVO und die Vorgaben des EuGH ausreichend umzusetzen. Wir befinden uns hierzu in Gesprächen mit den Unternehmen, prüfen jedoch auch die Ergreifung aufsichtsbehördlicher Abhilfebefugnisse.

Sofern Unternehmen die Einhaltung datenschutzrechtlicher Vorgaben durch eine Zertifizierung [236] anstreben und hierbei auch Übermittlungen personenbezogener Daten in Drittländer anfallen, müssen beantragende Unternehmen nachweisen, dass sie die Anforderungen an Übermittlungen nach der DSGVO einhalten können. Entsprechende Vorgaben müssen deshalb in den entsprechenden Prüfprogrammen für Zertifizierungsstellen enthalten sein. Unsere Behörde begleitet ein solches Programm vor dem EDSA und prüft dabei auch dessen Konformität mit Kapitel V der DSGVO.[237]

Wie sich am zunehmenden Beschwerdeaufkommen aus sämtlichen Wirtschaftsbereichen zeigt, besteht weiterhin großer Beratungsbedarf im Bereich des Internationalen Datenverkehrs. Wir bringen uns im Rahmen der deutschen und europäischen Zusammenarbeit intensiv bei der Klärung verbliebener Fragen und der Durchsetzung der Vorgaben des EuGH ein. Ein etwaiger zukünftiger Angemessenheitsbeschluss für die USA muss die Vorgaben aus dem „Schrems II"-Urteil des

234 Siehe Empfehlungen 01/2020 des EDSA: „Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten", abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de; siehe ebenso das DSK-Gutachten zum US-Überwachungsrecht von Stephen I. Vladeck, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2022/2022-Vladek_Rechtsgutachten_DSK_de.pdf.

235 Siehe JB 2021, 1.1.

236 I. S. v. Art. 42 DSGVO.

237 Siehe 15.2.

EuGH vollumfänglich umsetzen, um den Schutz personenbezogener Daten bei entsprechendem Auslandsbezug sowie die Rechtssicherheit für Unternehmen und Bürger:innen zu gewährleisten. Bis zum endgültigen Wirksamwerden eines Angemessenheitsbeschlusses für die USA müssen Verantwortliche auf andere Instrumente aus Kapitel V der DSGVO zurückgreifen und diese gemäß den Vorgaben aus dem „Schrems II"-Urteil umsetzen.

15.4 Europäische Kooperation

Die DSGVO sieht eine enge Zusammenarbeit zwischen den europäischen Aufsichtsbehörden vor. Dabei geht es insbesondere um Fälle, die eine grenzüberschreitende Verarbeitung personenbezogener Daten beinhalten.

Ein Fall ist dann grenzüberschreitend, wenn die Datenverarbeitung entweder in mehreren Niederlassungen in verschiedenen Mitgliedstaaten der Europäischen Union (EU) erfolgt oder wenn die Verarbeitung in nur einer Niederlassung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.[238] Dabei bearbeitet unsere Behörde diejenigen Fälle federführend, in denen das verantwortliche Unternehmen seinen Hauptsitz in Berlin hat. Befindet sich der Hauptsitz des Unternehmens in einem anderen Mitgliedstaat der EU bzw. des EWR, übermitteln wir die bei uns eingegangenen Fälle an die Aufsichtsbehörde des jeweiligen Mitgliedstaats. Wir sind in diesem Fall lediglich betroffene Aufsichtsbehörde. Die federführende Aufsichtsbehörde ermittelt den Fall und steht dabei in ständigem Austausch mit den betroffenen Aufsichtsbehörden.[239] Sobald die federführende Aufsichtsbehörde einen Fall ausermittelt hat, stellt sie allen betroffenen Aufsichtsbehörden einen Beschlussentwurf zur Abstimmung bereit. Dementsprechend hat unsere Behörde auch in diesem Jahr die Beschlussentwürfe anderer federführender Aufsichtsbehörden gesichtet und bei abweichenden Positionen Einspruch eingelegt. Auf diesem Wege haben wir zu einer Vielzahl von Fragen Stellung genommen, die zwischen den europäischen Aufsichtsbehörden abstimmungsbedürftig sind.

238 Art. 4 Nr. 23 DSGVO.
239 Art. 60 DSGVO.

In denjenigen Fällen, in denen die federführende Behörde dem Einspruch einer betroffenen Behörde nicht folgen möchte, kontaktiert sie den EDSA zur Streitbeilegung.[240] Die deutschen Behörden stimmen solche Einsprüche inhaltlich zunächst untereinander ab. So haben wir uns in diesem Jahr an vier innerdeutsch abgestimmten Einsprüchen gegen Beschlussentwürfe der irischen Datenschutzaufsichtsbehörde (DPC) in Bezug auf große Internetkonzerne beteiligt, die dann in das Streitbeilegungsverfahren gingen.

Beispielhaft kann ein Einspruch gegen einen Beschlussentwurf der DPC zur Datenverarbeitung zwecks verhaltensbasierter Werbung durch einen großen sozialen Mediendienst gesehen werden, gegen den neben weiteren europäischen Aufsichtsbehörden auch Deutschland unter Federführung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit Einspruch einlegte. Der Einspruch, an dessen Erstellung wir maßgeblich beteiligt waren, beanstandete, dass der Mediendienst personenbezogene Daten widerrechtlich verarbeitete,[241] da er über keine Rechtsgrundlage für die umfangreiche Verarbeitung der Daten,[242] darunter auch besonders schützenswerte Daten,[243] verfügt. Ein genereller Verweis auf die Erfüllung des Nutzungsvertrags[244] sei hierbei nicht ausreichend. Zwar werde eine Einwilligung der betroffenen Personen eingeholt, eine Ablehnung führe aber zur gänzlichen Verweigerung des Angebots und sei zudem nicht von der Einwilligung zu anderen Sachverhalten zu trennen.[245] Ebenso wurde beanstandet, dass der Beschluss die Rechtsfolge für das Unternehmen nicht hinreichend eindeutig festlegt. Der Einspruch forderte die DPC auf, den Verantwortlichen anzuweisen, die widerrechtlich verarbeiteten Daten zu löschen, zukünftige Datenverarbeitung ohne Rechtsgrundlage zu verbieten und ein angemessenes und abschreckendes Bußgeld zu verhängen.[246] Hinsichtlich dieser Einsprüche fasste der EDSA am 5. Dezember dieses Jahres den verbindlichen Beschluss 3/2022:[247] Obgleich der EDSA nicht allen Argumenten der Einsprüche folgt, stimmt er im vorliegenden Fall zu, dass sich der Verantwortliche im Fall verhaltensbezogener Werbung

240 Art. 65 DSGVO.
241 Siehe Art. 5 Abs. 1 lit. a DSGVO.
242 Siehe Art. 6 DSGVO.
243 Siehe Art. 9 DSGVO.
244 Art. 6 Abs. 1 Satz 1 lit. b DSGVO.
245 Siehe Art. 7 Abs. 2 DSGVO.
246 Gemäß Art. 58 Abs. 2 lit. c, f und i DSGVO.
247 Abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_bg.

nicht auf die Erfüllung seiner vertraglichen Rechte aus dem Nutzungsvertrag gegenüber den Betroffenen stützen kann.

Darüber hinaus haben wir im Rahmen des DSK-Arbeitskreises „Organisation und Struktur“ an der Verbesserung der innerdeutsche Koordination solcher Einsprüche mitgewirkt: Im letzten Jahr hatten wir berichtet, dass einer unserer Einsprüche ins Streitbeilegungsverfahren gegangen war.[248] Gemeinsam mit unseren Kolleg:innen aus Niedersachsen und Hamburg, die ebenfalls Erfahrungen mit Streitbeilegungsverfahren haben, boten wir für die deutschen Aufsichtsbehörden einen Workshop zum Thema an, der sehr positiv aufgenommen wurde. Außerdem haben wir auch eigene Beschlussentwürfe im Kooperationsverfahren abgestimmt. In 15 Fällen konnten wir im Konsens mit den betroffenen Aufsichtsbehörden in Europa endgültige Beschlüsse erlassen und somit Klarheit für betroffene Personen und Verantwortliche schaffen.[249]

Insgesamt führt die zunehmende Erfahrung aller Aufsichtsbehörden mit dem europäischen Kooperationsverfahren zu einem immer reibungsloseren Ablauf, der einen produktiven inhaltlichen Austausch mit dem Ziel der Konsensfindung ermöglicht.

248 Siehe JB 2021, 16.2.
249 Siehe 18.6.

16 Informationsfreiheit

16.1 Entwicklungen in Deutschland

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) hat in diesem Jahr unter dem Vorsitz der Landesbeauftragten für Datenschutz Schleswig-Holstein drei Entschließungen gefasst.

Mit einer Entschließung forderte die IFK die Beteiligten an den Koalitionsverhandlungen nach den Landtagswahlen in Niedersachsen auf, den Erlass eines Transparenzgesetzes in den Koalitionsvertrag aufzunehmen.[250] Ein entsprechender Passus findet sich nun im Koalitionsvertrag von SPD und Bündnis 90/Die Grünen.[251] In einer weiteren Entschließung empfiehlt die IFK den Verwaltungen in Bund und Ländern, jegliche relevante behördliche Kommunikation in verkörperter Form – unabhängig davon, ob in Papierform, als E-Mail, per SMS oder unter Nutzung sozialer Medien kommuniziert wird – zu dokumentieren, um den Zugang nach dem Informationsfreiheitsrecht zu garantieren.[252] Die IFK verweist dabei auf ein Urteil des Bundesverwaltungsgerichts (BVerwG) über die Offenlegung von Twitter-Direktnachrichten des Bundesministerium des Innern und für Heimat.[253] In einer dritten Entschließung stellt die IFK angesichts des Umgangs der Landesregierung Mecklenburg-Vorpommern mit dem Zugang zu Informationen über die Stiftung Klima- und Umweltschutz MV fest, dass bei Stiftungen, die öffentliche Aufgaben wahrnehmen, die Öffentlichkeit einen Anspruch auf Informationen hat. Das Recht auf Informationszugang besteht dann unabhängig davon, ob es sich um eine Stiftung des öffentlichen Rechts oder – wie bei der Stiftung Klima- und

250 Entschließung der IFK vom 26. Oktober 2022: „Niedersachsen: Die Zeit für ein Transparenzgesetz ist gekommen!“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk.

251 Siehe Zeilen 28–33 im Koalitionsvertrag „Sicher in Zeiten des Wandels – Niedersachsen zukunftsfest und solidarisch gestalten“ für den Zeitraum 2022–2027, S. 102.

252 Entschließung der IFK vom 30. Juni 2022: „SMS in die Akte: Behördliche Kommunikation unterliegt umfassend den Regeln der Informationsfreiheit!“, abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk.

253 BVerwG, Urteil vom 28. Oktober 2021, 10 C 3.20.

Umweltschutz MV – um eine solche des bürgerlichen Rechts handelt.[254] Die gewählte Organisationsform darf die staatliche Transparenzpflicht nicht unterlaufen.

16.2 Doch kein Transparenzgesetz für Berlin

In den beiden letzten Jahren haben wir ausführlich über die Bestrebungen berichtet, das veraltete Berliner Informationsfreiheitsgesetz (IFG) von 1999 durch ein modernes Transparenzgesetz abzulösen.[255]

In diesem Jahr war nun festzustellen, dass die entsprechende Aussage im rot-grün-roten Koalitionsvertrag, 2022 ein Transparenzgesetz nach Hamburger Vorbild einzuführen und dabei die hohen Standards des IFG zu erhalten, keine Priorität hatte.

16.3 Transparente Lebensmittelüberwachung

In den beiden letzten Jahren haben wir über die Verbesserung der Information für Verbraucher:innen durch die Einführung des Lebensmittelüberwachungstransparenzgesetzes (LMÜTranspG) berichtet,[256] die wir sehr begrüßen. Das Gesetz ist inzwischen unter dem Begriff „Saubere-Küchen-Gesetz" bekannt und tritt am 1. Januar 2023 in Kraft. Einzelheiten zum behördlichen Vorgehen sind in einer Durchführungsverordnung geregelt,[257] die uns zur Stellungnahme im Entwurf vorgelegt worden war.[258] Sie enthält die Details zum Bewertungssystem und zur Darstellung des offenzulegenden sog. Lebensmittelüberwachungstransparenzbarometers.

254 Entschließung der IFK vom 30. Juni 2022: „Keine Umgehung der Informationsfreiheit durch Errichtung von Stiftungen bürgerlichen Rechts!", abrufbar unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-ifk.

255 Siehe JB 2020, 19.2.2; JB 2021, 17.2.1.

256 Siehe JB 2020, 19.2.3; JB 2021, 17.2.1.

257 Sog. Lebensmittelüberwachungstransparenzgesetzdurchführungsverordnung (LMÜTranspG-DVO), GVBl. 2023, S. 7 ff.

258 Die Berliner Beauftragte für Datenschutz und Informationsfreiheit ist vor dem Erlass von Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften anzuhören, wenn sie die Informationsfreiheit oder die Verarbeitung personenbezogener Daten betreffen; siehe § 18 Abs. 2 Satz 3 IFG und § 11 Abs. 2 Satz 2 Berliner Datenschutzgesetz (BlnDSG).

Für die Bewertung ist zu 50 % das Hygienemanagement im Betrieb maßgeblich, während die Einhaltung lebensmittelrechtlicher Bestimmungen mit 6,25 % eine eher untergeordnete Rolle im Kontrollergebnis spielt. Es ist nach Sinn und Zweck der neuen Vorschriften erforderlich und angemessen, dass zugunsten der Gesundheit der Verbraucher:innen unter Umständen nicht bestandskräftige Verwaltungsmaßnahmen gegen den Lebensmittelbetrieb als Kriterium für die Bewertung der „Einhaltung lebensmittelrechtlicher Bestimmungen" zusätzlich berücksichtigt werden; die Verwaltungsmaßnahmen selbst sind nicht im offenzulegenden Transparenzbarometer aufgeführt. Wir haben uns allerdings dafür ausgesprochen, dass der maßgebliche Zeitraum, in dem Verfehlungen der Lebensmittelunternehmen überhaupt nur relevant sein dürfen, nicht unendlich lange zurückreicht, sondern auf die letzten sechs Jahre beschränkt ist. Diesen Zeitraum halten wir für sachgerecht, weil er einerseits den europäischen Vorgaben Rechnung trägt, nach denen Ergebnisse aus früheren amtlichen Kontrollen einzubeziehen sind,[259] und andererseits das bundesrechtlich geregelte Kontrollintervall von drei Jahren für Betriebe mit einem geringen Risiko berücksichtigt.[260] Dadurch ist gewährleistet, dass auch bei diesen Betrieben mehr als nur eine amtliche Kontrolle in die aktuelle Überwachungsmaßnahme einfließen kann.

16.4 Transparentes Schulsystem?

Im Jahr 2020 haben wir im Zuge der Diskussion um die zahlreichen Bereichsausnahmen in einem neuen Transparenzgesetz kritisiert, dass der gesamte Schulbereich von vornherein aus dem Anwendungsbereich ausgenommen war.[261] Begründet wurde dies im damaligen Senatsentwurf damit, dass eine Rangliste für Schulen zu vermeiden sei. Das beabsichtigte Gesetz wurde bekanntlich nicht verabschiedet.[262]

Der Wissenschaftliche Parlamentsdienst (WPD) hat auf Anfrage einer Fraktion die aufgeworfenen Fragen gemäß IFG und Verfassungsrecht umfassend geprüft und in

259 Verordnung (EU) 2017/625 des Europäischen Parlaments und des Rates.
260 Allgemeine Verwaltungsvorschrift über Grundsätze zur Durchführung der amtlichen Überwachung der Einhaltung der Vorschriften des Lebensmittelrechts [...] (AVV Rahmen-Überwachung).
261 Siehe JB 2020, 19.2.2.
262 Siehe JB 2020, 16.2.1.

einem Gutachten festgestellt, dass ein Geheimhaltungsbedarf in Bezug auf erhobene statistische Einzelschuldaten grundsätzlich nicht besteht.[263]

16.5 Bearbeitung von IFG-Anträgen – Auch ohne Postanschrift!

Wir erhielten mehrere Eingaben von Bürger:innen, weil die jeweils angefragte Stelle – allen voran die Polizei – vor Erstbefassung mit dem jeweiligen IFG-Antrag die Postanschrift der antragstellenden Person verlangt hatte. Die Forderung wurde unabhängig vom Verfahrensstadium ausgesprochen, also auch dann, wenn zunächst nur eine Kostenvorabinformation gewünscht war. Die Polizei begründete dies wie folgt: „Die Angaben sind erforderlich, um eine gebührenbelastende Herausgabe von Informationen an eine anonyme Antragstellung zu vermeiden sowie um eine identifizierbare Zugänglichmachung des Bescheides zu ermöglichen." Sie wies die Antragsteller:innen darauf hin, dass ohne Anschrift keine weitere Bearbeitung erfolge.

Wir haben der Polizei mitgeteilt, dass eine „anonyme Antragstellung" angesichts des mitgeteilten Namens nicht vorliegt und dass die Erhebung der Postanschrift gegen das IFG verstößt.[264] Danach ist die Verarbeitung personenbezogener Daten zulässig, soweit dies zur Erfüllung der in diesem Gesetz genannten Aufgaben erforderlich ist. Darüber hinaus haben wir darauf hingewiesen, dass eine Akteneinsicht nach dem IFG mündlich, schriftlich oder elektronisch erteilt werden kann.[265] Die Verweigerung oder Beschränkung der Akteneinsicht oder Aktenauskunft ist regelmäßig schriftlich oder elektronisch zu begründen.[266] Die Erweiterung dieser Bestimmungen durch die Formulierung „oder elektronisch" erfolgte durch Artikel 21 des Gesetzes zur Anpassung der Formanforderungen im Berliner Landesrecht (FormAnpassG).

263 Gutachten des WPD vom 8. April 2022: „Fragen der Existenz und Reichweite eines Informationsanspruches im Hinblick auf bestimmte statistische Daten zu einzelnen Schulen im Land Berlin", abrufbar unter https://www.parlament-berlin.de/media/download/2819.
264 Siehe § 4a IFG.
265 § 13 Abs. 3 IFG.
266 § 15 Abs. 1 IFG.

Die Vorlage hierfür hatte die Senatsverwaltung für Inneres und Sport erarbeitet.[267] Danach reicht die einfache elektronische Kommunikation in IFG-Fällen vollkommen aus.[268] Wir haben der Polizei mitgeteilt, dass deren Auffassung dem eindeutigen Willen des Gesetzgebers entgegensteht: Von IFG-Antragsteller:innen die Postanschrift als Voraussetzung für die Erstbearbeitung des IFG-Antrags zu verlangen, ist nicht erforderlich.[269]

Da die Polizei ihr Verfahren nicht geändert und sich auch nicht mit unserer Auffassung auseinandergesetzt hat, haben wir bei der Senatsverwaltung für Inneres, Digitalisierung und Sport wegen ihrer Grundsatzzuständigkeit für das Informationsfreiheitsrecht eine Beschwerde und Bitte um Unterstützung wegen fehlerhafter Anwendung des IFG durch die Polizei eingereicht. Die Innenverwaltung teilte unsere Auffassung nicht und stellte dabei primär auf § 13 Abs. 1 IFG ab, der eine anonyme Antragstellung nicht vorsieht. Nicht eingegangen ist die Innenverwaltung auf unsere Argumentation, dass die Gesetzesänderung zur Zulässigkeit der einfachen elektronischen Kommunikation von ihr selbst initiiert und diese seinerzeit für zulässig befunden wurde. Wir sehen uns in unserer Auffassung durch das zwischenzeitlich ergangene Urteil des Oberverwaltungsgerichts (OVG) Nordrhein-Westfalen bestärkt,[270] das das anderslautende

267 Siehe Abghs.-Drs. 18/0420 vom 21. Juni 2017; auf S. 16 dieser Vorlage heißt es: „Mit dieser oder einer bedeutungsgleichen Formanforderung werden neben der hergebrachten Schriftform auch alle elektronischen Formen, einschließlich der ‚einfachen' elektronischen Formen zugelassen. Durch den Begriff ‚schriftlich oder' wird auch bzgl. der elektronischen Formen festgelegt, dass der Inhalt/Text dem der Papierform entsprechen muss. Kurz: Immer wenn jedenfalls eine E-Mail ausreichend ist, sollte diese Formanforderung gewählt werden."

268 Siehe auch die weiteren Ausführungen in Bezug auf § 15 Abs. 1 IFG in ebd., S. 18: „Nach dem Sinn und Zweck der Regelung in § 15 soll die antragstellende Person die Möglichkeit erhalten, die Gründe für die Ablehnung zu überprüfen. Das Schriftformerfordernis dient der textlichen Fixierung (Ausschluss der Mündlichkeit). Auf die besondere, über die qualifizierte elektronische Signatur vermittelte Beweis- und Authentifizierungsfunktion kommt es nicht an. Bei der Entscheidung handelt es sich zudem um einen Verwaltungsakt. Nach § 37 Absatz 2 Verwaltungsverfahrensgesetz kann ein Verwaltungsakt schriftlich, elektronisch, mündlich oder in anderer Weise erlassen werden. Die einfache elektronische Form ohne qualifizierte Signatur ist daher ausreichend."

269 Insofern erhalten wir die im JB 2021 unter Ziffer 17.2.3.1 vertretene Auffassung, dass für die „ordnungsgemäße Zustellung eines (Gebühren-)Bescheides eine zustellungsfähige Postanschrift" immer angegeben werden müsse, nicht aufrecht.

270 Siehe OVG Nordrhein-Westfalen, Urteil vom 15. Juni 2022, 16 A 857/21 (nicht rechtskräftig).

Urteil der Vorinstanz[271] in Bezug auf die in Rede stehende Problematik kassiert hat. So heißt es im vierten Leitsatz des Urteils des OVG: „Weder aus den Vorschriften des Informationsfreiheitsgesetzes noch aus allgemeinen Verfahrensvorschriften ergibt sich die generelle Pflicht eines IFG-Antragstellers, bei Antragstellung seine Postanschrift anzugeben." Das angerufene Bundesverwaltungsgericht wird eine Klärung herbeiführen.

Wir appellieren an die öffentlichen Stellen im Land Berlin, die Postanschrift der Antragsteller:innen möglichst nicht einzufordern, wenn sie für die Bearbeitung des IFG-Antrags, z. B. für die gewünschte Kostenvorabinformation, tatsächlich nicht benötigt wird.

16.6 Schatten und Licht in der Senatsverwaltung für Bildung

Ein Bürger beantragte bei der Senatsverwaltung für Bildung, Jugend und Familie die Offenlegung der letzten Ausschreibungs- und Vergabeunterlagen zu den „IT-Experten Schulen". Er stellte den Antrag nicht unter seinem Klarnamen, sondern verwendete ein Pseudonym.

Auf seinen Antrag hin erhielt der Bürger von der Bildungsverwaltung die Auskunft, dass es im Jahr 2018 eine Vergabeunterlage mit mehreren Losen für alle Bewerber:innen gegeben habe. Allerdings sei eine Übersendung der Unterlagen nach dem IFG nicht vorgesehen, sodass alternativ nur eine telefonische Aktenauskunft oder die Einsichtnahme vor Ort möglich sei; über die Gebühr hierfür würde je nach gewählter Variante entschieden. Als sich in der weiteren Kommunikation herausstellte, dass der Bürger bei seinem Antrag ein Pseudonym angegeben hatte, verlangte die Senatsverwaltung die Identifikation und die Angabe einer Postadresse, um den stattgebenden IFG-Bescheid zuzuschicken.

Unsere Prüfung hat ergeben, dass die begehrte Information seinerzeit im Internet allgemein verfügbar war. Vor diesem Hintergrund konnten wir die Senatsverwaltung

271 Siehe Verwaltungsgericht (VG) Köln, Urteil vom 18. März 2021, 13 K 1190/20.

schließlich davon überzeugen, dem Antragsteller die gewünschte, elektronisch vorhandene Information gebührenfrei zu übersenden, ohne hierfür den Klarnamen und die Postanschrift zu verlangen. Die dem Antrag stattgebende Nachricht war für den Bürger nicht nachteilig und konnte daher formlos verschickt werden.

Wir begrüßen die ergebnisorientierte und bürgerfreundliche Kehrtwende der Senatsverwaltung für Bildung, Jugend und Familie.

16.7 IFG-Verweigerung bei der Stiftungsaufsicht

Ein Bürger beschwerte sich bei unserer Behörde darüber, dass die bei der Senatsverwaltung für Justiz, Vielfalt und Antidiskriminierung angesiedelte Stiftungsaufsicht die Satzung einer Stiftung des bürgerlichen Rechts nicht offenlegen wollte. Die Stiftungsaufsicht begründete die Verweigerung des Informationszugangs u. a. damit, dass das Informationsfreiheitsrecht nicht uneingeschränkt gelte, sondern es (neben den Einschränkungen im IFG selbst) „auf der Grundlage allgemeiner Rechtsgrundsätze Grenzen" erfahre. Die offenbar beabsichtigte Veröffentlichung der Satzung über die Onlineplattform FragDenStaat würde die Stiftung einer Publizität unterwerfen, der sie grundsätzlich nicht unterliege. Hiergegen hat der Bürger Widerspruch erhoben und uns um Unterstützung seines Begehrens gebeten.

Wir haben der Stiftungsaufsicht mitgeteilt, dass der von ihr ausgestellte Bescheid insbesondere deshalb rechtswidrig ist, weil er keine Aussage dazu enthält, aufgrund welches konkreten Ausnahmetatbestands des IFG der Informationszugang verwehrt wird. Vielmehr ließen die allgemeinen Ausführungen erkennen, dass die Stiftungsaufsicht davon ausging, dass der Informationszugang zu sämtlichen, ihr unterstehenden Unterlagen von vornherein ausgeschlossen sei. Solange es allerdings eine solche gesetzliche Bereichsausnahme für die Stiftungsaufsicht nicht gibt, muss sich die Behörde in jedem Einzelfall und in Bezug auf jedes angefragte Dokument mit den IFG-Ausnahmetatbeständen[272] auseinandersetzen und ggf. das gesetzlich vorgesehene Anhörungsverfahren mit der betroffenen Stiftung durchführen.[273]

272 §§ 5 ff. IFG.
273 § 14 Abs. 2 IFG.

Die Stiftungsaufsicht hat sich unserer Auffassung nicht angeschlossen und den Widerspruch schließlich zurückgewiesen, diesmal u. a. mit der Begründung, dass dem IFG-Antrag wie jedem anderen Rechtsanspruch „übergreifende Rechtsmaßstäbe als Einwand entgegengehalten werden können, wenn diese der Ausübung des geltend gemachten Rechts entgegenstehen". Dies sei z. B. bei „Wertungswidersprüchen innerhalb der Rechtsordnung" der Fall. Da auch diese allgemein gehaltenen Aussagen unserer Ansicht nach nicht stichhaltig waren und weiterhin keine Ausführungen zu einschränkenden oder den Anspruch ausschließenden IFG-Tatbeständen gemacht wurden, konnten wir dem Bürger nur die gerichtliche Klärung empfehlen.

Auch für die Stiftungsaufsicht gilt das IFG. Sie muss wie alle anderen öffentlichen Stellen des Landes Berlin Informationszugangsanträge zu Stiftungsunterlagen anhand der Ausnahmetatbestände des IFG prüfen und kann sich nicht allein auf übergreifende Rechtsmaßstäbe berufen.

16.8 Verfassungsbeschwerde der Humboldt-Universität zu Berlin

Im Zusammenhang mit der von der Humboldt-Universität zu Berlin (HU) eingereichten Verfassungsbeschwerde zur Überprüfung, ob mit der Novellierung des Berliner Hochschulgesetzes (BerlHG)[274] die gesetzgeberische Kompetenz überschritten worden sei, stellte ein Bürger den Antrag auf Offenlegung verschiedener Unterlagen. Hierzu gehörten der Beschwerdeschriftsatz sowie Informationen zu den vertraglich vereinbarten Kosten für die juristische Beratung. Die HU lehnte den Antrag unter Berufung auf schützenswerte Betriebs- und Geschäftsgeheimnisse ab und berief sich darüber hinaus auf die anwaltliche Verschwiegenheitspflicht. Der Offenlegung des Beschwerdeschriftsatzes stünde auch das laufende Gerichtsverfahren entgegen. Im Übrigen sei er urheberrechtlich geschützt.

Wir haben der HU mitgeteilt, dass im Widerspruchsverfahren zu klären ist, warum in Bezug auf den Vertrag mit der juristischen Vertretung auch eine teilweise Offenlegung

274 Der neu gefasste § 110 Abs. 6 BerlHG regelt bei befristeten Beschäftigungsverhältnissen die sog. Anschlusszusage für wissenschaftliche sowie promovierte Mitarbeiter:innen.

nicht in Betracht kommt.[275] Denn nicht jede Information im Vertrag ist von vornherein ein schützenswertes Betriebs- oder Geschäftsgeheimnis.[276] Auch steht das Berufsgeheimnis der von der HU beauftragten Rechtsanwälte dem Informationszugang nicht entgegen. Die HU kann sich als „Herrin des Geheimnisses" nicht auf das Berufsgeheimnis des von ihr mandatierten Geheimnisträgers stützen.[277] Schließlich wurde nicht hinreichend deutlich, warum durch die Offenlegung des Beschwerdeschriftsatzes nachteilige Auswirkungen für das Land Berlin bei der Durchführung eines laufenden Gerichtsverfahrens zu befürchten sind.[278] Die Feststellung der konkreten Möglichkeit nachteiliger Auswirkungen setzt seitens der informationspflichtigen Stelle die – hier fehlende – Darlegung von Tatsachen voraus, aus denen sich eine Beeinträchtigung des Schutzguts ergeben kann.[279]

Der Beschwerdeschriftsatz ist auch kein nach dem Urheberrecht zu schützendes Werk, denn hiernach genießen nur persönliche, geistige Schöpfungen Urheberrechtsschutz.[280] An der erforderlichen Originalität fehlt es, wenn die Schaffung eines Gegenstands durch technische Erwägungen, durch Regeln oder durch andere Zwänge bestimmt wurde. Arbeitsaufwand oder bedeutende Sachkenntnis, die in die Gestaltung eingeflossen sind, genügen demnach nicht.[281] Vorliegend war daher nicht plausibel, dass der Beschwerdeschriftsatz der Verfasser:innen der von der HU mandatierten Anwaltskanzlei nicht nach den Vorgaben der HU – nämlich in Bezug auf das zu erzielende und stichhaltig zu begründende Verfahrensergebnis – erstellt wurde. Die Schaffung des Beschwerdeschriftsatzes wurde also durch Vorgaben der HU bestimmt, sodass es sich bei dem Schriftsatz nicht um eine persönliche, geistige Schöpfung, mithin nicht um ein urheberrechtlich geschütztes Werk handelte. Vor diesem Hintergrund haben wir der HU die Herausgabe des Beschwerdeschriftsatzes empfohlen und überdies – auch angesichts des öffentlichen Interesses – sogar die proaktive Veröffentlichung auf deren Internetpräsenz angeraten.

275 Siehe § 12 IFG.
276 Siehe § 7 IFG.
277 Siehe BVerwG, Urteil vom 15. Dezember 2020, 10 C 25/19.
278 Siehe § 9 Abs. 1 Satz 2 IFG.
279 Siehe VG Berlin, Urteil vom 8. Dezember 2021, VG 2 K 48/20, unter Berufung auf BVerwG, Urteil vom 27. November 2014, 7 C 12/13.
280 § 2 Abs. 2 Urheberrechtsgesetz (UrhG).
281 VG Berlin, Urteil vom 1. November 2021, VG 2 K 142/20.

Die HU hat sich unserer Auffassung nicht angeschlossen. Der Bürger hat gegen den entsprechenden Widerspruchsbescheid der HU Klage beim Verwaltungsgericht (VG) Berlin erhoben.

Wir begrüßen die vom Bürger initiierte Klärung der zahlreichen Rechtsfragen durch das VG Berlin.

16.9 Publikation der Polizei als dauerhafte Verschlusssache?

Ein Bürger beschwerte sich bei uns darüber, dass in der Datenbank einer Universitätsbibliothek eine Publikation der Polizei von 2005 über die Aufenthaltsverbotsverfügung zwar gelistet war, allerdings als Verschlusssache von der Polizei nicht offengelegt wurde. Die Polizei begründete dies damit, dass durch die Offenlegung Rückschlüsse auf das taktische Vorgehen der Polizei gezogen werden könnten, was einen schwerwiegenden Nachteil für das Land Berlin darstellen würde. Weiter hieß es: „Staatliches Handeln, insbesondere polizeiliches, darf nicht kalkulierbar oder voraussehbar sein, da sonst die gesetzlich übertragenen Aufgaben der Polizei zur Gefahrenabwehr und vorbeugenden Strafverfolgung nicht mehr erfüllt werden können. Es besteht deshalb die Gefahr, dass, wenn Dritte in solchen Fällen Kenntnis über derartige Informationen erlangten, diese sich zukünftig auf polizeiliches Handeln derart einstellen könnten, was eine effektive polizeiliche Aufgabenerfüllung wesentlich erschweren würde. Die Weitergabe dieser Schrift zur Fortbildung an Personen oder Stellen außerhalb der Berliner Polizei ist untersagt."

Wir haben der Polizei mitgeteilt, dass der entsprechende Bescheid an den Bürger rechtswidrig ist. Denn er enthält einen uns aus zahlreichen anderen Fällen bekannten Standardtext und setzt sich nicht mit der Tatsache auseinander, dass das begehrte Dokument inzwischen mehr als 16 Jahre alt ist. Insofern bezweifeln wir, dass die dortigen Erkenntnisse noch immer geeignet sind, Rückschlüsse auf das taktische Vorgehen der Polizei zu ziehen, und deshalb die Offenlegung weiterhin einen schwerwiegenden Nachteil für das Land Berlin darstellen würde.[282] Darüber hinaus enthielt der

282 Siehe § 11 IFG.

Bescheid keine Aussage dazu, ob die Gründe für die bisherige Geheimhaltungsstufe „VS-Vertraulich“ zwischenzeitlich entfallen sind. Die Polizei hat sich hierzu trotz zweifacher Erinnerung nicht geäußert.

Wir müssen feststellen, dass sich die Polizei hier, aber auch in weiteren Fällen nicht oder nicht ausreichend mit unserer Rechtsauffassung auseinandersetzt. Bei einer Novellierung des Informationsfreiheitsrechts werden wir dafür eintreten, dass unsere Empfehlungen an informationspflichtige Stellen bei deren Entscheidung über den Informationszugang berücksichtigt werden müssen.

16.10 Polizeidienstvorschrift über die Polizeidiensttauglichkeit

Wir erhielten die Beschwerde eines Bürgers, der die Offenlegung der polizeilichen Verwaltungsvorschrift PDV 300 verlangte. Diese regelt u. a. die gesundheitliche Eignungsfeststellung für den Polizeidienst. Die Polizei verweigerte die Offenlegung und begründete dies damit, dass dadurch mögliche nachteilige Auswirkungen auf die Belange der öffentlichen Sicherheit zu besorgen seien.

Die Polizei führte aus, dass bei Kenntnis der Vorschrift und bereits vorhandenen Krankheitssymptomen versucht werden könnte, die Symptome bei einer Untersuchung entsprechend zu verschleiern, um entgegen der notwendigen Voraussetzung in den Polizeivollzugsdienst eintreten und diesen ausüben zu können. Zudem zählten die Unterlagen zum Schutz des behördlichen Entscheidungsprozesses nach § 10 Abs. 4 IFG: „Durch deren Veröffentlichung könnte der inner- und zwischenbehördliche Willensprozess beeinträchtigt sein.“

Die Verweigerung des Informationszugangs kann nicht auf § 10 Abs. 4 IFG gestützt werden: Denn hiernach ist nur die Besprechung, Beratschlagung und Abwägung, mithin der eigentliche Vorgang des Überlegens, geschützt. Dagegen gehört die Verwaltungsvorschrift als Grundlage der Willensbildung gerade nicht zum Schutzbereich des § 10 Abs. 4 IFG. Auch § 11 IFG wurde falsch angewandt. Denn es wurden entgegen dem Gesetzeswortlaut lediglich „mögliche nachteilige Auswirkungen“ auf die Belange der öffentlichen Sicherheit durch die Offenlegung der Polizeidienstvorschrift angenommen.

Diese möglichen „einfachen“ Nachteile, die schon nicht als stichhaltige Argumente gegen eine Offenlegung anzusehen sind, reichen jedoch nicht aus: Erforderlich sind nach dem Gesetzeswortlaut vielmehr „schwerwiegende“ Nachteile für das Wohl des Bundes oder eines Landes. Diese waren erst recht nicht erkennbar.

Auch in diesem Fall hat sich die Polizei nicht mit unseren Argumenten auseinandergesetzt und den Widerspruch des Bürgers gegen ihre Entscheidung mit nach wie vor nicht stichhaltiger Begründung zurückgewiesen. Es stellt sich die Frage nach der Sinnhaftigkeit unserer gesetzlich normierten Beratungsbefugnis,[283] wenn unsere Argumente bei der Entscheidung über IFG-Anträge regelmäßig keine Rolle spielen.

16.11 Bezirksamtsvorlage in Mitte

Ein Bürger begehrte vom Bezirksamt Mitte die Übermittlung der Bezirksamtsvorlage Nr. 1400/2021, die die Genehmigung einer Zusatzvereinbarung eines Kaufvertrags zum Besucher- und Informationszentrum des Deutschen Bundestags zum Gegenstand hat. Der Antrag wurde mit der Begründung abgelehnt, es handle sich um ein internes Dokument, das dem Willensbildungsprozess und der Beratung innerhalb des Bezirksamts diene und damit nicht dem Informationsrecht nach dem IFG unterliege.

Wir haben den Widerspruch des Bürgers gegen diese Entscheidung unterstützt. Eine Akteneinsicht oder -auskunft soll versagt werden, wenn sich der Inhalt der Akten auf den Prozess der Willensbildung innerhalb von und zwischen Behörden bezieht.[284] Das Recht auf Akteneinsicht oder -auskunft besteht nicht, soweit sich Akten auf die Beratung des Senats und der Bezirksämter sowie deren Vorbereitung beziehen.[285] Diese Vorschrift schützt den Kernbereich der exekutiven Eigenverantwortung, also das Beratungsgeheimnis der genannten Gremien. Hierzu zählt nur die Besprechung, Beratschlagung und Abwägung, mithin der eigentliche Vorgang des Überlegens. Nicht geschützt sind bei beiden genannten Ausnahmetatbeständen die Tatsachengrundlagen und das Ergebnis der Willensbildung.[286]

283 § 18 Abs. 2 Satz 2 IFG.
284 § 10 Abs. 4 IFG.
285 § 10 Abs. 3 Nr. 1 IFG.
286 VG Berlin, Urteil vom 25. August 2016, 2 K 92.15.

Daher teilten wir dem Bezirksamt mit, dass eine Bezirksamtsvorlage nur die Tatsachengrundlage für den späteren Bezirksamtsbeschluss bildet und deshalb grundsätzlich offenzulegen sei. Das Bezirksamt hielt andere Bezirksamtsvorlagen offenbar regelmäßig selbst nicht für schutzbedürftig, denn zahlreiche Vorlagen sind sogar proaktiv im bezirklichen Internetangebot offengelegt. Deshalb machten wir deutlich, dass der Widerspruchsbescheid ggf. zusätzlich Aussagen enthalten müsse, aus denen sich der Schutzbedarf gerade in Bezug auf die im vorliegenden Fall beantragte Bezirksamtsvorlage ergibt.

Aufgrund unserer Intervention hat das Bezirksamt Mitte dem Bürger schließlich nicht nur das gewünschte Dokument gebührenfrei übersandt, sondern dieses zusätzlich auf der bezirklichen Website veröffentlicht.

Wir begrüßen die reibungslose Kommunikation mit dem Bezirksamt und im vorliegenden Fall insbesondere, dass auch unsere Empfehlung aufgegriffen wurde, das beantragte Dokument nachträglich für alle Interessierten im Internet zugänglich zu machen.

16.12 Lebensmittelkontrollen in Pankow

Uns erreichten zwei Beschwerden über das Veterinär- und Lebensmittelaufsichtsamt Pankow. In einem Fall begehrte ein Bürger Informationen über die letzten Lebensmittelkontrollen in einem Biomarkt. In einem anderen Fall erfragte ein Bürger angesichts der automatisierten Verweise das Aktenzeichen und den Gerichtsstand des Musterverfahrens sowie Anweisungen, die den Umgang mit Anfragen zu Kontrollberichten betreffen.

Im ersten Fall erhielt der Bürger auf seine zahlreichen Erinnerungen jedes Mal die folgende Standardnachricht: „Das anhängige Musterverfahren beim Verwaltungsgericht ist noch nicht abschließend entschieden. Sobald eine Entscheidung vorliegt, wird entsprechend verfahren. Bis zu diesem Zeitpunkt wird darum gebeten, von Nachfragen abzusehen. Alternativ verweisen wir auf unsere Internetseite […].“ Wir mussten dem Bürger mitteilen, dass wir in dieser Sache nicht vermitteln können. Denn unsere Behörde hat in Angelegenheiten des hier tangierten Gesetzes zur Verbesserung der

gesundheitsbezogenen Verbraucherinformation[287] nicht die Funktion einer Schiedsstelle inne. Diese Funktion wurde uns nur in Bezug auf das IFG vom Landesgesetzgeber übertragen.[288] Wir konnten dem Bürger hier also nicht dazu verhelfen, dass das Bezirksamt Pankow einen inhaltlichen Bescheid erteilt.

Im zweiten Fall wurden wir allerdings gegenüber dem Bezirksamt Pankow tätig. Denn das Bezirksamt verkannte, dass bei den wenigen begehrten Informationen keine gesundheitsbezogenen Verbraucherinformationen betroffen, sondern nur allgemeine Informationen gewünscht waren, für die das IFG gilt. Das Amt nannte uns daraufhin das Aktenzeichen und das zuständige Gericht, informierte uns aber auch darüber, dass die angefragten Anweisungen nicht existieren. Diese Information hatte es dem Bürger zunächst verschwiegen. Erst nach unserem Hinweis, dass unsere Behörde nur als Schiedsstelle und nicht als Überbringerin von Antworten der angefragten Stelle an die antragstellende Person agiert, holte das Amt sein Versäumnis nach und unterrichtete den Bürger.

Bei Anfragen im Zusammenhang mit Lebensmittelkontrollen muss die angefragte Behörde in jedem Einzelfall genau prüfen, welche Rechtsgrundlage für die Offenlegung von Informationen in Betracht kommt.

287 Abgekürzt auch als Verbraucherinformationsgesetz (VIG) bezeichnet.
288 § 18 IFG.

16.13 IFG-Verweigerung beim RBB

Wir erhielten zwei Beschwerden von Bürgern gegen den Rundfunk Berlin-Brandenburg (RBB). In einem Fall wurde die Offenlegung der Position des RBB im Vorfeld der Ausarbeitung der Staatsvertragsnovelle in Bezug auf die Einstellung der terrestrischen bzw. linearen Hörfunkverbreitung über UKW, die DAB-Verbreitung und die Verbreitung von Hörfunkprogrammen über Mobilfunk erbeten. Im anderen Fall begehrte ein Bürger Einzelheiten zum „Ideenmanagement" im RBB, d. h. welche Verbesserungsvorschläge seit 2018 eingereicht und mit einer Geld- oder Sachprämie belohnt wurden.

Beide Begehren wurden seitens des RBB abgelehnt und die Ablehnung wie folgt standardmäßig begründet: „Eine Auskunftsverpflichtung des RBB kann lediglich für die Bereiche bestehen, in denen der RBB im engeren Sinne hoheitlich tätig wird, z. B. im Rahmen des Einzugs von Rundfunkbeiträgen oder bei der Vergabe von Sendezeiten an Parteien." Zusätzlich wurde darauf hingewiesen, dass von der Auskunftspflicht des RBB grundsätzlich der gesamte Bereich redaktionell-journalistischer Tätigkeit ausgenommen sei und nach dem IFG auch keine Informationen gewährt werden müssten, die in irgendeiner Weise Rückschlüsse auf das Redaktionsgeheimnis und den Programmauftrag zuließen.

In Bezug auf den Beschwerdefall „Staatsvertragsnovelle" haben wir dem RBB mitgeteilt, dass er sich dem Informationszugang hier nicht entziehen könne, weil die Stellungnahmen des RBB nicht zur in der Tat verfassungsrechtlich geschützten journalistisch-redaktionellen Tätigkeit[289] gehören und auch nicht das Redaktionsgeheimnis betreffen. Denn hierzu gehört vor allem die Geheimhaltung der Informationsquellen. Solche Informationen waren hier aber nicht tangiert. Auch ein inhaltlicher Bezug des Auskunftsbegehrens zum Programmauftrag[290] war nicht ersichtlich. Wir haben deshalb um Überprüfung des Informationsbegehrens gebeten, und zwar unter Beachtung der Möglichkeit einer unter Umständen nur teilweisen Offenlegung.[291]

289 Diese Tätigkeit unterfällt dem Schutzbereich von Art. 5 Abs. 1 Satz 2 Grundgesetz (GG).
290 Dieser ist in § 26 Medienstaatsvertrag (MStV) und § 3 des Staatsvertrags über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg (RBB-Staatsvertrag) festgelegt.
291 Siehe § 12 IFG.

Zum Beschwerdefall „Ideenmanagement“ haben wir dem RBB dargelegt, dass die gewählte Standardformulierung als alleinige Begründung für die Informationsverweigerung nicht ausreiche, sondern das konkrete Begehren des Bürgers IFG-konform zu beantworten sei. Der RBB hat dem Antragsteller schließlich mitgeteilt, dass die gewünschten Informationen nicht vorhanden seien.

Auch der RBB ist grundsätzlich zu einer IFG-konformen Bescheidung, ggf. unter Berücksichtigung der IFG-Ausnahmetatbestände,[292] verpflichtet. Wird der Informationszugang nach dem IFG verweigert, ist diese Entscheidung letztlich auch gerichtlich überprüfbar.[293]

16.14 Informationszugang bei der Tempelhof Projekt GmbH

Eine Bürgerin begehrte bei der Tempelhof Projekt GmbH, ein zu 100 % landeseigenes Unternehmen, eine Übersicht über sämtliche Gutachten mit Umweltrelevanz zum Flughafengebäude Tempelhof. Die GmbH teilte ihr mit, dass sie nicht unter den Anwendungsbereich des IFG falle. Die Bürgerin bat uns um Unterstützung ihres Anliegens.

Wir haben die Tempelhof Projekt GmbH darauf aufmerksam gemacht, dass sie zwar nicht dem Anwendungsbereich des IFG im Hinblick auf allgemeine Informationen unterliegt,[294] dass jedoch der Zugang zu Umweltinformationen, wie den hier erfragten, von den Sonderregelungen in § 18a IFG i. V. m. dem Umweltinformationsgesetz (UIG) bestimmt wird.[295] Private informationspflichtige Stellen können demnach solche sein,[296] die öffentliche Aufgaben wahrnehmen oder öffentliche Dienstleistungen erbringen, die im Zusammenhang mit der Umwelt stehen, insbesondere solche der umweltbezogenen Daseinsvorsorge, und dabei der Kontrolle des Landes Berlin oder einer unter der Aufsicht des Landes Berlin stehenden juristischen Person des öffentlichen Rechts

292 §§ 5 ff. IFG.
293 Siehe Art. 19 Abs. 4 GG (Rechtsweggarantie).
294 § 2 Abs. 1 IFG.
295 Siehe § 2 Abs. 2 IFG.
296 Siehe § 2 Abs. 1 Nr. 2 UIG.

unterliegen. Vor diesem Hintergrund haben wir die GmbH gebeten, den Antrag erneut zu prüfen und nach den Vorgaben von § 18a IFG i.V.m. dem UIG zu bescheiden. Zusätzlich haben wir darauf hingewiesen, dass im vorliegenden Fall der Rechtsweg zum Verwaltungsgericht Berlin gegeben ist.[297] Das bedeutet, dass die Antragstellerin die Entscheidung der GmbH ggf. gerichtlich überprüfen lassen kann, was wir ihr auch empfohlen haben. Allerdings mussten wir der Bürgerin mitteilen, dass wir darüber hinaus nicht weiter für sie tätig werden können, weil sich unsere Schiedsstellenfunktion formal nur auf Behörden und sonstige öffentliche Stellen des Landes Berlin erstreckt.[298]

Die Offenlegung von Umweltinformationen kann nicht nur bei öffentlichen Stellen, sondern grundsätzlich auch von privaten Einrichtungen verlangt werden.

297 § 18a Abs. 3 IFG.
298 § 18 Abs. 2 Satz 1 IFG.

17 Aus der Dienststelle

Unsere Dienststelle hat in diesem Jahr einige grundlegende Neuerungen erfahren. Neben dem Umzug in ein neues Dienstgebäude war für uns vor allem die Wahl und Besetzung der vakanten Stelle der Berliner Beauftragten für Datenschutz und Informationsfreiheit entscheidend.

Nach dem Ausscheiden von Maja Smoltczyk Ende Oktober 2021 war die Stelle der Berliner Beauftragten für Datenschutz und Informationsfreiheit über ein Jahr lang nicht besetzt. In dieser Zeit wurde die Dienststelle kommissarisch von Stellvertreter Volker Brozio geleitet. Am 6. Oktober dieses Jahres wurde Meike Kamp zur neuen Berliner Beauftragten für Datenschutz und Informationsfreiheit gewählt. Mit ihrem Amtsantritt am 15. November hat sie die Leitung der Dienststelle übernommen.

Ende September ist unsere Behörde von der Friedrichstraße in neue Diensträume in Alt-Moabit gezogen.

17.1 Zusammenarbeit mit dem Abgeordnetenhaus

Der Ausschuss für Digitalisierung und Datenschutz (DiDat) trat in diesem Jahr insgesamt 17 Mal zusammen und befasste sich mit Themen der Modernisierung und digitalen Transformation der Verwaltung. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit nahm an allen Sitzungen teil und beriet das Gremium umfassend gemeinsam mit ihren Expert:innen.

Die Umsetzung des Onlinezugangsgesetzes,[299] die Digitalisierung der Krankenhäuser[300] und der Schulen[301] waren dabei wichtige Tagesordnungspunkte auf der Agenda des Ausschusses. In einer der letzten Sitzungen des Jahres erhielt Meike Kamp, die neu gewählte Berliner Beauftragte für Datenschutz und Informations

299 Siehe 1.2.
300 Siehe 5.1.
301 Siehe 4.4.

freiheit, Gelegenheit, dem Ausschuss ihre Vorstellungen für die kommende Amtszeit darzulegen.[302]

17.2 Zusammenarbeit in nationalen und internationalen Konferenzen

Unsere Behörde nahm auch in diesem Jahr an den Treffen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) sowie der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) teil und arbeitete intensiv mit den Kolleg:innen der anderen Bundesländer zusammen.

Die DSK tagte in diesem Jahr unter dem Vorsitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 22. bis 24. März in Bonn und vom 22. bis 24. November in Königswinter. Daneben fanden drei Zwischenkonferenzen am 27. Januar, 22. Juni und 21. September in Berlin statt. Die DSK fasste während ihrer Sitzungen zahlreiche Entschließungen und Beschlüsse zu aktuellen datenschutzrechtlichen Themen, u. a. zum datenschutzkonformen Onlinehandel mittels Gastzugang,[303] zu Facebook-Seiten und zur Verarbeitung von personenbezogenen Daten für Zwecke der wissenschaftlichen Forschung.[304]

Die IFK tagte vom 29. bis 30. Juni und vom 8. bis 9. November jeweils in Kiel unter dem Vorsitz der Landesbeauftragten für Datenschutz Schleswig-Holstein. Es wurden drei Entschließungen gefasst: zum Informationszugang zu sämtlicher behördlicher Kommunikation, zum Informationszugang bei Stiftungen bürgerlichen Rechts und zur Notwendigkeit eines Transparenzgesetzes in Niedersachsen.[305]

Die Global Privacy Assembly (GPA)[306] fand als zweitägige Präsenzkonferenz vom 27. bis 28. Oktober in Istanbul statt. Im Fokus der Konferenz stand das Recht auf Privatsphäre in einer Zeit des rasanten technologischen Fortschritts. Darüber hin

302 Siehe https://www.parlament-berlin.de/ados/19/DiDat/protokoll/dd19-016-ip.pdf.
303 Siehe 10.4.
304 Alle Entschließungen und Beschlüsse der DSK sind auf unserer Website unter https://www.datenschutz-berlin.de/infothek/beschluesse-der-dsk abrufbar.
305 Siehe 16.1.
306 Ehemals International Conference of Data Protection and Privacy Commissioners.

aus war die institutionelle Entwicklung der GPA wieder ein wichtiges Thema. Die GPA nahm zahlreiche Entschließungen und Berichte an, u.a. über die Grundsätze und Erwartungen für die angemessene Nutzung personenbezogener Daten in der Gesichtserkennungstechnologie.[307]

17.3 Servicestelle Bürgereingaben

Die Servicestelle Bürgereingaben stellt den zentralen Anlaufpunkt für Personen dar, um eine Verletzung ihrer Datenschutzrechte bei uns anzuzeigen oder sich über Möglichkeiten zum Selbstdatenschutz zu informieren. In diesem Jahr erreichten uns knapp 4.500 Eingaben, die von der Servicestelle entweder durch kurzfristige Beratung oder Bereitstellung der benötigten Informationen bearbeitet oder in formale Verwaltungsverfahren überführt wurden.

Wie in sämtlichen Bereichen unserer Behörde wurden weitere Fortschritte hinsichtlich der anstehenden Umstellung auf ein voll digitalisiertes Verfahren erzielt. Von den knapp 4.500 Anfragen und Beschwerden, die die Servicestelle in diesem Jahr verzeichnete, wurden mehr als 1.500 in Verwaltungsvorgänge überführt. Thematisch hervorzuheben sind die Datenverarbeitungen im Gesundheitsmanagement, wo fortschreitende Digitalisierungsprozesse und die Corona-Pandemie eine Rolle spielten.[308] Auch bei Unternehmen der Wohnungswirtschaft, bei Zahlungsdiensten und bei Mobilitätsunternehmen herrscht oftmals Nachbesserungsbedarf im Umgang mit personenbezogenen Daten.[309] Ebenso finden sich staatliche Stellen und hier insbesondere die Polizeibehörden immer wieder in unserem Ermittlungsfokus.[310] Vermehrt erreichten uns zudem Anfragen aufgrund von Betrugsversuchen auf Onlineplattformen, Abmahnschreiben oder gefälschten Angaben auf Internetseiten, die auf unterschiedliche Weise auch Datenschutzrechte betroffener Personen beeinträchtigten.[311] Außerdem sorgte die Durchführung des Zensus für eine Vielzahl von Eingaben durch Personen, die die

307 Alle Entschließungen und Berichte der GPA sind auf deren Website unter https://globalprivacyassembly.org/document-archive/adopted-resolutions/ und https://globalprivacyassembly.org/document-archive/working-group-reports/ abrufbar.
308 Siehe 5.2-5.4; 12.1-12.2.
309 Siehe 6.2; 9.1-9.2; 11.1-11.2; 13.4.
310 Siehe 2.1-2.3; 12.3.
311 Siehe 10.11; 12.6; 13.1.

dort getätigten Abfragen für zu weitgehend hielten.[312] Diese wurden von uns zuständigkeitshalber an die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht (LDA) Brandenburg abgegeben.

Vielfach mussten wir in diesem Jahr auf andere Behörden oder Institutionen verweisen, wenn Betrugsversuche im digitalen Raum zwar die Verarbeitung personenbezogener Daten beinhalteten, ein Datenschutzverstoß aber nicht im Vordergrund stand. So zeigten sich einige Personen besorgt, bei einem Internetportal gemeldet zu werden, das vorgeblich Impfgegner:innen an Gesundheitsämter melden sollte. Im Impressum des Portals wurde eine Scheinbehörde genannt, die tatsächlichen Urheber:innen waren nicht zu ermitteln. Personen, die befürchteten, über das Portal gemeldet worden zu sein, empfahlen wir eine Selbstauskunftsanfrage beim zuständigen Gesundheitsamt, für weitere Schritte konnten wir nur an die Strafverfolgungsbehörden verweisen. Mittlerweile ist die Website gesperrt.

Ähnlich verhielt es sich bei gefälschten Einladungen, die vermeintlich durch die Polizei unter Abfrage persönlicher Daten per E-Mail versendet wurden. Hier konnten wir über den mutmaßlichen Phishing-Betrug aufklären, verwiesen aber zugleich an die Polizei, die sich angesichts der Betrugsversuche ebenfalls an die Öffentlichkeit gewandt hatte. Auch die vielfach wegen des Einbettens von Google Fonts auf der eigenen Website versendeten Abmahnungen durch eine Anwaltskanzlei wurden uns von Betroffenen weitergeleitet. Hier konnten wir über den Sachverhalt aufklären und in vielen Fällen für etwas Beruhigung sorgen, was den Schutz der eigenen Daten angeht.[313]

Bei der Servicestelle Bürgereingaben gehen in hoher Zahl unterschiedlichste Anfragen zum Datenschutz und zur Informationsfreiheit ein. Auch hinsichtlich anderer Lebensbereiche, die Bezüge zum Datenschutz und zur digitalen Welt aufweisen, wenden sich Berliner:innen vertrauensvoll an uns.

312 Siehe 2.6.
313 Siehe 13.1.

17.4 Datenschutzkompetenz für Kinder und Jugendliche

Nach den Einschränkungen durch die Corona-Pandemie konnten wir in diesem Jahr wieder regelmäßig Workshops an Grundschulen anbieten. Zudem haben wir unsere Websites für Kinder und Jugendliche überarbeitet und stellten neues Unterrichtsmaterial für Lehrkräfte bereit.

In unseren Schul-Workshops, die jeweils fünf Unterrichtsstunden umfassen, entdecken die Kinder der Jahrgangsstufen 4 bis 6, was Daten sind, wie sie erhoben werden und wieso sie schützenswert sind. Anhand von eigens erstellten Fallbeispielen vertiefen die Schüler:innen ihr Verständnis von personalisierter Werbung und der Nutzung bereits veröffentlichter Daten. Von Anfang Mai bis zum Jahresende haben wir 15 Workshops durchgeführt und so über 300 Schüler:innen erreicht. Ein Baustein ist dabei auch die Zusammenarbeit mit der KinderUni Lichtenberg (KUL), für die wir im Rahmen von „KUL unterwegs“ 90-minütige Workshops zum Thema „Deine Daten, deine Rechte“ entwickelt haben.[314] Diese fanden im Herbst an Schulen in Lichtenberg, Treptow-Köpenick, Wuhletal und Buch statt.

Anlässlich des diesjährigen Safer Internet Day veröffentlichten wir im Frühjahr zudem neue Unterrichtsmaterialien zum Thema Datenschutz und Sicherheit im Internet.[315] Diese sind in fünf Einheiten aufgeteilt, in denen die Schüler:innen u. a. lernen, was personenbezogene Daten sind, welche Rechte sie haben und was es beim Onlineunterricht zu beachten gilt. Die Materialien richten sich an Lehrkräfte der Klassen 4 bis 6, können aber bei Bedarf auch an die Bedürfnisse höherer Klassen angepasst werden. Die Einheiten sind jeweils für eine Schulstunde konzipiert und enthalten neben Arbeitsblättern auch eine detaillierte Anleitung sowie Hintergrundinformationen für die Lehrer:innen.

Ebenso für Lehrkräfte haben wir im Rahmen des Aktionstags „Datenkompetenz macht Schule“ einen Datenschutz-Workshop angeboten. Der Aktionstag fand am 17. Mai dieses Jahres statt und wurde von DigiBitS (Digitale Bildung trifft Schule), einem Projekt

314 Siehe https://kul-unterwegs.de/angebot/workshop/deine-daten-deine-rechte.
315 Abrufbar unter https://data-kids.de/fuer-lehrkraefte/unterrichtsmaterialien.

vom Deutschland sicher im Netz e. V., organisiert.[316] An unserem Workshop nahmen rund 40 Lehrer:innen teil, denen wir diejenigen Datenschutzregelungen vermittelten, die im Umgang mit personenbezogenen Daten von Schüler:innen besonders zu beachten sind. Die Teilnehmer:innen erfuhren, wie Kinder und Jugendliche für den sicheren Umgang mit ihren persönlichen Daten sensibilisiert werden können, und erhielten praxisnahe und methodische Anregungen, um die Medienkompetenz der Schüler:innen zu stärken.

In einer länderübergreifenden Arbeitsgruppe haben wir zudem die Website youngdata.de neu konzipiert und deren Relaunch im kommenden Jahr vorbereitet. Youngdata ist ein Internetportal für Jugendliche, das von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder sowie des Schweizer Kantons Zürich angeboten wird. Auf dieser Plattform finden Jugendliche und junge Erwachsene Informationen zum Datenschutz und zu ihrem Recht auf Informationsfreiheit. Auch unsere Website data-kids.de, die sich vor allem an Kinder im Alter von 6 bis 12 Jahren sowie Eltern und Pädagog:innen richtet, haben wir um weitere Materialien und neue Formate ergänzt.

17.5 Öffentlichkeitsarbeit

Der Schwerpunkt unserer Öffentlichkeitsarbeit lag in diesem Jahr im Ausbau der digitalen Kommunikation und der Erweiterung unseres medialen Informationsangebots. So eröffneten wir unser Profil bei Mastodon, führten unsere Start-up-Schule ein und überarbeiteten unseren Internetauftritt.

Mitte Februar starteten wir unseren Account im sozialen Netzwerk Mastodon.[317] Bei Mastodon handelt es sich um einen dezentralen Mikrobloggingdienst, der eine datenschutzgerechte Alternative zu Twitter darstellt. Über ein Profil werden kurze Beiträge veröffentlicht, in denen wir auf aktuelle Themen des Datenschutzes und der Informationsfreiheit aufmerksam machen und Fragen von mittlerweile knapp 2.400 Follower:innen beantworten.

316 Siehe https://www.sicher-im-netz.de/datenkompetenz-mit-digibits---aktionstag-für-mehr-digitale-aufklärung.

317 Siehe https://social.bund.de/@blnbdi.

Mit der Einführung der virtuellen Veranstaltungsreihe „Start-up-Schule“ Ende März konnten wir unser Angebot an Informationsveranstaltungen erweitern. Die Start-up-Schule richtet sich an Berliner Start-ups und Vereine, die wir mit den Veranstaltungen in datenschutzrechtlichen Belangen gezielt unterstützen.[318] Die vorgestellten Themenbereiche reichten von der Einhaltung des Datenschutzes bei der Datenverarbeitung und der Einbindung externer Dienstleister:innen über die datenschutzkonforme Gestaltung von Websites bis hin zur Erfüllung der unternehmerischen Transparenzpflichten. Die Start-up-Schule resultiert aus dem bisherigen Angebot der Start-up-Sprechstunde und bündelt das anhaltend starke Informationsbedürfnis neu gegründeter Unternehmen und Vereine zu Themen des Datenschutzes und der Anwendung der datenschutzrechtlichen Vorschriften.

Nach den pandemiebedingten Einschränkungen haben wir in diesem Jahr wieder verstärkt Präsenztermine wahrgenommen und unsere Arbeit mit Vorträgen und Informationsständen auf diversen Kongressen und Tagungen präsentiert. Vortragsthemen waren u. a. der Datenschutz im Schulkontext, die Videoüberwachung in Museen, die Sanktionspraxis der Datenschutzaufsichtsbehörden sowie die häufigsten Fragen zur Verwendung von Cookies. Durch die Teilnahme an den Veranstaltungen konnten wir die Bürger:innen über aktuelle datenschutzrechtliche Fragestellungen informieren und zahlreiche Kontakte für zukünftige Projekte und Kooperationen knüpfen.

318 Siehe https://www.datenschutz-berlin.de/themen/unternehmen/start-up-schule.

18 Statistik

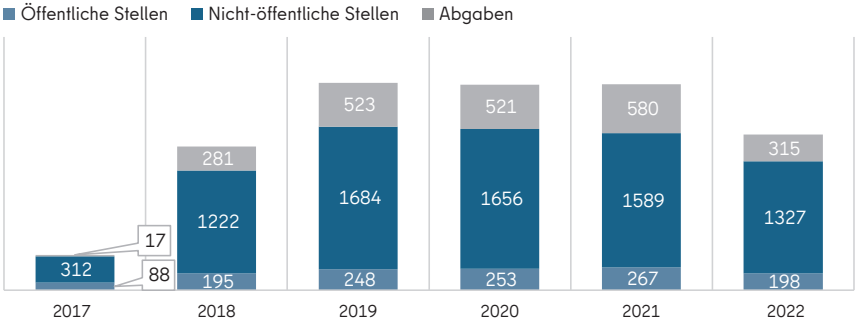
Die folgenden Ausführungen zur Anzahl der Beschwerden und Datenpannen im Jahr 2022 erfüllen nicht nur unsere Berichtspflichten aus der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG), sie orientieren sich auch an den einheitlichen Statistikkriterien, die die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beschlossen hat.

18.1 Beschwerden

Insgesamt erreichten unsere Behörde dieses Jahr 4.445 Eingaben von Betroffenen, von denen 840 als förmliche Beschwerden i. S. v. Art. 77 DSGVO zu behandeln waren. Für den Großteil der Beschwerden eröffneten wir Verfahren in eigener Zuständigkeit. Dies waren in diesem Jahr 1.525 Verfahren. Davon richteten sich knapp 85 % gegen private Stellen (1.327), der Rest gegen Behörden und andere öffentliche Stellen (198). In 315 Fällen lagen die Beschwerden nicht in unserem Zuständigkeitsbereich, weshalb sie den jeweils zuständigen Aufsichtsbehörden übergeben wurden.

Die nachfolgende Grafik führt die Anzahl der Beschwerden gegenüber öffentlichen und nicht-öffentlichen Stellen sowie über unsere Abgaben an andere deutsche Aufsichtsbehörden im Vergleich der letzten sechs Jahre auf.

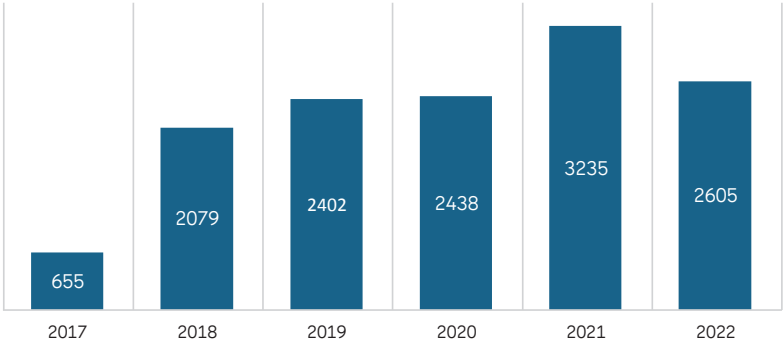
Beschwerden



18.2 Beratungen

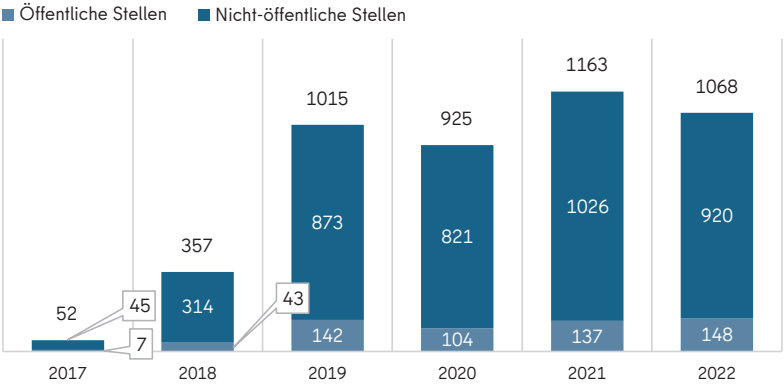
Unter Beratungen sind alle schriftlichen Auskünfte gegenüber betroffenen Personen, Verantwortlichen und Vertreter:innen der öffentlichen Verwaltung zusammengefasst. Den Schwerpunkt nahmen mit 2.605 Fällen die Beratungen betroffener Personen ein. Daneben berieten wir Verantwortliche in 133 Fällen und erteilten eine Vielzahl telefonischer Auskünfte, die statistisch jedoch nicht erfasst werden.

Beratungen betroffener Personen



18.3 Datenpannen

Meldungen von Datenpannen



In diesem Jahr kam es zu insgesamt 1.068 Meldungen, von denen 920 Meldungen auf den nicht-öffentlichen Bereich, d. h. vor allem auf private Unternehmen, entfielen. Öffentliche Stellen meldeten uns 148 Datenpannen.

18.4 Abhilfemaßnahmen

Stellen wir einen Verstoß von Verantwortlichen gegen die DSGVO fest, können wir verschiedene Abhilfemaßnahmen ergreifen.[319] Dementsprechend haben wir in diesem Jahr 7 Warnungen und 269 Verwarnungen ausgesprochen. In einem Fall wurde eine Anordnung erlassen. Wir haben 35 Bußgeldbescheide mit 326 Bußgeldern in Höhe von insgesamt 716.575 Euro erlassen. Die entsprechenden Verfahren waren bis zum Ende des Jahres jedoch noch nicht alle rechtskräftig abgeschlossen. Zudem wurden 44 Zwangsgeldbescheide erlassen. In 5 Fällen haben wir einen Strafantrag gestellt. Über das Jahr verteilt wurden 23 Bußgeldverfahren eingestellt. Zusätzlich wurde eine größere Anzahl weiterer Verfahren eröffnet, in denen noch kein Bescheid ergangen ist.

Abhilfemaßnahmen 2022

Warnungen	7
Verwarnungen	269
Anweisungen und Anordnungen	4
Geldbußen	326

319 Siehe Art. 58 Abs. 2 DSGVO.

18.5 Förmliche Begleitung bei Rechtsetzungsvorhaben

Unsere Behörde hat nach dem Berliner Datenschutzgesetz (BlnDSG) u. a. die Aufgabe, das Abgeordnetenhaus, den Senat und andere Gremien und Einrichtungen über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen zu beraten.[320] Dazu gehören sowohl schriftliche Stellungnahmen als auch Besprechungen mit Fraktionen und Abgeordneten sowie förmliche Anhörungen im Abgeordnetenhaus und in dessen Ausschüssen.

In diesem Jahr haben wir mehrere Gesetzgebungsvorhaben begleitet, wie z. B. die Novellierung des Landeskrankenhausgesetzes (LKG).[321] Gemeinsam mit der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA) Brandenburg gaben wir eine Stellungnahme zum Entwurf des RBB-Staatsvertrags ab.[322] Hinzu kamen Beratungen bei Rechtsetzungsvorhaben, die die Schaffung und Änderung von Rechtsverordnungen und Verwaltungsvorschriften zum Gegenstand hatten. Als Beispiel sei hier die Anpassung der Ausführungsvorschriften für die Jugendhilfe im Strafverfahren (JuHiS) an die Regelungen der DSGVO genannt.[323] Bei Projekten der Bundesgesetzgebung nahmen wir zudem gemeinsam mit den anderen Aufsichtsbehörden des Bundes und der Länder Stellung.

18.6 Europäische Verfahren

Die DSGVO sieht vor, dass die europäischen Datenschutzaufsichtsbehörden bei grenzüberschreitenden Fällen zusammenarbeiten.[324] Im Rahmen des Kooperationsverfahrens wird dazu eine federführende Aufsichtsbehörde bestimmt, die im jeweiligen Fall die Ermittlungen führt.[325] Weitere Aufsichtsbehörden können sich als betroffene Behörden melden, wenn die Verantwortlichen über eine Niederlassung in ihrem Land verfügen oder die Datenverarbeitung erhebliche Auswirkungen auf die Bürger:innen ihres Lan

320 § 11 Abs. 1 Satz 1 Nr. 3 BlnDSG.
321 Siehe 5.1.
322 Siehe 13.5.
323 Siehe 4.1.
324 Art. 60 ff. DSGVO; siehe auch 15.4.
325 Art. 56 Abs. 1 DSGVO.

des hat. Nach Abschluss ihrer Ermittlungen legt die federführende Aufsichtsbehörde den betroffenen Aufsichtsbehörden einen Beschlussentwurf zur Stellungnahme vor.[326]

Insgesamt veröffentlichte unsere Behörde in diesem Jahr 15 Beschlussentwürfe und 15 endgültige Beschlüsse. Zur Abstimmung und Kooperation nutzen wir wie die anderen europäischen Aufsichtsbehörden das elektronische Binnenmarkt-Informationssystem (IMI). Die nachfolgende Tabelle gibt einen Überblick über unsere Beteiligung an den wichtigsten dieser europäischen Verfahren.

Europäische Verfahren mit unserer Beteiligung 2022

Verfahren nach Art. 56 DSGVO (betroffen)	335
Verfahren nach Art 56 DSGVO (federführend)	21
Verfahren nach Art. 60 ff. DSGVO (federführend)	30

326 Art. 60 Abs. 3 Satz 2 DSGVO.

www.datenschutz-berlin.de

BERLIN