Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Datenschutz und Informationsfreiheit

Jahresbericht 2020

Jahresbericht

der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2020

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis ihrer Tätigkeit vorzulegen (§§ 12 Berliner Datenschutzgesetz, 18 Abs. 4 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den am 3. April 2020 vorgelegten Jahresbericht 2019 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2020 ab.

Der Jahresbericht ist auch auf unserer Internetseite abrufbar, siehe unter: https://www.datenschutz-berlin.de

Impressum

Herausgeberin: Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin
Telefon: (0 30) + 138 89-0
Telefax: (0 30) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: https://www.datenschutz-berlin.de/

Gestaltung: april agentur GbR

Satz: LayoutManufaktur.com

Druck: ARNOLD group

Inhalt

Abkürzungsverzeichnis

Abghs.-Drs.	Abgeordnetenhausdrucksache
ADFC	Allgemeiner Deutscher Fahrrad-Club
AfD	Alternative für Deutschland
AO	Abgabenordnung
ASOG	Allgemeines Sicherheits- und Ordnungsgesetz
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BlnAGBMG	Berliner Ausführungsgesetz zum Bundesmeldegesetz
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BlnDSAnpG-EU	Berliner Datenschutz-Anpassungsgesetz EU
BlnDSG	Berliner Datenschutzgesetz
BlnTG	Berliner Transparenzgesetz
BMG	Bundesmeldegesetz
BR-Drs.	Bundesratsdrucksache
BürgBG RP	Landesgesetz über den Bürgerbeauftragten des Landes Rheinland-Pfalz und den Beauftragten für die Landespolizei
BvD	Bundesverband der Datenschutzbeauftragten e. V.
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVG	Berliner Verkehrsbetriebe
BWG	Bundeswahlgesetz
BWO	Bundeswahlordnung
DAkks	Deutsche Akkreditierungsstelle
DEHOGA	Deutscher Hotel- und Gaststättenverband
DIHK	Deutscher Industrie- und Handelskammertag e. V.
Drs.	Drucksache
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
EDSA	Europäischer Datenschutzausschuss

EFM	Elektronisches Fahrgeldmanagement
EG	Erwägungsgrund
EGMR	Europäischer Gerichtshof für Menschenrechte
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuWG	Europawahlgesetz
EWR	Europäischer Wirtschaftsraum
GBV	Grundbuchverfügung
GDD	Gesellschaft für Datenschutz und Datensicherheit e. V.
GewO	Gewerbeordnung
GG	Grundgesetz
GJPA	Gemeinsames Juristisches Prüfungsamt Berlin-Brandenburg
GKDZ	Gemeinsames Kontroll- und Dienstleistungszentrum
GRCh	Charta der Grundrechte der Europäischen Union
GStU	Gesamtstädtische Steuerung der Unterbringung
GVBl.	Gesetz- und Verordnungsblatt für Berlin
GVG	Gerichtsverfassungsgesetz
HGB	Handelsgesetzbuch
IBAN	Internationale Bankkontonummer
ID	Identifikator
IFG	Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
IfSG	Infektionsschutzgesetz
IKT	Informations- und Kommunikationstechnik
IMI	Binnenmarkt-Informationssystem
IT	Informationstechnik
ITDZ	IT-Dienstleistungszentrum Berlin
IWGDPT	Internationale Arbeitsgruppe für Datenschutz in der Technologie (Berlin-Group)
JB	Jahresbericht
KG	Kammergericht
KI	Künstliche Intelligenz
KTDat	Ausschuss für Kommunikationstechnologie und Datenschutz
LKG	Landeskrankenhausgesetz
LMÜTranspG	Lebensmittelüberwachungstransparenzgesetz
MDK	Medizinischer Dienst der Krankenversicherungen
ÖPNV	Öffentlicher Personennahverkehr

OVG	Oberverwaltungsgericht
OZG	Onlinezugangsgesetz
PassG	Passgesetz
PassVwV	Allgemeine Verwaltungsvorschrift zur Durchführung des Passgesetzes
PAuswG	Personalausweisgesetz
PKS	Polizeiliche Kriminalstatistik
POLIKS	Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung
rbb	Rundfunk Berlin–Brandenburg
RefE	Referentenentwurf
RegMoG	Registermodernisierungsgesetz
RL	Richtlinie
SaaS	Software-as-a-Service
SARS-CoV-2	schweres akutes respiratorisches Syndrom 2 (Coronavirus)
SBC	Server Based Computer
SchulG	Schulgesetz
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
TTDSG	Telekommunikations-Telemedien-Datenschutz-Gesetz
VAG	Gesetz über die Beaufsichtigung von Versicherungsunternehmen
VBB	Verkehrsverbund Berlin-Brandenburg
VDV	Verband Deutscher Verkehrsunternehmen
VersFG-E	Versammlungsfreiheitsgesetz-Entwurf
VersVermV	Versicherungsvermittlerverordnung
VG	Verwaltungsgericht
VSG Bln	Verfassungsschutzgesetz Berlin
VvB	Verfassung von Berlin
VwVfG Bln	Verwaltungsverfahrensgesetz Berlin
WbeauftrG	Gesetz über den Wehrbeauftragten des Deutschen Bundestages
WEG	Wohnungseigentumsgemeinschaft
ZBS	Zentraler Beitragsservice
ZPO	Zivilprozessordnung
ZustKatOrd	Zuständigkeitskatalog Ordnungsaufgaben

Hinweis
Das Glossar (am Ende der Broschüre) bietet eine Liste mit Erklärungen verschiedener Fachbegriffe.

Vorwort

Das Jahr 2020 war vor allem geprägt durch die Corona-Pandemie und ihre Auswirkungen auf das gesellschaftliche Leben, auf Bildung, Ausbildung und Arbeit. Unser Alltag wurde teilweise völlig auf den Kopf gestellt: Die Arbeit war plötzlich gar nicht mehr oder oft nur noch „Remote" – also aus der Ferne – möglich. Die Schulen zu, die Kindertagesstätten im Notbetrieb, die meisten Behörden und anderen öffentlichen Einrichtungen allenfalls zeitweise geöffnet. Geschäfte – mit einigen wenigen Ausnahmen –, Gast- und Kulturstätten: Geschlossen. Und allem voran: Die empfindliche Einschränkung sozialer Kontakte. Der Lockdown löste einen wahren Digitalisierungsschub aus und stellte auch den Datenschutz auf eine harte Bewährungsprobe. Videokonferenzen, „Homeschooling" und digitale Kontaktnachverfolgung wurden quasi über Nacht zur neuen Selbstverständlichkeit. Nicht ganz so selbstverständlich hingegen war dabei der Rückgriff auf datenschutzkonforme Dienste und Software.

Dies mag in der ersten Phase unerwarteten und unmittelbaren Handlungsbedarfs nachvollziehbar gewesen sein, um das gesellschaftliche und wirtschaftliche Leben einigermaßen aufrechtzuerhalten. Die Nutzung nicht datenschutzgerechter und damit rechtlich nicht zulässiger Dienste darf sich aber nicht verstetigen. Die in der Zeit der Pandemie häufig überstürzte Digitalisierung eröffnet zugleich auch die Chance, sich der damit verbundenen Probleme und Gefahren bewusst zu werden, um nach Überwinden der kritischsten Pandemiephase nachzusteuern und intensiv an der datenschutzgerechten Gestaltung von Datenverarbeitungen zu arbeiten. Gerade jetzt sollten wir uns immer wieder vor Augen führen, dass der Datenschutz nicht der Verhinderung der Digitalisierung dient, sondern dem Schutz der Menschen vor den damit verbundenen Gefahren. Er ist ein Grundrecht der Bürgerinnen und Bürger und zugleich eine rechtliche Verpflichtung aller für die Datenverarbeitung Verantwortlichen, gegen die nicht verstoßen werden darf.

Dass der datenschutzkonforme Einsatz digitaler Mittel vielen Bürger*innen wichtig ist, zeigt sich auch an der Vielzahl von Anfragen und Beschwerden, die meine Behörde in der Hochphase der Pandemie zu diesem Themenkomplex erreicht hat. Wir haben daher bereits sehr früh grundsätzliche Empfehlungen und Hilfestellungen zum Einsatz digitaler Lernplattformen und zur Nutzung von Videokonferenzdiensten herausgegeben. Zusätzlich führten wir eine detailliertere Prüfung verschiedener Videokonferenzdienste durch, deren Ergebnis wir mit einer Ampelbewertung versehen und veröffentlicht haben. Unsere Hinweise riefen nicht nur bei den Nutzenden solcher Dienste, sondern auch bei den Diensteanbietern selbst ein großes Echo hervor. Rund ein Dutzend von ihnen hat in Folge unserer Veröffentlichung seine Verträge nach intensivem Austausch mit uns bis Ende 2020 datenschutzgerecht ausgestaltet. Die Auswahl an datenschutzfreundlichen Diensten ist inzwischen daher so groß, dass es keine Ausrede mehr für die Verwendung datenschutzrechtlich bedenklicher Angebote geben kann.

Dies ist ein gutes Beispiel dafür, dass Datenschutz kein Hindernis für die Digitalisierung ist, sondern im Gegenteil deren Qualität erhöht. Dass es dabei auch von Anfang an datenschutzkonform zugehen kann, zeigt die Entwicklung der Corona-Warn-App. In Windeseile wurde auf europäischer Ebene der datenschutzrechtliche Rahmen für mobile Anwendungen zur Kontaktnachverfolgung festgesetzt. Meine Behörde hat sich an der Ausarbeitung der entsprechenden Leitlinie tatkräftig beteiligt und die Verantwortlichen in Deutschland bei der Umsetzung der Vorgaben umfassend beraten. Und auch, wenn im Nachhinein Funktionalitäten bei der App vermisst werden, ändert dies nichts an dem grundsätzlichen Erfolg des Projekts. Die Corona-Warn-App ist der Beweis dafür, dass die Entwicklung datenschutzfreundlicher Lösungen möglich ist, wenn alle an einem Strang ziehen, und dass sie zugleich auch in Rekordzeit gelingen kann. Als solche stellt sie ein Musterbeispiel für andere digitale Projekte der öffentlichen Verwaltung dar. Und die große Zahl derjenigen, die die App nutzen, ist ein Beleg dafür, dass Menschen digitalen Produkten gegenüber offener sind, wenn sie darauf vertrauen können, dass ihre Daten nicht missbraucht werden. In Ländern, die sich für ein weniger datenschutzkonformes Modell entschieden haben, sind die Nutzungszahlen erheblich niedriger.

Etwas schleppender ging es dagegen bei der Anpassung des Berliner Landesrechts an die Vorgaben der europäischen Datenschutz-Grundverordnung (DS-GVO)

voran. Das Gesetzesvorhaben, mit dem etwa 80 Berliner Gesetze an das europäische Datenschutzrecht angeglichen wurden, wurde mehr als zwei Jahre nach Ablauf der Umsetzungsfrist schließlich vom Abgeordnetenhaus verabschiedet. Wir haben es – soweit es uns ermöglicht wurde – eng begleitet und unsere Expertise eingebracht. Trotzdem kann hinter dieses Großprojekt kein Haken gesetzt werden, denn das Berliner Landesrecht weist weiterhin zahlreiche datenschutzrechtliche Mängel auf und wird dem europäischen Rechtsrahmen nicht immer gerecht. Insbesondere das grundlegende datenschutzrechtliche Regelwerk Berlins, das Berliner Datenschutzgesetz, hat erhebliche Defizite im Bereich der Datenschutzaufsicht und -kontrolle. Es bleibt daher nur zu hoffen, dass das Abgeordnetenhaus unsere Kritik ernst nimmt und das Berliner Datenschutzgesetz – wie bereits angekündigt – noch in dieser Legislaturperiode evaluiert und entsprechend anpasst.

Währenddessen erhielt der Datenschutz auf europäischer Ebene erneut starken Rückenwind durch die EuGH-Entscheidung „Schrems II", die die Weltwirtschaft in Aufregung versetzte. Grundsätzlich dürfen nach der DS-GVO personenbezogene Daten nur in solche Drittländer übermittelt werden, die über ein Datenschutzniveau verfügen, das dem Schutzniveau der DS-GVO gleichwertig ist. Für die USA stellte das Gericht jedoch fest, dass US-Behörden zu weitreichende Zugriffsmöglichkeiten auf Daten europäischer Bürger*innen haben, und kippte in der Folge das sog. „EU-US Privacy Shield" als bis dahin verwendete Grundlage für Übermittlungen personenbezogener Daten in die USA. Damit dürfen personenbezogene Daten in der Regel nicht mehr in die USA übermittelt werden. Das Urteil hat zwar letztlich nichts Überraschendes verkündet, sondern sich nur auf die Regelungen der DS-GVO bezogen. Doch durch die unmissverständliche Klarstellung der Rechtslage sehen sich spätestens jetzt viele europäische Unternehmen vor enorme Herausforderungen gestellt, wenn sie auch nach Wirksamwerden der DS-GVO US-amerikanische Dienste und Software genutzt und auf das EU-US Privacy Shield als Rechtsgrundlage gesetzt haben. Der EuGH hat mit seiner Entscheidung klargemacht, dass das Privacy Shield keinen Bestand haben kann vor der DS-GVO. Damit hat es das Grundrecht auf informationelle Selbstbestimmung noch einmal erheblich gestärkt und deutlich gemacht, dass es wirtschaftlichen Interessen nicht untergeordnet werden darf – ein wichtiges Signal für alle europäischen datenverarbeitenden Stellen, die das Thema Datenschutz bislang eher stiefmütterlich behandelt und sich diesbezüglich eine „Wird-schon-gut-gehen"-Attitüde zugelegt haben.

Auch die Verwaltung muss eine andere Haltung einnehmen und sich bewusst machen, welche Daten sie verarbeitet und auf welche Weise dies geschieht. Zugleich muss sie sich weiter für Bürger*innen öffnen. Es ist daher überaus erfreulich, dass mit dem Referent*innenentwurf für ein Berliner Transparenzgesetz die Novellierung des Berliner Informationsfreiheitsgesetzes endlich Gestalt anzunehmen scheint. Ziel ist es, unabhängig von einem berechtigten Interesse ein umfassendes Recht auf Zugang zu amtlichen Informationen und Umweltinformationen zu gewährleisten und öffentliche Stellen antragsunabhängig zur Bereitstellung von Informationen in einem Transparenzportal zu verpflichten. Leider bleibt der derzeitige Entwurf des Gesetzes weit hinter den Erwartungen an ein modernes Transparenzgesetz zurück. Die zahlreich vorgesehenen Bereichsausnahmen und Einschränkungen der Veröffentlichungspflicht schränken die Informationsfreiheit nämlich de facto ein, anstatt sie auszuweiten. Damit läuft das Gesetz Gefahr, entgegen seiner ursprünglichen Bestimmung die Entwicklung einer modernen und transparenten Verwaltung eher zu unterbinden als zu fördern.

Vertrauen in staatliche Strukturen und in die Politik ist die grundlegende Basis für ein friedvolles und geordnetes Miteinander. Wie wichtig diese Parameter sind, zeigt uns die Corona-Pandemie Tag für Tag aufs Neue. Auch wenn manche von uns meinen, datenschutzrechtliche Fragen würden in diesen Zeiten eine eher nachgeordnete Rolle in unserem Leben spielen, dürfen wir nicht den Fehler begehen und ausblenden, dass dieses Bürger*innenrecht auch, nein gerade in Krisenzeiten ein Gut darstellt, das es unbedingt zu wahren gilt. Daten, die einmal digital verarbeitet wurden, sind der Gefahr des Missbrauchs ausgesetzt. Und Daten, die einmal in falsche Hände geraten sind, können nicht mehr zurückgeholt werden. Damit sind Betroffene unter Umständen ein Leben lang von schwerwiegenden Folgen bedroht.

Es kann daher nicht die Lösung sein, eine Absenkung des Datenschutzniveaus aus kurzsichtigen Praktikabilitätsgründen in Kauf zu nehmen. Ebenso wenig ist die Verbannung digitaler Mittel aus unserem Alltag die Lösung, sind sie doch unschätzbare Hilfsmittel, gerade auch um die Herausforderungen der Corona-Krise zu meistern. Ziel muss vielmehr die Entwicklung und Nutzung datenschutzgerechter Produkte sein. Digitale Lösungen müssen grundlegend neu gedacht und digitale Technik muss von Anfang an datenschutzgerecht gestaltet werden. Digitalisierung und Datenschutz sind keine Gegensätze, sondern müssen zusammen-

gebracht werden, um beides zum optimalen Nutzen der Menschen zukunftsfähig zu machen. Hierfür werden meine Behörde und ich uns weiterhin einsetzen.

Berlin, den 8. April 2021

Maja Smoltczyk
Berliner Beauftragte für Datenschutz und Informationsfreiheit

1 Schwerpunkte

1.1 Corona

1.1.1 Die Corona-Warn-App – Datenschutz durch Technikgestaltung

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit beteiligte sich an der Ausarbeitung eines Anforderungskatalogs für mobile Anwendungen zur Verfolgung der Kontakte von Personen, die an Covid-19 erkrankt sind.

Zur Bekämpfung der Corona-Pandemie wurde eine Reihe von technischen Lösungen vorgeschlagen. Diese sollten dazu dienen, Informationen über die Verbreitung der Pandemie zu sammeln, Personen festzustellen, die mit Erkrankten Kontakt hatten, oder die Diagnostik zu unterstützen. Im Rahmen unserer Zuständigkeit haben wir die Verantwortlichen bei diesen Projekten beraten, die oft unter hohem Zeitdruck entwickelt und in Anwendung gebracht wurden.

Eine zentrale Strategie bei der Begrenzung der Verbreitung des Corona-Virus besteht darin, infizierte Personen anhand ihrer persönlichen Kontakte zu finden und an der Weitergabe der Infektion zu hindern. Es liegt nahe, die Fähigkeiten von Smartphones hierfür einzusetzen, die mehr als 80 % der über Vierzehnjährigen bei sich tragen: Sie verfügen über eine Reihe von Sensoren, die zur Feststellung von Kontakten genutzt werden können.

Der erste Ansatz bestand darin, Daten über den Standort der Geräte zu nutzen, die viele der Geräte erfassen und oft auch an Dritte weitergeben. Ein Aufenthalt von zwei Personen mit Smartphones zum selben Zeitpunkt am selben Ort stellt einen Kontakt dar. Natürlich wäre es möglich, in einer großen Datenbank durch Nutzung dieser Daten die Aufenthaltsorte eines großen Anteils der Bevölkerung miteinander zu vergleichen, um mögliche Ansteckungsquellen festzustellen. Technisch wäre dies effizient durchführbar. Und in der Tat wurde in einigen ostasiatischen Ländern so verfahren. Doch aus dem Blickwinkel der Freiheitsrechte der Bür-

gerinnen und Bürger betrachtet, ist das keine gute Idee. Wer immer die Daten sammelt, erhält einen äußerst tiefgehenden Einblick in das Leben der Menschen, ihre Gewohnheiten und sozialen Kontakte, ihre Interessen und Laster. Letztlich ergibt sich hieraus eine immense Macht über die Betroffenen mit einem riesigen Missbrauchspotenzial. Hinzu kommt, dass bei diesem Verfahren die Ortsangaben oft nicht präzise genug sind, um wirklich ein epidemiologisch relevantes Zusammentreffen feststellen zu können.

Zum Glück wurde schnell klar, dass alternative Ansätze verfügbar sind, die diese Probleme vermeiden. Smartphones empfangen nicht nur Daten, sie versenden sie auch. Und das nicht nur per Mobilfunk oder Wi-Fi, sondern auch mit Funkverfahren kurzer Reichweite. Das gängigste dieser Verfahren, das von der überwiegenden Zahl der Smartphones unterstützt wird, heißt Bluetooth. Es dient z. B. dazu, kabellose Kopfhörer mit dem Smartphone zu verbinden, kann jedoch auch zum Übertragen von Nachrichten zwischen zwei Smartphones genutzt werden, die sich nah beieinander befinden.

So können alle Personen, die über den Kontakt mit Erkrankten informiert werden wollen, eine Kontaktadresse per Bluetooth versenden. Smartphones in der Nähe können diese Kontaktdaten sammeln. Werden ihre Besitzerinnen oder Besitzer als infiziert diagnostiziert, können sie ihre Kontaktpersonen anhand der Kontaktdaten informieren. Diese Daten müssen keine Telefonnummern, E-Mail-Adressen oder gar postalische Adressen sein. Ein für diesen Zweck eingerichteter Kontaktdienst, bei dem die Smartphones Nachrichten abholen können, genügt auch. Diesen Weg beschreitet z. B. das französische System.

Dieses Verfahren sieht zudem vor, dass der Kontaktdienst die Wahrscheinlichkeit einer Infektion aus dem oder den Kontakten errechnet. Dazu nutzt er die Angaben über Häufigkeit und Länge der Kontakte sowie den Abstand zwischen den Smartphones (und damit ihrer Besitzerinnen bzw. Besitzer) während des Kontakts. Dieser Abstand lässt sich aus der Stärke des Signals ableiten, mit dem die Smartphones die jeweiligen Signale empfangen haben.

Doch auch in diesem System fällt bei dem zentralen Kontaktdienst eine große Menge an Daten über die Kontakte der Menschen untereinander an. Zwar nicht über den Ort, an dem sie zusammengetroffen sind oder sich aufgehalten haben,

und damit viel weniger als beim Umgang mit Standortdaten. Aber es wird offengelegt, wer wen traf. Zudem können die Angaben im Zuge des Datenabrufs möglicherweise identifizierbaren Personen zugeordnet werden. Verhindern lässt sich diese Zuordnung nur, wenn die Abrufenden spezielle Vorsichtsmaßnahmen treffen. Nur wenige, besonders technikkundige Menschen sind dazu jedoch in der Lage.

Um dem zu begegnen, wurde eine weitere Idee entwickelt. Sie besteht darin, die Dokumentation der Kontakte zwischen den Menschen auf deren Smartphones zu verlagern. Jede Person, die an dem System teilnimmt, sendet an alle anderen, denen sie begegnet, per Bluetooth ein Pseudonym. Die Kontaktpersonen registrieren dieses. Erfährt die erste Person, dass sie infiziert ist, dann veröffentlicht sie ihr Pseudonym ohne Nennung des eigenen Namens. Wer dieses Pseudonym zu einem früheren Zeitpunkt registriert hatte, war in der Nähe der infizierten Person. Das Smartphone ruft daher regelmäßig die veröffentlichten Pseudonyme ab und vergleicht sie mit den bei sich registrierten Pseudonymen. Findet sich ein Treffer, wird die jeweilige Kontaktperson gewarnt. Auch einen Schätzwert für die Wahrscheinlichkeit einer Infektion durch den Kontakt kann das Smartphone berechnen und anzeigen. Dabei kann der gleiche Algorithmus zur Anwendung kommen, wie er im französischen System zentral ausgeführt wird.

Das Pseudonym wird dabei häufig gewechselt. Im Falle der Veröffentlichung einer Infektion werden dann alle Pseudonyme aus dem Zeitraum, in dem die betreffende Person infektiös war, erfasst. Das lässt sich datensparsam organisieren. Und es verhindert ohne Beeinträchtigung der Funktionalität der App, dass Menschen bei ihrer Bewegung im öffentlichen Raum anhand der Pseudonyme verfolgt werden können, die ihre Smartphones rundum versenden.

Dieser Ansatz wurde von unserer Behörde unterstützt. Er hat sich in Deutschland und mehreren anderen europäischen Ländern durchgesetzt.

Den datenschutzrechtlichen Rahmen für die Umsetzung hat der Europäische Datenschutzausschuss (EDSA)[1] in einer Veröffentlichung von Leitlinien mit Anforderungen an die „Verwendung von Standortdaten und Tools zur Kontaktnachverfol-

1 Siehe Art. 68 DS-GVO

gung im Zusammenhang mit dem Ausbruch von COVID-19“[2] umrissen. Ergänzt wurde diese Veröffentlichung durch eine „Erklärung über die Datenschutzfolgen der Interoperabilität von Kontaktnachverfolgungs-Apps“[3]. An der Erarbeitung der genannten Dokumente waren wir aktiv beteiligt. Angesichts der Dringlichkeit arbeitete der Ausschuss in Rekordzeit.

Der EDSA stellt zunächst fest, dass die Teilnahme an einer elektronischen Kontaktverfolgung freiwillig sein sollte. Er geht dabei davon aus, dass eine datenschutzfreundliche, vertrauenswürdige und transparente Umsetzung zur Akzeptanz des Verfahrens beiträgt. Für ein System, das bei hohen Teilnahmequoten deutlich an Wirksamkeit gewinnt, ist das ein wichtiger Faktor.

Im Einzelnen stellt der Ausschuss insbesondere Folgendes heraus:

- Die gesetzliche Vorgabe zur Minimierung der Datenverarbeitung und Beschränkung auf das Erforderliche ist einzuhalten.

- Angesichts bestehender Alternativen widerspricht eine Verarbeitung von Standortdaten für den Zweck der Kontaktverfolgung den Datenschutz-Grundsätzen.

- Das System soll nur mit geprüften Angaben über Infektionen arbeiten, um Betroffene nicht unnötig zu alarmieren.

- Die Entscheidung über die Freigabe der Information über die Infektion einer Person muss in deren Händen bleiben.

- In Hinweisen auf den Kontakt mit einer infizierten Person darf diese nicht benannt werden.

- Nicht mehr benötigte Daten sind unverzüglich zu löschen, sowohl auf zentralen Servern wie auf den Smartphones der Bürgerinnen und Bürger.

2 Siehe https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitlinien

3 Siehe https://edpb.europa.eu/our-work-tools/our-documents/muu/statement-data-protection-impact-interoperability-contact-tracing_de

In einem Anhang stellt der Ausschuss dann konkrete Prüfkriterien für die Umsetzung des Verfahrens zusammen. Diese betreffen die Einbettung in die allgemeine Durchführung der Kontaktverfolgung, die strikte Einschränkung der Nutzung der in dem Verfahren gesammelten Daten auf die Kontaktverfolgung, die Bereitstellung geeigneter Informationen über das Verfahren für die Nutzenden, die Sicherheit von Verfahren und eingesetzter Informationstechnik sowie eine Evaluierung der Wirksamkeit des Vorgehens.

Außen vor bleiben die Risiken, die bereits mit der dauerhaften Aktivierung von Bluetooth in den Smartphones der Nutzenden verbunden sind. Es gibt eine nicht unerhebliche Zahl von Smartphones, die mit veralteter Software betrieben werden, weil die Hersteller*innen sie nicht über eine ausreichende Zeitspanne hinweg mit Aktualisierungen versorgen. Darin schlummert eine Schwachstelle, die Smartphones mit aktiviertem Bluetooth angreifbar macht. Ebenso unglücklich ist, dass Google als Hersteller des Android-Betriebssystems die Aktivierung von Bluetooth an die Aktivierung des Standortdienstes knüpft und von der auf diesem Wege ermöglichten Sammlung von Standortdaten profitiert. Diesen Defiziten muss mit anderen Mitteln begegnet werden: der gesetzlichen Normierung der Herstellerpflicht, Sicherheitsupdates bereitzustellen, und einer Kontrolle der Datenverarbeitungen von Google durch die zuständige irische Datenschutz-Aufsichtsbehörde.

In der Abwägung aller Vor- und Nachteile einschließlich der genannten Risiken halten wir jedoch das in Deutschland praktizierte System der elektronischen Kontaktverfolgung mit der Corona-Warn-App für datenschutzgerecht und beispielhaft für andere digitale Projekte der öffentlichen Verwaltung.

Wenn Politik, Verantwortliche, Hersteller*innen und Aufsichtsbehörden in ihren jeweiligen Rollen konstruktiv zusammenwirken, können auch unter dem Druck einer bedeutenden Krise des Gesundheitssystems wie der Covid-19-Pandemie datenschutzfreundliche Lösungen gefunden werden, die eine Einbindung der Bevölkerung in eine effektive Eindämmung der Krise ermöglichen, tiefe Eingriffe in das Privatleben der Menschen jedoch vermeiden und den Schutz der verarbeiteten personenbezogenen Daten garantieren.

1.1.2 CovApp – Erfassung von Covid-Symptomen im Netz

Zusammen mit unseren Brandenburger Kolleginnen und Kollegen berieten wir die Charité bei dem Einsatz eines webbasierten Werkzeugs zur Erfassung von Daten über Personen, die sich einem Test auf eine Corona-Infektion unterziehen wollen.

Wie bei jeder medizinischen Leistung müssen auch bei einem Corona-Test grundlegende Informationen über den Gesundheitszustand der zu testenden Personen erhoben werden. Die Aufenthaltszeit im Testzentrum soll dabei so kurz wie möglich gehalten werden. Daher bietet es sich an, den Fragebogen schon vorab zur Verfügung zu stellen. Geschieht das in elektronischer Form, ist die Datenübernahme besonders einfach. Diesen Weg beschritt die Charité, unterstützt durch ein Brandenburger Unternehmen, das digitale Gesundheitslösungen entwickelt.

Aus Brandenburg auf das Projekt CovApp aufmerksam gemacht, haben wir uns die technische Umsetzung angesehen und auf festgestellte Defizite hingewiesen. Da das Projekt im Laufe des Jahres ausgebaut wurde, um neue Funktionalitäten anzubieten, war es notwendig, die Überprüfung nach einiger Zeit zu wiederholen.

Der Aufbau des elektronischen Fragebogens war dabei grundsätzlich nicht zu beanstanden. Die Charité stellt ihn als Webanwendung (Web-App) im Rahmen ihres allgemeinen Webangebots zur Verfügung. Einmal geladen, kommuniziert die Webanwendung zunächst nicht weiter mit den Servern der Charité, sondern speichert die in mehreren Schritten durch eine Befragung der Patientin oder des Patienten erhobenen Daten im Webbrowser. Am Ende werden die Daten mit einem einfachen Algorithmus ausgewertet und es wird eine Empfehlung zum weiteren Vorgehen – Wahrnehmen des Tests oder Verzicht darauf – ausgesprochen. Kommt es zu einem Test, können die Daten von der Charité durch Auslesen der Anzeige des Webbrowsers übernommen werden.

Probleme gab es lediglich im Detail. Der Hersteller der Web-App wollte gern die Nutzung (nicht die Eingaben der Nutzenden) nachverfolgen – auch das ist jedoch

lediglich mit Einwilligung erlaubt. Die Einholung der Einwilligung wurde nachgetragen. Darüber hinaus funktionierte die Löschung der Daten nach absolvierter Befragung nicht zuverlässig. Dies ist deswegen heikel, da die Gefahr besteht, dass andere Web-Angebote, die die Patient*innen besuchen, die Daten auslesen. Die Funktion wurde zwar repariert, allerdings muss die Löschung verfahrensbedingt nach wie vor durch die Nutzenden aktiv angestoßen werden.

Schließlich wollte die Charité die Patientinnen und Patienten bitten, ihre Angaben auch für die Forschung freizugeben. Doch die Informationen, die für eine wirksame Einwilligung notwendig sind, waren nicht ausreichend und ließen sowohl die Rollen der Beteiligten als auch die Zwecke der Forschung im Unklaren. Diese Möglichkeit einer „Datenspende" wurde im weiteren Verlauf des Jahres aus dem Programm entfernt und durch eine Übernahme der Daten in Symptomtagebuch-Apps auf freiwilliger Basis ersetzt. Mindestens eine davon sah ihrerseits eine Weitergabe der Daten für Forschungszwecke vor.[4]

In der Summe konnten wir feststellen, dass die Charité mit der CovApp eine praktikable Lösung bereitstellt, die den Datenschutzanforderungen genügt.

Die elektronische Befragung von Patientinnen und Patienten kann sicher und datensparsam ausgestaltet werden. Transparenz und technische Sorgfalt sind dabei von grundlegender Bedeutung.

1.1.3 Umgang mit Kontaktlisten zur Eindämmung der Corona-Pandemie

Uns erreichte eine Vielzahl an Beschwerden zu Restaurants, Cafés, Bars und anderen Lokalitäten, bei denen sich die Gäste in offen zugängliche Listen eintragen

4 Wir haben keine Hinweise darauf, dass die Weitergabe von Anamnesedaten an Forschungseinrichtungen für Zwecke der medizinischen Forschung hierbei unrechtmäßig erfolgte. Es wurden jeweils Einwilligungen eingeholt, deren Formulierung sich derzeit jedoch nicht mehr nachvollziehen lässt, da die Studien mittlerweile beendet wurden und keine Datenerhebung mehr erfolgt. Diese Datenverarbeitung fand im Übrigen außerhalb unseres Zuständigkeitsbereichs statt, da die Betreiber der Symptomtagebücher ihren Sitz in Lübeck bzw. Freiburg haben.

sollten. Nur in einem Fall stand dabei zusätzlich eine zweckwidrige Nutzung der so erhobenen Daten im Raum.

Zu einem zentralen Bestandteil der Eindämmung des Corona-Virus ist die Nachverfolgung von Infektionsketten geworden. Damit Gesundheitsämter Infektionsketten effektiv nachverfolgen können, sahen die Infektionsschutzverordnungen der Bundesländer im Berichtszeitraum Regelungen zur Erhebung von Kontaktdaten vor. Die Pflicht zur Anwesenheitsdokumentation traf in Berlin u.a. Hotels und gastronomische Einrichtungen.[5]

Die Dokumentation musste neben dem Vor- und Familiennamen die Telefonnummer sowie den Bezirk oder die Gemeinde des Wohnortes oder des Ortes des ständigen Aufenthaltes enthalten.[6] Darüber hinaus waren entweder die vollständige Anschrift oder die E-Mail-Adresse des Gastes, die Anwesenheitszeit sowie – soweit vorhanden – eine Platz- oder Tischnummer zu dokumentieren und für die Dauer von vier Wochen nach Ende der Veranstaltung oder Inanspruchnahme der Dienstleistung aufzubewahren.[7] Weil die Erfassung der korrekten Daten von entscheidender Bedeutung für eine Kontaktnachverfolgung durch die Gesundheitsämter ist, ist die Angabe falscher Daten zwischenzeitlich auch bußgeldbewehrt.[8]

In der datenschutzrechtlichen Praxis zeichneten sich schnell Probleme bei der Umsetzung der Kontaktdatenerfassung ab. Uns erreichten zahlreiche Beschwerden von Bürgerinnen und Bürgern, die über offen ausliegende Sammellisten in Restaurants und über die Erfassung der Daten von mehreren Personen auf einem einzigen Kontaktdatenformular berichteten. So bestand z. B. neben der Kenntnisnahme der Daten durch anwesende Gäste auch die Gefahr, dass diese Listen abfotografiert werden.

5 Mit Inkrafttreten der SARS-CoV-2-Infektionsschutzmaßnahmenverordnung (InfSchMV) vom 14. Dezember 2020, die die bis dahin geltende SARS-CoV-2-Infektionsschutzverordnung ersetzte, war die Erhebung von Kontaktdaten aufgrund der Pflicht zur Schließung vieler Einrichtungen nur noch sehr eingeschränkt möglich; siehe insbesondere §§ 15, 16 InfSchMV.

6 § 3 Abs. 2 Satz 1 SARS-CoV2-Infektionsschutzverordnung (vom 3. November 2020)

7 § 3 Abs. 2 Satz 2 SARS-CoV2-Infektionsschutzverordnung (vom 3. November 2020)

8 § 3 Abs. 3 SARS-CoV2-Infektionsschutzverordnung (vom 3. November 2020)

Eine Erfassung der Daten mittels ausliegender Papierlisten, die offen einsehbar sind, steht nicht im Einklang mit datenschutzrechtlichen Vorgaben. Die nach den infektionsschutzrechtlichen Regelungen geforderte Dokumentation von Kontaktdaten muss vor der Einsichtnahme Dritter geschützt aufbewahrt oder gespeichert werden.[9] Durch geeignete technisch-organisatorische Maßnahmen müssen Restaurants, Cafés, Hotels oder anderen Lokalitäten gewährleisten, dass eine Kenntnisnahme personenbezogener Daten durch unberechtigte Personen ausgeschlossen ist. Die Daten müssen daher ab Beginn des Führens einer Anwesenheitsdokumentation für jede Person auf einem gesonderten Blatt erfasst und sicher aufbewahrt werden.

Die von uns geprüften Restaurants, Cafés und Bars wurden auf den datenschutzkonformen Umgang mit den Kontaktdatenlisten hingewiesen und aufgrund der Offenlegung von personenbezogenen Daten an unberechtigte Dritte teilweise verwarnt. Nur in einem Fall stand eine zweckwidrige Nutzung der Kontaktdaten u.a. für einen Newsletter des Restaurants im Raum. Diesen Fall haben wir an unsere Sanktionsstelle abgegeben.

Im Rahmen der Bearbeitung der einzelnen Beschwerden wurde uns insbesondere mitgeteilt, dass die in einigen Restaurants verwendeten Kontaktdatenlisten auf einer Muster-Vorlage des Hotel- und Gaststättenverbandes (DEHOGA) beruhten. Eine Rückfrage beim DEHOGA hat ergeben, dass das Musterformular nicht als Sammelliste konzipiert war, sondern auf die Erfassung von sechs Personen abzielte, die sich an einem Tisch befanden. Aufgrund des Umstands, dass die Vorlage missverstanden werden konnte und die Infektionsschutzverordnungen der Länder unterschiedlich ausgestaltet waren, hat der DEHOGA die Mustervorlage im Mai wieder von ihrer Webseite genommen und die einzelnen Landesverbände darüber informiert.

Auf unserer Webseite haben wir selbst ein Musterformular zur Kontaktnachverfolgung durch Betriebe veröffentlicht, das wir entsprechend der aktuellen Infektionsschutzbestimmungen laufend aktualisieren.[10]

9 § 3 Abs. 2 Satz 2 SARS-CoV2-Infektionsschutzverordnung (vom 3. November 2020); siehe auch Art. 5 Abs. 1 lit. f DS-GVO

10 Siehe https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/corona-pandemie

Durch Verordnungen zum Schutz vor Infektionen mit dem Coronavirus SARS-CoV-2 vorgeschriebene Anwesenheitsdokumentationen müssen geschützt vor der Einsichtnahme Dritter aufbewahrt oder gespeichert werden. Kontaktdatenformulare, die eine Erfassung mehrerer Personen vorsehen oder gar offen ausliegen, sind unzulässig.

1.1.4 Nur fieberfrei in den Supermarkt?

Im Zusammenhang mit der Covid-19-Pandemie erreichten uns mehrere Anfragen von Unternehmen, die elektronische Fiebermessungen als Einlasskontrolle in Supermärkten vornehmen wollten. Es war geplant, Personen mit erhöhter Körpertemperatur den Zugang zu Einzelhandelsgeschäften zu verwehren.

Wir halten dies nicht für sinnvoll. Eine erhöhte Körpertemperatur kann nicht zwangsläufig als Indiz für eine SARS-CoV-2-Infektion angesehen werden. Viele Infizierte weisen keine Symptome und damit auch keine erhöhte Temperatur auf. Umgekehrt weist eine erhöhte Temperatur auch nicht zwangsläufig auf eine SARS-CoV-2-Infektion hin. Zudem sind mildere Maßnahmen, wie z. B. die Einhaltung der Lüftungsroutine und der Hygiene- und Abstandsbestimmungen, zur Eindämmung der Pandemie effektiver. Dies gilt insbesondere auch für die im Einzelhandel bereits üblichen Maßnahmen, wie etwa die Begrenzung der Anzahl an Kund*innen, das Anbringen von Hinweisschildern zu Verhaltensregeln und Zutrittsbeschränkungen, die Gewährleistung der Einhaltung von Mindestabständen, die Aufforderung zum Tragen eines Mund-Nasen-Schutzes, die Anbringung von Trennwänden im Kassenbereich und an Verkaufstresen sowie die Implementierung von Hygienevorgaben. Ein derartiges Maßnahmenpaket verspricht gerade auch im Hinblick auf eine potenzielle Ansteckung durch symptomfreie und nicht als infiziert erkannte Personen einen nachhaltigeren Schutz von Kund*innen und Beschäftigten als eine elektronische Erhebung von Gesundheitsdaten, die ihrerseits gesetzlich besonders geschützt sind.[11]

Rechtlich gesehen ist eine elektronische Temperaturmessung, die darauf gerichtet ist, Personen zu identifizieren, die mit SARS-CoV-2 infiziert sind, nur mit

11 Siehe Art. 4 Nr. 15 i. V. m. Art. 9 DS-GVO

Einwilligung oder auf der Grundlage einer gesetzlichen Regelung zulässig.[12] Die Einholung entsprechender Einwilligungen von allen Kund*innen dürfte nicht praktikabel oder sogar kontraproduktiv sein, falls es bei dem Prozedere der Einwilligungserklärung und der Fiebermessung zu längeren Warteschlangen käme. Gesetzliche Regelungen, auf die eine entsprechende Fiebermessung im Einzelhandel gestützt werden könnte, existieren bislang nicht. Allerdings enthält die Datenschutz-Grundverordnung (DS-GVO) Spielräume für die nationale Gesetzgebung, die Erhebung von Gesundheitsdaten in bestimmten Bereichen zu regeln.[13] Vor dem o. g. Hintergrund halten wir eine entsprechende Regelung jedoch zumindest zum jetzigen Zeitpunkt nicht für sinnvoll.

Gemeinsam mit den Datenschutz-Aufsichtsbehörden des Bundes und der anderen Länder haben wir zum Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie Hinweise erarbeitet, die auf unserer Internetseite abgerufen werden können.[14] Dort finden sich auch weitere wichtige Informationen zum Einsatz von Wärmebildkameras in anderen Bereichen, wie z. B. in Flughäfen, Behörden und Arbeitsstätten.

1.1.5 Umgang mit der Maskenpflicht in Schulen

Mit der Einführung der Pflicht zum Tragen einer Mund-Nasen-Bedeckung in den Schulen haben sich neue datenschutzrechtliche Fragen im Zusammenhang mit der Corona-Pandemie ergeben. So erreichte uns nach der Einführung der Maskenpflicht in Schulen eine Vielzahl von Anfragen besorgter Eltern. Sie wollten ihr Kind von der Maskenpflicht befreien lassen und fragten nach, inwieweit die Schule die Vorlage eines ärztlichen Attests verlangen dürfe und welche Angaben darin enthalten sein dürften.

Die Verpflichtung zum Tragen einer Mund-Nasen-Bedeckung ergibt sich aus der in Berlin geltenden SARS-CoV-2-Infektionsschutzmaßnahmenverordnung in der

12 Siehe Art. 6 Abs. 1 Satz 1 i. V. m. Art. 9 Abs. 1, 2 DS-GVO

13 Siehe nur Art. 6 Abs. 1 Satz 1 lit. c, Abs. 2, 3 i. V. m. Art. 9 Abs. 2 lit. g–j DS-GVO

14 Siehe https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

jeweils geltenden Fassung.[15] Eine Ausnahme von der in Schulen geltenden Pflicht zum Tragen einer Mund-Nasen-Bedeckung gilt für Personen, die aufgrund einer ärztlich bescheinigten gesundheitlichen Beeinträchtigung, einer ärztlich bescheinigten chronischen Erkrankung oder einer Behinderung keine Mund-Nasen-Bedeckung tragen können.[16] Bei einem ärztlichen Attest und den darin enthaltenen Informationen handelt es sich um sensitive Gesundheitsdaten, die zu den Kategorien personenbezogener Daten mit einem besonderen Schutz gehören. Ihre Verarbeitung ist nur erlaubt, wenn die betroffene Person entweder (freiwillig, informiert und ausdrücklich) einwilligt oder wenn die Verarbeitung aufgrund einer gesetzlichen Regelung zulässig ist.[17] Die DS-GVO als unmittelbar in den EU-Mitgliedsstaaten geltendes Recht lässt eine Verarbeitung zu, wenn diese aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie z. B. dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, auf der Grundlage einer bestimmten Anforderungen genügenden gesetzlichen Regelung erforderlich ist.[18] Für Schulen ist die Befugnis, sich zur Glaubhaftmachung eines Befreiungsgrunds ein Attest vorlegen zu lassen, insbesondere in der SARS-CoV-2-Infektionsschutzmaßnahmenverordnung i. V. m. dem Schulgesetz (SchulG) geregelt.

Die Frage, ob ein ärztliches Attest konkrete gesundheitliche Informationen beinhalten muss, richtet sich danach, ob dies zur Erreichung des Zwecks erforderlich ist. Zweck der Maskenpflicht in Schulen ist es, die Ansteckung von Schüler*innen und Lehrkräften (und dadurch auch die weitere Verbreitung der Infektion in der Bevölkerung) unter den besonderen Bedingungen einer Gemeinschaftseinrichtung zu verhindern. Die Schulleitung ist dafür zuständig, über eine individuelle Befreiung von der Maskenpflicht zu entscheiden. Ihr muss der Grund für die Befreiung mithilfe des ärztlichen Attests glaubhaft gemacht werden. Da es sich

15 Seit dem 14. Dezember 2020 heißt die Verordnung nebst Änderungsfassungen nicht mehr SARS-CoV-2-Infektionsschutzverordnung, sondern SARS-CoV-2-Infektionsschutz**maßnahmen**verordnung.

16 § 4 Abs. 3 Nr. 2 SARS-CoV-2-Infektionsschutzmaßnahmenverordnung (in der Fassung vom 14. Dezember 2020). Während die Anforderung eines ärztlichen Attests sich vorher u.a. aus dem Sinn und Zweck der Verordnung, einen effektiven Infektionsschutz zu gewährleisten, ergab, ist diese seit der 10. Fassung der SARS-CoV-2-Infektionsschutzverordnung ausdrücklich geregelt.

17 Art. 4 Nr. 15 DS-GVO; Art. 6 Abs. 1 DS-GVO; Art. 9 Abs. 1, 2 DS-GVO

18 Art. 9 Abs. 2 lit. i) DS-GVO

bei der Befreiung um eine Ausnahmeregelung handelt, reicht die Feststellung allgemeiner Beeinträchtigungen, die bei allen Schüler*innen auftreten können, nicht aus. Vielmehr muss in dem Attest eine darüber hinausgehende individuelle Beeinträchtigung der betroffenen Person dargelegt werden. Dafür ist es in der Regel erforderlich, dass konkrete Angaben zu Vorerkrankungen oder aktuellen Besonderheiten gemacht werden und erläutert wird, zu welchen Nachteilen die individuelle Beeinträchtigung durch das Tragen einer Maske in möglichen relevanten Fallgestaltungen in der Schule führen kann. Nur so kann die Schulleitung als verantwortliche Stelle eine sachgerechte Entscheidung über die Befreiung von der Maskenpflicht treffen.

Die Situation ist dabei eine andere als etwa bei einer Krankschreibung, in der die Diagnose nicht aufgeführt ist. Denn bei der Befreiung von der Maskenpflicht sind auch die Grundrechtspositionen der anderen Schüler*innen und des Schulpersonals, wie das Recht auf Leben und körperliche Unversehrtheit, betroffen. Die Schutzpflicht des Staates gilt im Schulkontext in besonderer Weise, da Schüler*innen aufgrund der allgemeinen Schulpflicht keine Wahl haben, sich in Schulklassen (mit oder ohne ausreichenden Mindestabstand) aufzuhalten oder nicht.

Nach der Entscheidung der Schulleitung ist es im Regelfall nicht erforderlich und damit auch nicht zulässig, dass die Schule eine Kopie des Attestes aufbewahrt. Die Schulleitung sollte vielmehr die erfolgte Glaubhaftmachung in einem separaten Dokument bestätigen, ohne dass dieser Vermerk gesundheitliche Angaben enthält. Lehrkräfte dürfen für die laufende Kontrolle im Schulbetrieb lediglich die Information erhalten, dass ein Befreiungsgrund glaubhaft gemacht wurde.

Schulen sind berechtigt, sich zur Glaubhaftmachung eines Befreiungsgrundes ein ärztliches Attest vorlegen zu lassen, das auf die konkrete gesundheitliche Situation der betroffenen Person eingeht. Eine Aufbewahrung einer Kopie des Attestes ist dagegen nicht erforderlich und damit nicht zulässig.

1.1.6 „Bitte Mund und Nase bedecken“ – Kontrollbefugnisse der Verkehrsunternehmen

Zur Eindämmung der Corona-Pandemie wurden in den vergangenen Monaten verschiedene Maßnahmen durch die Verordnungsgeber der einzelnen Bundesländer beschlossen. Seit April besteht u.a. eine Pflicht zum Tragen einer Mund-Nasen-Bedeckung in Berliner U-Bahnen, Straßenbahnen und Bussen sowie in der S-Bahn. Nicht selten konnte man Menschen ohne eine solche Mund-Nasen-Bedeckung im öffentlichen Personennahverkehr (ÖPNV) antreffen. Da für bestimmte Gruppen im Falle gesundheitlicher Beeinträchtigungen Ausnahmen von der Maskenpflicht bestehen, ist dies ggf. durch entsprechende Bescheinigungen nachzuweisen. Eine besondere Herausforderung besteht darin, die Maskenpflicht i. S. d. Infektionsschutzes durchzusetzen und gleichzeitig beim Nachweis eines Ausnahmetatbestandes die personenbezogenen Daten zu schützen.

Die SARS-CoV-2-Infektionsschutzmaßnahmenverordnung sieht das Tragen einer Mund-Nasen-Bedeckung insbesondere in öffentlichen Verkehrsmitteln nebst Bahnhöfen, Flughäfen und Fährterminals und in sonstigen Fahrzeugen, in denen sich wechselnde Fahrgäste aufhalten, vor.[19] Eine Ausnahme gilt u.a. für Personen, die aufgrund gesundheitlicher Beeinträchtigungen, chronischer Erkrankungen oder einer Behinderung keine Maske tragen können.[20] Bei Personen, die sich auf diese Ausnahme berufen, haben die jeweiligen Verantwortlichen in ihren Räumen das Recht bzw. die Pflicht, sich ein ärztliches Attest vorlegen zu lassen.[21]

In den öffentlichen Verkehrsmitteln kommt darüber hinaus das Hausrecht des jeweiligen Verkehrsbetriebs zum Tragen. So ist es im Falle der Nutzungsordnung der Berliner Verkehrsbetriebe nicht gestattet, sich ohne Mund-Nasen-Bedeckung in den Verkehrsmitteln aufzuhalten, es sei denn, diese Pflicht entfällt aufgrund

19 § 4 Abs. 1 Nr. 1 SARS-CoV-2-Infektionsschutzmaßnahmenverordnung (in der Fassung vom 22. Dezember 2020)

20 § 4 Abs. 3 SARS-CoV-2-Infektionsschutzmaßnahmenverordnung (in der Fassung vom 22. Dezember 2020)

21 Siehe Art. 6 Abs. 1 Satz 1 lit. e, Art. 9 Abs. 2 lit. i DS-GVO i. V. m. § 4 SARS-CoV-2-Infektionsschutzmaßnahmenverordnung (in der Fassung vom 22. Dezember 2020)

der Ausnahmen, welche die jeweils geltende SARS-CoV-2-Verordnung vorsieht.[22] Bei Verstößen gegen die Maskenpflicht in den Verkehrsmitteln sieht die Nutzungsordnung eine Vertragsstrafe in Höhe von 50,00 Euro vor. Zudem weist die Nutzungsordnung auf das Hausrecht hin, wonach bei Verstößen Hausverweise, Haus- bzw. Betretungsverbote und Beförderungsausschlüsse ausgesprochen werden können.

In der SARS-CoV-2-Infektionsschutzmaßnahmenverordnung ist zwar nicht ausdrücklich vorgeschrieben, dass die Tatsachen, die zu einer Ausnahmeregelung von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung führen, glaubhaft gemacht werden müssen. Die Anforderung eines Nachweises ergibt sich jedoch sowohl aus dem Sinn und Zweck der SARS-CoV-2-Infektionsschutzmaßnahmenverordnung, einen effektiven Infektionsschutz zu gewährleisten, als auch aus dem rechtlichen Grundsatz, dass diejenigen, die sich auf eine Ausnahme berufen, das Vorliegen einer solchen Ausnahme nachweisen müssen. Dem jeweiligen Verantwortlichen muss es hierfür ermöglicht werden, die Echtheit eines entsprechenden Attestes zu prüfen und es der vorzeigenden Person zuordnen zu können. Hingegen ist für die Erfüllung der Prüfpflicht die Kenntnis der ärztlichen Diagnose, die der Befreiung von der Maskenpflicht zugrunde liegt, nicht erforderlich.

Bürgerinnen und Bürger, die aufgrund einer gesundheitlichen Beeinträchtigung vom Tragen einer Mund-Nasen-Bedeckung befreit sind, können daher die der Befreiung zugrunde liegende Diagnose in der ärztlichen Bescheinigung schwärzen, wenn diese der Vorlage im öffentlichen Personennahverkehr dient.

22 § 3 der Nutzungsordnung der Berliner Verkehrsbetriebe

1.2 Internationaler Datenverkehr nach der „Schrems II"-Entscheidung des Europäischen Gerichtshofs

Mit seinem Urteil vom 16. Juli 2020[23] hat der Europäische Gerichtshof (EuGH) mit dem „Privacy Shield" zum zweiten Mal Sonderregelungen für die Übermittlung personenbezogener Daten in die USA für ungültig erklärt. Die von der EU-Kommission erlassenen Standardvertragsklauseln für Datenexporte in Drittländer bleiben zwar weiterhin gültig, können allerdings für sich allein Datenexporte nicht mehr rechtfertigen. Dadurch ist bspw. die Nutzung von US-amerikanischen Cloud-Diensten durch Unternehmen und Behörden nur noch in besonderen Ausnahmefällen zulässig.

Die Beschwerde des Österreichers Maximilian Schrems gegen die Übermittlung seiner Daten durch Facebook in die USA war damit zum zweiten Mal Gegenstand einer Grundsatz-Entscheidung des EuGH. Das nunmehr für ungültig erklärte „Privacy Shield"-Abkommen war entwickelt worden in Nachfolge des 2015 ebenfalls auf eine Beschwerde von Herrn Schrems hin für ungültig erklärten[24] „Safe Harbor"-Abkommens.

Der „EU-U.S. Privacy Shield" sah – ähnlich den „Safe Harbor"-Regelungen – vor, dass sich US-Unternehmen in die sog. „Privacy Shield"-Liste eintragen und damit zur Einhaltung bestimmter Regelungen zum Datenschutz verpflichten können. Die US-Regierung machte zudem einige Zusagen zum Datenschutz bei behördlichen Zugriffen auf personenbezogene Daten. Durch einen Angemessenheitsbeschluss der EU-Kommission war der „Privacy Shield" daher als Grundlage zur Rechtfertigung von Übermittlungen personenbezogener Daten an US-Unternehmen anerkannt worden.[25]

23 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II"

24 EuGH, Urteil vom 6. Oktober 2015 – C-362/14, „Schrems I"; siehe hierzu JB 2015, 14.1

25 Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (bekannt gegeben unter Aktenzeichen C(2016) 4176); siehe hierzu JB 2016, 1.1

In seinem Urteil „Schrems II" analysierte der EuGH nunmehr im Detail die Rechtslage in den USA und stellte mit verschiedenen, jeweils für sich genommen bereits ausreichenden Begründungen fest, dass das Datenschutzniveau in den USA nicht den Anforderungen für einen zulässigen Datenexport entspricht.[26] Denn das dortige Recht gibt den US-Behörden unbeschränkte Überwachungsbefugnisse, den betroffenen Personen hingegen keinerlei Garantien für ihre Rechte.[27] Die Überwachungsbefugnisse der US-Behörden verstoßen daher gegen den Verhältnismäßigkeitsgrundsatz.[28] Zudem haben betroffene Personen keinerlei gerichtliche Rechtsschutzmöglichkeiten gegenüber US-Behörden.[29]

Die von der EU-Kommission verfassten Standardvertragsklauseln können demgegenüber grundsätzlich weiter zur Rechtfertigung von Datenexporten herangezogen werden. Allerdings werden dadurch nur auf zivilrechtlicher Ebene die für einen Datenexport erforderlichen Garantien geschaffen, denn ein Vertrag zwischen Datenexporteur und Datenimporteur kann die Behörden des jeweiligen Drittstaats nicht binden. Wer die Standardvertragsklauseln weiter einsetzen möchte, muss deshalb künftig die Rechtsordnung und Praxis des Drittlandes hinsichtlich eines etwaigen Zugriffs der Behörden dieses Landes auf die übermittelten personenbezogenen Daten prüfen.[30] Nur wenn für die exportierten Daten auch hinsichtlich möglicher Behördenzugriffe das gebotene Schutzniveau gegeben ist, sorgen die Standardvertragsklauseln für den erforderlichen Datenschutz. Wenn dies – wie im Fall der USA – nicht der Fall ist, müssen die Garantien in den Standardvertragsklauseln durch zusätzliche Maßnahmen ergänzt werden.[31]

Lassen sich keine ergänzenden Maßnahmen finden, die die Datenschutz-Mängel im Drittland beseitigen, müssen Datenexporte unterbleiben und bereits exportierte Daten zurückgeholt werden.[32] Eine Verpflichtung zur Aussetzung oder Beendigung des Datenexports besteht insbesondere dann, wenn das Recht des jeweiligen Drittlands dem Datenimporteur Verpflichtungen z. B. hinsichtlich des

26 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 185, 191, 197 ff.
27 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 180, 183
28 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 184
29 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 181, 182, 192
30 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 104
31 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 132 f.
32 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 135, 140

Zugangsrechts der Behörden dieses Drittlands zu den Daten auferlegt, die den Standardvertragsklauseln widersprechen und die daher geeignet sind, die vertraglich vereinbarte Garantie eines angemessenen Schutzniveaus zu untergraben.[33]

Wir haben die Konsequenzen des EuGH-Urteils „Schrems II" umgehend analysiert und die datenverarbeitenden Stellen in Berlin bereits am Tag nach Urteilsverkündung aufgefordert, in den USA gespeicherte personenbezogene Daten nach Europa zu verlagern, soweit nicht die Datenverarbeitung in den USA ausnahmsweise zulässig ist, insbesondere in den gesetzlich vorgesehenen Sonderfällen.[34]

Die europäischen Datenschutzaufsichtsbehörden haben – unter unserer maßgeblichen Beteiligung – Empfehlungen erarbeitet, wie Verantwortliche und Auftragsverarbeiter*innen, die personenbezogene Daten in Drittländer übermitteln wollen, vorgehen sollten.[35] Diese Empfehlungen enthalten neben einer Schritt-für-Schritt-Anleitung auch denkbare ergänzende Maßnahmen, um Defizite des Datenschutzniveaus im Zielland des Datenexports u. U. auszugleichen.

Das aufgrund der Rechtsprechung des EuGH erforderliche Vorgehen zur Prüfung von Datenexporten in Drittländer, für die kein Beschluss der EU-Kommission über die Angemessenheit des Datenschutzniveaus existiert,[36] ist sehr aufwendig. Datenexporteure müssen – ggf. in Zusammenarbeit mit den Datenimporteuren – beurteilen, ob es irgendetwas in der Gesetzgebung oder Praxis des Drittlands gibt, das die Wirksamkeit der vereinbarten Garantien beeinträchtigen könnte. Ist dies der Fall, etwa weil Behörden des Drittlands unverhältnismäßige Zugriffsrechte auf die verarbeiteten Daten haben, müssen ergänzende Maßnahmen ergriffen

33 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 135, 140

34 Pressemitteilung von 17. Juli 2020, siehe https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf

35 EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data; abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

36 Die EU-Kommission veröffentlicht eine Liste der Angemessenheitsbeschlüsse unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de

werden. Für die Beantwortung der Frage, welche Zugriffsrechte unverhältnismäßig sind, ist auf die europäischen Grundrechte abzustellen.[37]

Wenn z. B. wie im Fall der USA bei Anbietern von elektronischen Cloud- und Kommunikationsdiensten unverhältnismäßige Zugriffsrechte der Behörden des Drittlands auf die zu exportierenden Daten bestehen, können die ergänzenden Maßnahmen nur technischer Art sein.[38] Diese Maßnahmen müssen verhindern, dass die Behörden des Drittlands überhaupt Zugriff auf die Daten erhalten können, oder zumindest, dass sie mit diesen Daten etwas anfangen können.[39] Zu beachten ist, dass auch andere Empfänger*innen, die selbst keine Anbieter von elektronischen Kommunikationsdiensten im Sinne des US-Rechts sind, indirekt solch unverhältnismäßigen Zugriffsrechten unterliegen können, nämlich wenn sie die an sie übermittelten Daten durch einen Anbieter elektronischer Kommunikationsdienste verarbeiten lassen.

Im Fall der USA – und anderer Drittländer mit unverhältnismäßigen behördlichen Zugriffsrechten – bedeutet dies, dass etwa die Nutzung dortiger IT-Dienstleister wie Cloud-Provider nur noch in sehr wenigen Fällen zulässig ist. Aber auch andere Empfänger*innen können problematisch sein – nicht nur, wenn sie selbst Behördenzugriffen unterliegen, sondern weil viele Unternehmen Cloud-Dienste einsetzen und so indirekt der Überwachung unterliegen.

Die Nutzung von US-Cloud-Diensten zur Speicherung personenbezogener Daten kann z. B. dann in Betracht kommen, wenn diese Daten so verschlüsselt sind, dass über die gesamte Zeitdauer, über die sie vertraulich bleiben müssen, eine

37 Insbesondere Art. 47 und 52 der EU-Grundrechtecharta; siehe hierzu auch EDSA, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures; abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

38 EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Kapitel 2.3, Rn. 44; Kapitel 2.4, Rn. 48; abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

39 EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Kapitel 2.3, Rn. 44; abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

Entschlüsselung durch US-Behörden sicher ausgeschlossen werden kann.[40] Dies setzt neben diversen komplexen technischen Anforderungen u.a. voraus, dass der zur Entschlüsselung erforderliche Schlüssel niemals den Bereich verlassen darf, in dem ein angemessenes Datenschutzniveau herrscht. Denn ist der US-Cloud-Anbieter im Besitz des Schlüssels, können die dortigen Behörden nicht nur die Herausgabe der verschlüsselten Daten verlangen, sondern auch die Herausgabe des Schlüssels. Unter strikten Bedingungen können ausnahmsweise auch unverschlüsselte pseudonymisierte Daten exportiert werden, etwa zu Forschungszwecken.[41] Die Pseudonymisierung muss dabei so ausgestaltet werden, dass sie in den USA nicht aufgehoben werden kann, auch nicht durch Verknüpfung mit anderen Informationen.

Allerdings ist zu berücksichtigen, dass bei den typischen Anwendungsfällen von Dienstleistungen, die US-Unternehmen anbieten, regelmäßig der Zugriff auf Klardaten erforderlich ist. In solchen Fällen sind keine ausreichenden ergänzenden Maßnahmen denkbar.[42] Insbesondere genügen andere Maßnahmen wie etwa eine vertragliche Verpflichtung des Datenimporteurs, gegen Herausgabeanordnungen zu klagen, nicht. Datenexporte sind in solchen Fällen unzulässig, bereits exportierte Daten müssen sofort zurückgeholt werden.[43]

40 Im Detail zu den Anforderungen: EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Anhang 2, Use Case 1, Rn. 79; abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

41 Im Detail zu den Anforderungen: EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Anhang 2, Use Case 2, Rn. 80; abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

42 Im Detail zu den Anforderungen EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Anhang 2, Use Case 6, Rn. 88; abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

43 EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Kapitel 2.4, Rn. 52; abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

Dies betrifft im Fall der USA z. B.

- Kommunikationsdienste wie E-Mail, Videokonferenzen, Messenger, Web- und Shop-Hosting, Einbindung von Dritt-Inhalten auf der eigenen Webseite, in der Regel auch die Abwehr von (dDoS-)Angriffen,

- Dienste zur Verwaltung von Beziehungen zu Kund*innen (Customer Relations Management), zur Personalverwaltung, zum Projektmanagement oder zum Management von Anfragen (Ticket-Systeme),

- Dienste zur verteilten Zusammenarbeit, etwa zur gemeinsamen Bearbeitung von Textdokumenten, Präsentationen, Tabellen,

- Dienste zur Synchronisation von Daten zwischen verschiedenen Geräten, Datei-Speicherung, Kalender- und Aufgabenverwaltungs-Dienste,

- Verzeichnis- und andere Dienste, die zur Authentifizierung von Personen genutzt werden und Daten über diese enthalten,

- Dienstleister, die die Überprüfung von Ausweisen, Führerscheinen und anderen Dokumenten übernehmen.

Die von der EU-Kommission als Entwurf bereitgestellten neuen Standardvertragsklauseln[44] – an deren Kommentierung und Verbesserung wir uns zusammen mit anderen europäischen Aufsichtsbehörden beteiligt haben – ändern an dieser Problematik nichts und können dies auch nicht, da vertragliche Regelungen, an denen die ausländischen Behörden nicht beteiligt sind, diese nicht binden können.

Wie sich das Urteil „Schrems II" auf andere Rechtsgrundlagen für Datenexporte wie verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, BCR), Verhaltensregeln, Zertifizierungen und Einzelfallgenehmigungen auswirkt, ist derzeit noch unklar. Gleiches gilt für die Frage, ob US-Unternehmen oder ihre

44 Siehe https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

europäischen Tochtergesellschaften oder andere US-verflochtene Unternehmen den US-amerikanischen Überwachungsgesetzen unterliegen, wenn sie Daten nicht in den USA, sondern in der EU verarbeiten. Auch an diesen Diskussionen und Prüfungen beteiligen wir uns intensiv.

Sehr klar ist das Urteil „Schrems II" allerdings hinsichtlich der Folgen unzulässiger Datenexporte: Kommt eine Aufsichtsbehörde am Ende ihrer Untersuchung zu dem Ergebnis, dass die betroffene Person, deren Daten in ein Drittland übermittelt wurden, dort kein angemessenes Schutzniveau genießt, ist sie nach dem Unionsrecht verpflichtet, in geeigneter Weise zu reagieren, um der festgestellten Unzulänglichkeit abzuhelfen – unabhängig davon, welchen Ursprungs und welcher Art die Unzulänglichkeit ist.[45] Daraus folgert der EuGH eine Verpflichtung der jeweiligen Aufsichtsbehörde, eine Übermittlung personenbezogener Daten in ein Drittland ohne Einräumung einer Übergangs- oder Anpassungsfrist auszusetzen oder zu verbieten,[46] wenn sie im Lichte aller Umstände der konkreten Datenübermittlung der Auffassung ist, dass die Standarddatenschutzklauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht durch andere Mittel gewährleistet werden kann.[47] Einzige Ausnahme von der Verpflichtung zum Erlass eines solchen Verbots ist die Situation, dass der Datenexporteur die Übermittlung bereits selbst ausgesetzt oder beendet hat. Derartige rechtswidrige Datenexporte sind im Übrigen auch mit Geldbußen bedroht.[48]

Die Prüfung von Übermittlungen personenbezogener Daten in Drittländer, für die kein Angemessenheitsbeschluss der EU-Kommission vorliegt, ist zunächst eine Herausforderung für die Datenexporteure. Sie ist aber auch eine Herausforderung für die Aufsichtsbehörden, die diese Prüfungen wiederum selbst überprüfen und die Datenexporte ggf. verbieten müssen. Dieser Herausforderung, die der EuGH aus den Grundrechten der Menschen in der Europäischen Union herleitet, stellen wir uns.

45 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 111
46 Siehe Art. 58 Abs. 2 lit. f und j DS-GVO
47 EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II", Rn. 113, 121, 135, 146
48 Siehe Art. 83 Abs. 5 lit. c DS-GVO

Die Übermittlung personenbezogener Daten in Drittländer ohne von der EU-Kommission anerkanntes angemessenes Datenschutzniveau setzt detaillierte und genau dokumentierte Prüfungen seitens der Datenexporteure voraus. Hierfür stehen Empfehlungen des EDSA zur Verfügung. Je nach Ergebnis der Prüfung müssen ggf. ergänzende Maßnahmen getroffen werden. Liegt das datenschutzrechtliche Problem des Drittlandes (auch) in unverhältnismäßigen behördlichen Zugriffsrechten, kommen nur technische Maßnahmen in Betracht, die den Zugriff der Behörden ausschließen oder die Daten für die Behörden nutzlos machen. Solche Maßnahmen gibt es aktuell nur für ganz wenige Anwendungsfälle. Daher ist die Nutzung der allermeisten US-Dienstleister unzulässig und kann auch derzeit nicht rechtmäßig gestaltet werden. Verantwortliche, die solche Dienstleister direkt oder indirekt nutzen, müssen die verarbeiteten Daten sofort zurückholen.

1.3 Einsatz von Videokonferenzsystemen

Infolge der Pandemie hat sich die Zahl der Menschen, die in Heimarbeit tätig sind, vervielfacht. Auch Schulen schlossen und verlagerten einen Teil ihres Unterrichts in den digitalen Raum. Videokonferenzen sind unter diesen Bedingungen ein wichtiges Werkzeug zur Aufrechterhaltung der Kommunikation. Wir erhielten eine große Anzahl von Anfragen und Beschwerden zu dem Thema. Um hier so weitreichend wie möglich helfen zu können, haben wir neben der direkten Beratung von Verantwortlichen und Anbietern auch allgemeine Empfehlungen für Nutzer*innen veröffentlicht.

Videokonferenzen bieten einen deutlichen Mehrwert zur Kommunikation über das Telefon. Entsprechend groß war das Bedürfnis, sie unter den Bedingungen von Heimarbeit und Schulschließungen einzusetzen. Angebote insbesondere US-amerikanischer Anbieter fluteten den Markt. Ihre Inanspruchnahme steht allerdings vielfach im Widerspruch zum Datenschutzrecht. Doch auch bei den Angeboten europäischer Anbieter mussten wir teils umfangreiche Mängel feststellen. Im konstruktiven Austausch mit einer Vielzahl von Anbietern konnten wir erhebliche Verbesserungen auf rechtlicher wie auf technischer Ebene erreichen.

Grundsätzlich können Verantwortliche Videokonferenzen auf zwei Wegen bereitstellen:

Zum Ersten können sie selbst die notwendige Informationstechnik betreiben – entweder durch Bereitstellung des Dienstes im eigenen Haus oder durch den Betrieb in einem externen Rechenzentrum. Die nötige Software ist am Markt erhältlich und kann von den Verantwortlichen an ihre Bedürfnisse angepasst werden. Dabei ist darauf hinzuweisen, dass Datenschutz durch Technikgestaltung möglich ist. Doch nur große Institutionen können es sich leisten, die dafür nötige Expertise bereitzuhalten.

Die zweite Variante besteht darin, einen Dienstleister zu beauftragen, der die gesamte Arbeit übernimmt. Unweigerlich kommt er dabei vielfältig mit personenbezogenen Daten in Berührung: Daten über die Durchführung der Konferenz und die daran Teilnehmenden, Ton- und Videoaufnahmen der Konferenz selbst, möglicherweise auch Textnachrichten zwischen den Beteiligten und Dokumente, die präsentiert werden. Die Inhalte der Kommunikation können sich darüber hinaus auf Dritte beziehen. Auf jeden Fall aber sagen all diese Daten viel über die teilnehmenden Personen selbst aus.

Daher müssen Verantwortliche dafür Sorge tragen, dass die Daten rechtmäßig verarbeitet werden. Schwierig wird dies, wenn die Daten außerhalb der EU in einem Land wie den USA verarbeitet werden, das keinen angemessenen Datenschutz für EU-Bürger*innen gewährleistet. Der EuGH hat hierfür in seinem Urteil „Schrems II“ hohe Anforderungen aufgestellt.[49] In der Tat sind viele Anbieter von Videokonferenzdiensten in den USA beheimatet. Problematisch ist auch, dass sich etliche Anbieter vorbehalten, Daten über die Nutzung ihrer Dienste für eigene Zwecke zu verarbeiten. Das dürfen Verantwortliche regelmäßig nicht erlauben.

49 Siehe 1.2

Wir haben diese Anforderungen systematisiert und in einer Handreichung nebst Checkliste näher dargestellt.[50]

Als eine Herausforderung gerade für kleine und mittlere Verantwortliche hat sich die erforderliche Prüfung der Auftragsverarbeitungsverträge der Anbieter von Videokonferenzdiensten herausgestellt. Um Verantwortliche dabei zu unterstützen, haben wir die Ergebnisse der im Rahmen unserer Aufsichts- und Beratungstätigkeit erfolgten Prüfungen von Angeboten, die Videokonferenzen als Software-as-a-Service (SaaS)[51] anbieten, veröffentlicht.[52] Den Schwerpunkt haben wir dabei auf die Bewertung der Rechtskonformität der von den Anbietern angebotenen Auftragsverarbeitungsverträge gelegt, weil ohne rechtskonformen Auftragsverarbeitungsvertrag eine Nutzung durch Verantwortliche im Anwendungsbereich der DS-GVO ausgeschlossen ist. Sofern bei einer Kurzprüfung keine rechtlichen Mängel festzustellen waren oder die Anbieter die identifizierten Mängel beseitigten und uns Informationen bzw. einen Test-Zugang zur Verfügung stellten, erfolgte zudem eine kursorische Untersuchung einiger technischer Aspekte der Dienste.

Im Ergebnis konnten wir in der ersten Version unserer Hinweise fünf Dienste mit einer „grünen Ampel" auf der rechtlichen Ebene versehen, die unter Beachtung bestimmter technisch-organisatorischer Bedingungen rechtskonform genutzt werden können. Mit einer „roten Ampel" mussten wir dagegen vor allem Angebote von US-Unternehmen bzw. deren EU-Tochtergesellschaften bewerten. Die Probleme hatten allerdings nicht nur mit unzulässigen Datenexporten in die USA

50 Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf; Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Checkliste_Videokonferenzen.pdf

51 Bei Software-as-a-Service (SaaS) betreibt der Anbieter die Server und die Software für den jeweiligen Dienst. Nutzende erhalten nur einen Zugriff auf die Leistungen dieses Dienstes, meist nur die Oberfläche, die oft im Web-Browser angezeigt wird. Es handelt sich dabei um einen typischen Cloud-Dienst. Im Gegensatz dazu erwerben Nutzende bzw. ihre Institutionen im klassischen Modell Software und Server und betreiben die Software selbst.

52 Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

zu tun, sondern auch mit ganz grundlegenden Verstößen gegen den europäischen Datenschutz. Hierzu zählten z. B. teilweise extreme Beschränkungen der Nachweispflicht von Anbietern hinsichtlich der Erfüllung ihrer vertraglichen Verpflichtungen oder der Kontrollrechte der Verantwortlichen. Verantwortliche, die derartige Dienste nutzen, verstoßen nicht nur gegen die gesetzlichen Vorschriften zur Auftragsverarbeitung[53], sondern können auch ihrer gesetzlichen Rechenschaftspflicht[54] nicht nachkommen. Darüber hinaus verbauen sie sich die Möglichkeit, sich gegenüber Schadensersatzansprüchen betroffener Personen zu entlasten.[55]

Unsere Hinweise trafen auf ein enormes Interesse bei den Verantwortlichen. Wir erhielten im Übrigen eine Vielzahl an Anfragen von Anbietern, die ihre Produkte ebenfalls in die Liste aufgenommen sehen wollten. Im Laufe des Jahres führten wir viele konstruktive Gespräche sowohl mit Anbietern, bei deren Produkten wir Mängel festgestellt hatten, als auch mit neuen Anbietern und konnten so erhebliche Verbesserungen bei den rechtlichen Regelungen und auf der technischen Seite der Produkte erreichen. Zum Jahresende hatten insgesamt elf Anbieter im intensiven Austausch mit uns ihre Verträge so angepasst, dass wir sie als mangelfrei bewerten konnten. Der Auftragsverarbeitungsvertrag eines weiteren Anbieters war nunmehr an sich mangelfrei, sah jedoch unzulässige Datenexporte in die USA vor, die sich allerdings bei der Nutzung des Dienstes unter bestimmten Bedingungen vermeiden ließen. Ein (US-)Anbieter hatte seine Verträge so verbessert, dass neben der Problematik von Datenexporten nur noch der – durch den Anbieter nicht behebbare – Mangel bestehen blieb, dass er den nach europäischem Recht unzulässigen Zugriff von US-Behörden auf die von ihm verarbeiteten Daten nicht ausschließen konnte.

Bei der Prüfung der Auftragsverarbeitungsverträge mussten wir immer wieder ähnliche Mängel feststellen. Um Verantwortliche auch bei der Prüfung von Anbietern, die wir nicht selbst überprüft haben, zu unterstützen, haben wir daher

53 Siehe Art. 28 DS-GVO

54 Siehe Art. 5 Abs. 2, Art. 24 Abs. 1 Satz 1 DS-GVO

55 Siehe Art. 82 Abs. 3 DS-GVO

typische Mängel zusammengefasst und veröffentlicht.[56] Diese können natürlich auch von Anbietern und deren Rechtsberatenden genutzt werden, um ihre Verträge selbst auf leicht vermeidbare Mängel zu untersuchen.

Auch bei der technischen Gestaltung ist Sorgfalt nötig. Die Datenübertragung muss ausreichend sicher sein. Im Normalfall sollen nur die Eingeladenen an den Konferenzen teilnehmen können. Die für die Konferenzen notwendige Software soll keine Lücken aufweisen, die von Dritten angegriffen und ausgenutzt werden können.

Wenn eine größere Zahl von Beteiligten an den Konferenzen teilnimmt, die unterschiedliche Aufgaben haben – Lehrende und Lernende zum Beispiel –, dann muss die Software diese Rollen abbilden können. Wer eine Konferenz moderiert, benötigt die Rechte, einer teilnehmenden Person die Rede zu gestatten oder das Rederecht zu entziehen, die Präsentation von Dokumenten zu erlauben oder sie zu verbieten und ungebetene Gäste aus der Konferenz zu entfernen. Auch Mitschnitte von Ton und Bild anzufertigen – sofern dafür eine Rechtsgrundlage besteht – liegt in den Händen der Konferenzorganisation.

Auf der anderen Seite sollten weder die moderierende Person noch Dritte Einblick in die private Lebenswelt der Teilnehmenden erhalten. Es sollte die Entscheidung der Teilnehmenden bleiben, wann sie Kamera und Mikrofon einschalten und wann nicht. Diese rechtliche Anforderung wird allerdings von vielen Anbietern nicht umgesetzt, stattdessen erfolgt der Beitritt zu einer Videokonferenz oftmals zwangsweise mit aktivierter Kamera und/oder aktiviertem Mikrofon.

Schließlich sollen von einer Videokonferenz nach ihrem Ende nur die Daten übrigbleiben, die weiterhin benötigt werden. Das können Angaben über die Konferenz und ihre Teilnehmenden, Protokolldaten, Aufzeichnungen des Chats oder auch Mitschnitte sein. Werden sie nicht mehr benötigt oder ist die Rechtsgrundlage für ihre Verarbeitung mit Ende der Konferenz entfallen, sind sie zu löschen.

56 Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenz-Diensten: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Pruefung_Auftragsverarbeitungsvertraege_Videokonferenz-Dienste.pdf

Vor dem Hintergrund unserer eigenen Prüfungen haben wir zusätzlich auch an der Erstellung einer Orientierungshilfe der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zu dem Thema[57] mitgewirkt.

Videokonferenzen sind wichtige Werkzeuge unseres Berufsalltags und unserer Bildungseinrichtungen geworden. Die Wahl und Gestaltung des eingesetzten Videokonferenzdienstes muss die datenschutzrechtlichen Anforderungen berücksichtigen. Dies erfordert eine sorgfältige Prüfung und Planung. Wir haben dafür verschiedene Hilfestellungen in unserem Webangebot bereitgestellt. Die Auswahl rechtskonform nutzbarer Angebote ist mittlerweile so hoch, dass es keine Rechtfertigung mehr dafür gibt, weiterhin Dienste zu nutzen, die gegen das Datenschutzrecht verstoßen.

1.4 Digitalisierung der Schulen – BER 2.0?

Mit dem Beginn der Corona-Pandemie und den kurzfristig erfolgten flächendeckenden Schulschließungen im März wurden die erheblichen Defizite bei der Digitalisierung der Schulen offenbar. Die vergangenen Monate haben deutlich gezeigt, dass das Land Berlin es über viele Jahre versäumt hat, die notwendigen Maßnahmen zu ergreifen, um die Schüler*innen und ihre Lehrkräfte in die Lage zu versetzen, das digitale Lernen in der Praxis umzusetzen. Neben allen praktischen Problemen, ein halbwegs funktionierendes Lernen mittels digitaler Werkzeuge innerhalb und außerhalb der Schule überhaupt zu ermöglichen, mussten wir feststellen, dass zudem versäumt wurde, die datenschutzgerechte Ausgestaltung der genutzten Umgebungen in den Blick zu nehmen. Es ist ernüchternd, feststellen zu müssen, dass mit Blick auf eine nun bereits viele Monate andauernde Pandemie und erneut notwendige Schulschließungen auch zum Ende des Jahres 2020 keine positive Bilanz gezogen werden kann. Im Gegenteil: Die im Frühjahr festgestellten Defizite bestehen teilweise unverändert fort. An vielen Schulen wird nach wie vor auf digitale Lernwerkzeuge zurückgegriffen, die

57 Orientierungshilfe Videokonferenzsysteme und Checkliste Datenschutz in Videokonferenzsystemen; beide abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/orientierungshilfen

mit dem geltenden Datenschutzrecht nicht vereinbar sind und auch im Übrigen kommt die Digitalisierung der Schulen nur sehr schleppend voran.

Mit den Vorsorgemaßnahmen zur Eindämmung der Corona-Pandemie trafen die in allen Lebensbereichen notwendigen Einschränkungen die Schüler*innen, aber auch die Lehrkräfte und Eltern in besonderer Weise. Die Schulen standen vor der Herausforderung, mit den Schüler*innen und Lehrkräften von einem Tag auf den anderen einen Unterricht auf Distanz zu organisieren, meist ohne hierfür mit geeigneten Instrumenten ausgestattet zu sein. Überzeugt davon, dass die Pandemie den in diesem Bereich ohnehin anstehenden Wandel nur beschleunigt hat, haben wir die Entwicklungen das ganze Jahr über sehr intensiv begleitet. Wir haben dies in der Überzeugung getan, dass die Digitalisierung der Schulen nur dann erfolgreich sein kann, wenn der Datenschutz von vornherein mitberücksichtigt wird – auch wenn dies unter dem enormen Handlungsdruck der Pandemie anfangs nur eingeschränkt umsetzbar war. Aus unserer Sicht war es aber von grundlegender Bedeutung, dass die Anforderungen des Datenschutzes nicht aus dem Blick gerieten, um sie so schnell wie möglich zumindest nachbessern zu können. Denn bei der Digitalisierung des Schulunterrichts werden Daten von Kindern und Jugendlichen verarbeitet, die unter dem besonderen Schutz der DS-GVO stehen. Ein Missbrauch dieser Daten kann zu empfindlichen Konsequenzen für die Betroffenen führen.

So haben wir in der ersten Welle der Pandemie keinerlei Sanktionsmaßnahmen ergriffen, wenn nicht datenschutzgerechte digitale Lehrmittel eingesetzt wurden, sondern haben uns ausschließlich der intensiven Beratung der Betroffenen gewidmet und unsere Beratung der fachlich zuständigen Senatsverwaltung für Bildung, Jugend und Familie immer wieder angeboten. Gleichzeitig haben wir sehr frühzeitig darauf hingewiesen, dass die Nutzung entsprechender Werkzeuge mit erheblichen Gefahren für die Persönlichkeitsrechte der Schüler*innen auf der einen Seite, aber auch der Lehrkräfte auf der anderen Seite verbunden sein kann.

Im Gegensatz zum analogen Schulunterricht fällt bei der Nutzung digitaler Lernplattformen eine Vielzahl von Daten an. Es besteht die Gefahr, dass gerade private Anbieter das Nutzungsverhalten der Schüler*innen sehr genau auswerten und für eigene wirtschaftliche Zwecke nutzen. Fehlende Löschfunktionen bergen zudem die Gefahr, dass längst nicht mehr für pädagogische Aufgaben notwendige Infor-

mationen dauerhaft gespeichert bleiben und später nachteilig für die Schüler*innen genutzt werden. Spätestens seit der Entscheidung „Schrems II“ des EuGH[58] ist die Zulässigkeit der Nutzung von Angeboten US-amerikanischer Anbieter besonders kritisch zu überprüfen. Sofern sich Anbieter für Datenübermittlungen durch ihre Produkte z. B. noch immer auf das „US-Privacy Shield“ berufen, das vom EuGH für ungültig erklärt wurde, können diese im Schulkontext nicht zum Einsatz kommen.

Wir haben immer wieder darauf hingewiesen, dass digitale Lernumgebungen datenschutzkonform ausgestaltet werden müssen. Dies ist schon deswegen von grundlegender Bedeutung, weil damit das notwendige Vertrauen aller Beteiligten in die Nutzung digitaler Angebote aufgebaut werden kann. Die Vielzahl der in diesem Zusammenhang bei uns eingehenden Anfragen zeigt uns, dass auf Seiten der Schulleitungen und der Lehrkräfte eine große Rechtsunsicherheit besteht, welche Angebote datenschutzrechtlich unbedenklich eingesetzt werden können. Beschwerden von Eltern zeigen, dass eine große Sorge über einen zu laxen Umgang mit den Persönlichkeitsrechten der Schüler*innen in den Schulen besteht.

Um eine erste Hilfestellung zu bieten, haben wir bereits Anfang April Hinweise zum datenschutzkonformen Einsatz von digitalen Lernplattformen veröffentlicht.[59] Uns ging es darum, den Schulleitungen und Lehrkräften Kriterien an die Hand zu geben, die es ihnen erleichtern sollten, zu erkennen, welche Angebote datenschutzkonform bei der Unterrichtsgestaltung zum Einsatz kommen können.

Mit der Corona-Pandemie entstand in allen Bereichen auch ein hoher Bedarf für die Durchführung von Videokonferenzen. Wir haben ausführliche Hinweise für Verantwortliche zum Einsatz von Videokonferenzdiensten erarbeitet und veröffentlicht.[60] Diese Hinweise gelten selbstverständlich auch im Schulkontext.

58 Siehe 1.2

59 Hinweise zum datenschutzkonformen Einsatz von digitalen Lernplattformen im Unterricht: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Lernplattformen_Hinweise.pdf

60 Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf; siehe auch 1.3

Die Schulleitungen und Lehrkräfte sind mit der Aufgabe, die Datenschutzkonformität einzelner Produkte zu prüfen, regelmäßig überfordert. Dies ist verständlich, denn es handelt sich hierbei um eine technisch und rechtlich überaus komplexe Aufgabe, die weit über die Prüfung der pädagogischen Eignung hinausgeht. Wir sehen hier die Bildungsverwaltung in der Pflicht, entsprechende Angebote sowohl in pädagogischer Hinsicht als auch – gemäß den Regelungen der auch für den Schulbereich geltenden DS-GVO – im Hinblick auf die Einhaltung der Anforderungen des Datenschutzes und der Datensicherheit zu prüfen und den Schulen eine geeignete Vorauswahl zur Verfügung zu stellen. Es ist notwendig, dass die Bildungsverwaltung klare Vorgaben definiert, welche digitalen Lehr- und Lernmittel von den Schulen genutzt werden können, und den Lehrkräften rechtssichere Angebote unterbreitet. Die von der Bildungsverwaltung immer wieder angeführten Bedenken, eine Liste datenschutzkonformer Produkte könne aus rechtlichen Gründen nicht erstellt werden und würde im Übrigen in die durch das Schulgesetz garantierte Lehr- und Lernmittelfreiheit[61] eingreifen, ist nicht nachvollziehbar. Es ist selbstverständlich, dass Lehrkräfte selbst entscheiden können, welche Schulbücher aus ihrer Sicht pädagogisch für ihren Unterricht geeignet sind und zum Einsatz kommen sollen. Die Lage stellt sich jedoch bei digitalen Angeboten anders dar: Die Lehrkraft hat nicht nur über die pädagogische Eignung zu entscheiden, sondern ist gleichzeitig in der Pflicht, auch noch die Datenschutzkonformität des jeweiligen Produktes in rechtlicher und technischer Sicht zu prüfen. Die uns erreichenden Rückmeldungen zeigen, dass die Lehrkräfte sich gerade nicht in ihrer pädagogischen Freiheit eingeschränkt sehen, sondern sich vielmehr Unterstützung bei der Auswahl geeigneter und rechtskonformer digitaler Produkte sowie klare Vorgaben wünschen.

Leider mussten wir das ganze Jahr über feststellen, dass die Senatsverwaltung für Bildung, Jugend und Familie ihrer Aufgabe, den Schulen die notwendige Unterstützung zu geben, nicht gerecht wird. Unsere Behörde wurde in den notwendigen Prozess der datenschutzgerechten Ausgestaltung der schulischen Angebote ebenfalls nur unzureichend einbezogen. Wie die nachfolgenden Beispiele veranschaulichen, wurde die von uns wiederholt angebotene fachliche Unterstützung nur teilweise und dann auch nur sehr zögerlich angenommen.

61 Insbesondere § 7 Abs. 2 SchulG

1.4.1 „Lernraum Berlin“

Das Projekt „Lernraum Berlin“ existiert bereits seit 2005. Eine Einbindung unserer Behörde in das Projekt erfolgte zu keinem Zeitpunkt. Mit den Schulschließungen im März bekam der „Lernraum Berlin“ plötzlich eine ganz erhebliche Bedeutung für die Aufrechterhaltung des Unterrichtsbetriebes auf Distanz. Da wir bereits kurz vor Beginn der Corona-Pandemie Hinweise zu dem Projekt und zu damit verbundenen Datenschutzmängeln, wie z. B. eine fehlende Mandantenfähigkeit[62] und fehlende Löschroutinen, erhielten, hatten wir schon im Februar Unterlagen bei der zuständigen Senatsverwaltung angefordert, um eine Prüfung des Angebots vorzunehmen. Die Bildungsverwaltung reagierte darauf leider mehrere Monate nicht, sodass wir im Sommer die Übersendung der Unterlagen anmahnen mussten, gleichzeitig aber auch wieder unsere Beratung angeboten haben. Uns ging es darum, dass möglichst schon während der Sommerferien an der Beseitigung etwaiger Mängel und an der Umsetzung der für ein datenschutzkonformes Angebot notwendigen Anforderungen hätte gearbeitet werden können. Die ersten uns vorgelegten Unterlagen bestätigten das Vorliegen von erheblichen Mängeln in Bezug auf die Einhaltung des Datenschutzes und der Datensicherheit. Wir haben umfassende Hinweise zur Beseitigung der Mängel gegeben und befinden uns leider erst seit dem Ende der Sommerferien mit den für das Projekt „Lernraum Berlin“ Verantwortlichen in einem recht konstruktiven Austausch.

Wir begrüßen es, dass die Bildungsverwaltung mit dem „Lernraum Berlin“ ein eigenes, vom Land betriebenes Lernmanagementsystem für den digitalen Unterricht zur Verfügung stellt. Durch den intensiven Austausch in den vergangenen Monaten konnten deutliche Verbesserungen erzielt werden, sodass wir den „Lernraum Berlin“ mittlerweile auf einem guten Weg sehen. Es konnte zwischenzeitlich die mangels existierender Rechtsgrundlage für die Verarbeitung personenbezogener Daten bei der Nutzung digitaler Lehr- und Lernmittel noch immer notwendige Einwilligungserklärung für die Nutzung des „Lernraum Berlin“ überarbeitet werden. Sie entspricht jetzt den datenschutzrechtlichen Anforderungen. Da über den „Lernraum Berlin“ auch die Möglichkeit zur Durchführung von Video-

62 Bei der Gestaltung von Systemen ist darauf zu achten, dass diese, sofern sie für mehrere Verantwortliche (z. B. Schulen) auf ein und demselben Server laufen, so ausgestaltet sind, dass jeweils nur die Berechtigten auf ihre eigenen Daten zugreifen dürfen und ein gegenseitiger Zugriff ausgeschlossen wird.

konferenzen besteht, begrüßen wir es insbesondere, dass die Bildungsverwaltung die bisher darin eingebundene, datenschutzrechtlich bedenkliche Videokonferenzlösung durch eine datenschutzkonforme Lösung unter Nutzung der Open Source Software BigBlueButton ablöst.

Wir werden die Entwicklung des Projekts auch im Jahr 2021 weiterhin begleiten.

1.4.2 Digitale Endgeräte für benachteiligte Schüler*innen und sog. Sommerschulen

Viele Schüler*innen haben durch die Schulschließungen erhebliche Nachteile erlitten, z. B. weil es ihnen an der notwendigen Ausstattung mit entsprechenden Endgeräten mangelte. Die Beschaffung von Geräten für die betroffenen Schüler*innen ist selbstverständlich begrüßenswert, damit diese nicht den Anschluss verlieren. Auch die Durchführung von sog. Sommerschulen in den Sommer- und Herbstferien war sehr sinnvoll, um den Schüler*innen die Möglichkeit zu geben, versäumten Unterrichtsstoff nachzuholen.

Allerdings mussten wir in dem ganzen Verfahren doch eine mangelnde Sensibilität der Bildungsverwaltung in Bezug auf die Datenschutzbelange der betroffenen Schüler*innen feststellen: Die Schulen wurden von der Bildungsverwaltung aufgefordert, per unverschlüsselter E-Mail die personenbezogenen Daten der betroffenen Schüler*innen an die Bildungsverwaltung bzw. den privaten Träger, der die sog. Sommerschulen durchführen sollte, zu übermitteln. Es handelte sich bei diesen Daten um solche zur Anspruchsberechtigung nach dem Sozialgesetzbuch und damit um sensitive Sozialdaten. Unabhängig von der Frage, ob diese Daten überhaupt zulässig an die Bildungsverwaltung bzw. den freien Träger weitergegeben werden durften, wäre es ausreichend gewesen, die Anzahl der berechtigten Schüler*innen zu übermitteln und die personenbezogenen Daten in den Schulen zu belassen. Die Aufforderung der Bildungsverwaltung an die Schulen, die Daten in einer Excel-Tabelle per unverschlüsselter E-Mail zu übersenden, ist mit den Regelungen der DS-GVO nicht vereinbar. Die Bildungsverwaltung ist in der Position, für sichere Kommunikationskanäle zwischen ihr und den Schulen zu sorgen. Planungen der Bildungsverwaltung, sichere E-Mail-Adressen für alle Lehrkräfte einzurichten, werden von uns ausdrücklich begrüßt.

Im Laufe des Jahres hat die Bildungsverwaltung weitere ca. 40.000 Tablets für benachteiligte Schüler*innen beschafft. Aus Datenschutzsicht wäre es vorzugswürdig gewesen, Laptops für die Schüler*innen anzuschaffen. Laptops bieten deutliche Vorteile gegenüber Tablets, da sie wesentlich vielseitiger einsetzbar sind, mehr Freiheiten bei der Softwareauswahl bieten und auch ohne einen Cloudzugang bei Anbietern außerhalb der Europäischen Union und damit datenschutzgerecht nutzbar sind. Schließlich wäre durch günstigere Preise sicherlich auch eine umfassendere Verteilung an die Schüler*innen möglich gewesen, sodass eine einheitliche Lernumgebung für alle hätte geschaffen werden können. Wir bedauern es, dass unsere dahingehend gegenüber der Senatsverwaltung für Bildung, Jugend und Familie und dem Parlament abgegebenen Empfehlungen nicht berücksichtigt worden sind. [63]

1.4.3 Kommunikation über Messenger-Dienste

Die Kommunikation zwischen Lehrkräften, Schüler*innen und Eltern ist ein weiterhin wichtiges Thema. Im März wurden wir darüber informiert, dass die Qualitätsbeauftragte der Bildungssenatorin auf eine Anfrage zum Einsatz von WhatsApp in Schulen im Kontext der Corona-Pandemie geantwortet habe, bei Einverständnis aller Beteiligten dürften WhatsApp und Skype vorübergehend genutzt werden. Wir haben dies zum Anlass genommen, die Senatorin zu bitten, gegenüber den Schulen klarzustellen, dass ausschließlich datenschutzkonforme Angebote zum Einsatz kommen dürfen. Gleichzeitig haben wir unsere Unterstützung und Beratung angeboten. Eine Antwort haben wir jedoch nicht erhalten.

Angesichts bestehender Alternativen ist der Einsatz nicht datenschutzgerechter Produkte nicht hinnehmbar. In unserem letzten Jahresbericht haben wir ausführlich dargelegt, dass der Messenger-Dienst WhatsApp in Schulen nicht zum Einsatz kommen kann.[64] Vielmehr besteht die Notwendigkeit, dass das Land Berlin perspektivisch einen eigenen Messenger-Dienst zur Verfügung stellt. Aktuelle Beispiele anderer Bundesländer zeigen, dass datensichere Messenger-Dienste

63 Siehe https://www.parlament-berlin.de/adosservice/18/Haupt/vorgang/h18-2735.G-v.pdf

64 JB 2019, 1.1

auch kurzfristig eingerichtet werden können.[65] Es ist an der Zeit, dass auch das Land Berlin diesen Beispielen folgt.

1.4.4 Rechtsgrundlagen für die Schuldigitalisierung sind dringend notwendig

Wann immer personenbezogene Daten verarbeitet werden, setzt dies eine geeignete Rechtsgrundlage oder eine Einwilligung voraus. In Bereichen, in denen Daten von Minderjährigen verarbeitet werden, sollte das selbstverständlich sein. Kinder und Jugendliche stehen unter dem besonderen Schutz der DS-GVO.[66] Das Schulgesetz und die seit dem Jahre 1994 bestehende Schuldatenverordnung[67] enthalten keine Regelungen zum Einsatz digitaler Werkzeuge. Die allgemeinen Vorschriften des Schulgesetzes über die Verarbeitung personenbezogener Daten können hier nicht herangezogen werden.

Das Bundesverfassungsgericht legt in seiner Wesentlichkeitsrechtsprechung immer wieder dar, dass wesentliche Entscheidungen durch ein parlamentarisches Gesetz zu regeln sind. Die Entscheidung über den Einsatz digitaler Lehrmittel ist aufgrund der damit verbundenen Gefahren des Missbrauchs von Daten der Schüler*innen und Lehrkräfte ohne Zweifel als wesentlich zu bezeichnen. Der Wechsel von rein analogen Lehrmitteln hin zu digitalen Produkten bringt es mit sich, dass nicht mehr nur über die pädagogische Eignung des jeweiligen Produkts zu entscheiden ist, sondern nunmehr auch über die Einhaltung komplexester technischer und datenschutzrechtlicher Vorgaben. Angesichts der besonderen Qualität von Grundrechtseingriffen beim Einsatz digitaler Werkzeuge muss daher das Schulgesetz an diese Lage angepasst werden. Die konkrete Ausgestaltung sollte durch eine spezielle Rechtsverordnung erfolgen, die die datenschutzrechtlichen Anforderungen regelt.

65 Das Land Nordrhein-Westfalen stellt den Schulen seit August 2020 in Ergänzung zur Schulplattform LOGINEO NRW den LOGINEO NRW Messenger kostenlos zur Verfügung, um die Kommunikation mit den Schüler*innen zu ermöglichen, und das Kultusministerium Baden-Württemberg stellt den Lehrkräften eine kostenlose Lizenz des Messengers Threema Work Education zur Verfügung.

66 Siehe EG 38 DS-GVO

67 Zur Novellierung der Schuldatenverordnung, die im Jahr 2020 noch immer nicht abgeschlossen wurde, haben wir im JB 2019, 5.4 ausführlich berichtet.

Derzeit muss mangels einer ausreichenden Rechtsgrundlage auf die Einwilligung der Eltern für den Einsatz digitaler Lernmittel zurückgegriffen werden. Die Einwilligung begegnet im Schulkontext allerdings grundsätzlichen Bedenken. Eine Einwilligung kann nämlich nur wirksam sein, wenn sie freiwillig erfolgt. Zwischen den Schülerinnen und Schülern und den Lehrkräften besteht jedoch aufgrund der Schulpflicht ein Über-/Unterordnungsverhältnis. Die DS-GVO geht in solchen Fällen grundsätzlich davon aus, dass die Einwilligung unzulässig ist. Um das Kriterium der Freiwilligkeit in der Praxis dennoch erfüllen zu können, ist es daher notwendig, dass die Schulen denjenigen, die ihre Einwilligung für die Nutzung digitaler Angebote nicht erteilen möchten, gleichwertige alternative Lernangebote zur Verfügung stellen. Dies kann in der Praxis durchaus zu Umsetzungsschwierigkeiten führen. Um hier für alle Beteiligten die notwendige Rechtssicherheit und auch eine höhere Verbindlichkeit für die digitale Unterrichtsgestaltung zu erreichen, halten wir es für erforderlich, dass der Gesetzgeber zügig tätig wird.

Die Erfahrungen in diesem Jahr zeigen, dass das Ziel einer erfolgreichen und datenschutzkonformen Digitalisierung der Schulen noch weit entfernt ist. Schritte in die richtige Richtung – wie beim „Lernraum Berlin“ – sind durchaus erkennbar, dennoch sind diese noch viel zu klein, um das Ziel bald erreichen zu können. Wir erwarten, dass die Bildungsverwaltung endlich erkennt, dass der Datenschutz kein Selbstzweck oder gar ein Hindernis für die Digitalisierung ist, sondern eine notwendige Voraussetzung für ein sicheres und vertrauensvolles Arbeiten im digitalen Raum. Wir werden uns weiterhin dafür einsetzen, dass Kinder und Jugendliche im digitalen Unterricht sorglos und unbeobachtet lernen können, ohne dass ihnen Unternehmen über die Schulter schauen. Von der Bildungsverwaltung erwarten wir zügiges und entschiedenes Handeln, um in den Schulen eine geschützte digitale Lernumgebung für alle Schüler*innen zu schaffen.

1.5 Startschuss für die Zertifizierung

Hohe Qualität und Vertrauenswürdigkeit sind die wichtigsten Erwartungen an Zertifizierungsstellen, die Datenverarbeitungsvorgänge zertifizieren. Die DS-GVO sieht deshalb vor, dass eine entsprechende Qualifizierung und Organisation der Zertifizierungsstellen gewährleistet werden muss. Dies wird insbesondere

durch die vorherige Akkreditierung sichergestellt. Die deutschen Aufsichtsbehörden haben konkretisierte Anforderungen vorgelegt, was im Rahmen der Akkreditierung nachzuweisen ist.

Schon lange vor Inkrafttreten der DS-GVO wurde der Wunsch nach verlässlichen Datenschutzzertifikaten und -siegeln laut, an denen sich Verbraucher*innen orientieren können, die Wert auf Datenschutz und Privatsphäre legen, und welche zugleich den Wettbewerb um datenschutzfreundliche Anwendungen stärken. Mit der DS-GVO wurden dazu die rechtlichen Voraussetzungen geschaffen, die aber noch mit Leben erfüllt werden müssen. So müssen Zertifizierungen nicht unbedingt durch die Datenschutz-Aufsichtsbehörden selbst erfolgen. Nach dem in Deutschland gewählten Modell obliegt den Aufsichtsbehörden vielmehr die Aufgabe, in Kooperation mit der Deutschen Akkreditierungsstelle (DAkkS) Zertifizierungsstellen zu akkreditieren, die dann ihrerseits Zertifikate verleihen dürfen.

Als Zertifizierungsstelle können sich also alle Unternehmen oder sonstigen Stellen bewerben, die meinen, die Akkreditierungsvoraussetzungen zu erfüllen. Da sich diese Voraussetzungen nicht im Detail aus der DS-GVO oder anderen Normen ergeben, sieht die DS-GVO vor, dass die Aufsichtsbehörden die Anforderungen für Akkreditierungen im Datenschutzbereich konkretisieren. Unsere Behörde hat in den letzten zwei Jahren gemeinsam mit den anderen deutschen Aufsichtsbehörden in einer Arbeitsgruppe intensiv daran mitgearbeitet und „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065" entwickelt.[68] Das Dokument hat das erforderliche Stellungnahmeverfahren des EDSA bereits erfolgreich durchlaufen.[69]

Die wichtigsten Anforderungen sind:

Zertifizierungsgegenstand

Zur Vorbereitung einer Akkreditierung muss ein Zertifizierungsprogramm erstellt werden. Dieses Programm bezieht sich auf einen Zertifizierungsgegenstand. Ein Zertifizierungsgegenstand muss Datenverarbeitungsvorgänge betreffen,und zwar

68 Siehe https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/themen-a-z/a/2020-DSK-DIN17065-Ergaenzungen-de.pdf

69 Siehe https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202015_de_requirementscertificationbodies_en.pdf

nur solche, die in Produkten, Prozessen und Dienstleistungen erbracht werden. Das heißt, Produkte ohne konkreten Einsatzbereich bzw. Anwendungsfall sind nicht als Zertifizierungsgegenstände geeignet. Denn ohne eine konkrete Anwendung lässt sich nicht feststellen, ob eine DS-GVO-konforme Datenverarbeitung vorliegt. Managementsysteme für die Steuerung von Datenverarbeitungsvorgängen sind für sich genommen ebenfalls als Gegenstand der Zertifizierung ausgeschlossen. Sie finden allerdings als Teil eines „Zertifizierungsmechanismus" Berücksichtigung.

Unparteilichkeit

Die Unparteilichkeit ist eine zentrale Voraussetzung für die zuverlässige Tätigkeit einer Zertifizierungsstelle. Sie ist nur dann gegeben, wenn Unabhängigkeit und Objektivität gewährleistet sind. Interessenskonflikte dürfen nicht existieren. Es müssen insbesondere die folgenden Anforderungen erfüllt sein:

- Gegenüber der zuständigen Datenschutzaufsichtsbehörde ist die Unabhängigkeit nachzuweisen. Dies gilt insbesondere für die Finanzierung der Zertifizierungsstelle, soweit die Sicherstellung der Unparteilichkeit betroffen ist.

- Die Zertifizierungsstelle muss der zuständigen Datenschutzaufsichtsbehörde zudem nachweisen, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Solche Konflikte könnten sich z. B. durch eine hohe Umsatzabhängigkeit von bestimmten Kund*innen oder durch sonstigen wirtschaftlichen Druck auf die Zertifizierungsstelle ergeben.

- Bei einer Zertifizierungsstelle muss es sich im Verhältnis zu deren Kundschaft um einen unabhängigen Dritten handeln, der mit der Einrichtung, die er bewertet, in keinerlei Verbindung steht. Die Zertifizierungsstelle, ihre oberste Leitungsebene und die für die Erfüllung der Zertifizierungsaufgaben zuständigen Beschäftigten dürfen insbesondere nicht Konstrukteur*in, Hersteller*in, Lieferant*in, Installateur*in, Käufer*in, Eigentümer*in, Verwender*in oder Wartungsbetrieb der zu bewertenden Produkte sein.

- Der Status einer Zertifizierungsstelle als unabhängige dritte Stelle ist in manchen Fällen besonders aufmerksam zu hinterfragen. Gehört eine Zertifizierungsstelle z. B. einem Verband an, dessen Mitglieder ihrerseits Hersteller*in,

Anbieter*in, Auftragsverarbeiter*in oder Verantwortliche sind, die von dieser Zertifizierungsstelle zertifiziert werden, muss genauer hingeschaut werden. Die Unabhängigkeit bzw. Unparteilichkeiten sowie die Abwesenheit jedweder Interessenkonflikte müssen besonders in diesen Fällen genau nachgewiesen werden. Im hier gewählten Beispiel wirkt es sich positiv aus, wenn die Zertifizierungsstelle rechtlich von dem Verband getrennt ist. Auch das Personal der beiden Stellen muss getrennt sein. Das Personal des Verbandes darf in keiner Weise für die Zertifizierungsstelle, insbesondere in Zertifizierungs-, Prüf- und Inspektionsverfahren, tätig werden. Die oberste Leitung der Zertifizierungsstelle muss sich im Gesellschaftervertrag oder in der Satzung der Zertifizierungsstelle zur Unparteilichkeit verpflichtet haben. Positiv wirkt es sich zudem aus, wenn die Satzung oder der Gesellschaftervertrag einen Passus zur Weisungsunabhängigkeit der Geschäftsführung bzw. der Leitung der Zertifizierungsstelle enthält. Außerdem darf kein wirtschaftliches Abhängigkeitsverhältnis zu den Mitgliedern des Verbandes oder dem Verband selbst bestehen.

Haftung und Finanzierung

Ein weiteres wichtiges Kriterium für die Unparteilichkeit und Objektivität ist eine finanzielle Stabilität und Unabhängigkeit. Die Zertifizierungsstelle muss zum einen darlegen können, dass sie die Risiken, die aus ihren Zertifizierungstätigkeiten entstehen, beurteilt hat und abdecken kann. Hierfür sind z. B. Versicherungen oder Rücklagen geeignete Mittel. Die Zertifizierungsstelle hat zum anderen ihre finanzielle Stabilität und Unabhängigkeit selbst nachzuweisen. Die Entscheidung hinsichtlich der Auswahl und Benennung geeigneter Nachweise liegt im Ermessen der DAkkS und der zuständigen Datenschutzaufsichtsbehörde. Die Zertifizierungsstelle muss jedenfalls über eine für den Umfang ihrer Tätigkeit angemessene Vermögensschaden-Haftpflichtversicherung verfügen.

Öffentlich zugängliche Informationen

Transparenz ist eine wichtige Voraussetzung sowohl für die Qualität von Zertifizierungen als auch für das Vertrauen in sie. Um Transparenz zu gewährleisten, sind etwa Informationen zum Umgang mit Beschwerden von der Zertifizierungsstelle zu veröffentlichen. Diese Veröffentlichungspflicht bezieht sich insbesondere auf die Struktur und Verfahrensweise zur Bearbeitung von Beschwerden durch die Zertifizierungsstelle. Zudem sind Informationen über die von der Zertifizierungsstelle verwendeten Zertifizierungsprogramme sowie alle Versionen der geneh-

migten Zertifizierungskriterien unter Angabe des jeweiligen Verwendungszeitraums zu veröffentlichen.

Die Form der Veröffentlichung sollte geeignet sein, die Öffentlichkeit möglichst umfassend zu erreichen. Dies ist in der Regel durch die Veröffentlichung auf der Internetseite gewährleistet.

Verzeichnis zertifizierter Produkte, Prozesse und Dienstleistungen

Eine besondere Transparenzverpflichtung stellt die Pflicht zur Veröffentlichung eines Verzeichnisses zertifizierter Produkte, Prozesse und Dienstleistungen dar. Die Zertifizierungsstelle kann dieses Verzeichnis über das Internet allgemein abrufbar halten. Das Verzeichnis muss ein Kurzgutachten bezüglich des jeweiligen Zertifizierungsergebnisses umfassen. Aus diesem muss sich insbesondere der genaue Zertifizierungsgegenstand (inklusive Versions- oder Funktionsstand), das Prüfverfahren und -ergebnis sowie das Ablaufdatum der Zertifizierung ergeben.

Ressourcen und Personalkompetenz

Eine Zertifizierungsstelle muss sowohl das geeignete Fachwissen hinsichtlich des Datenschutzes als auch ihre Unabhängigkeit sowie spezifisches Fachwissen hinsichtlich des Zertifizierungsgegenstands nachweisen können. Dies dient insbesondere der Sicherstellung der erforderlichen Qualität von Zertifizierungen. Werden Zertifizierungstätigkeiten an externe Stellen ausgegliedert, so gelten für diese Stellen die gleichen Voraussetzungen wie für die Zertifizierungsstelle.

Um die Kompetenz der Zertifizierungsstelle bewerten zu können, wird im Akkreditierungsverfahren zusätzlich zu den schriftlich vorgelegten Unterlagen wie z. B. Ausbildungsnachweisen eine begleitende Begutachtung vorgenommen.

Die für die Zertifizierungstätigkeit erforderlichen Kenntnisse des Personals müssen auf dem aktuellen Stand gehalten werden. Ein Nachweis kann insbesondere durch Fortbildungsbescheinigungen und einschlägige Arbeitserfahrung, z. B. durchgeführte Zertifizierungsverfahren, erbracht werden.

Anforderungen an Prozesse – Evaluation

Die Zertifizierungsstelle muss geeignete Evaluationsmethoden, d. h. Verfahren zur Überprüfung, vorsehen, um die Übereinstimmung der Verarbeitungsvorgänge

mit den Zertifizierungskriterien zu bewerten. Diese Methoden und die Ergebnisse bzw. Erkenntnisse der Überprüfung müssen ausführlich dokumentiert werden.

Die Evaluationsmethoden müssen insbesondere folgende Bereiche abdecken:

- eine Methode zur Bewertung der Erforderlichkeit und Verhältnismäßigkeit von Verarbeitungsvorgängen in Bezug auf ihren Zweck und ggf. in Bezug auf die betroffene Person,

- eine Methode zur Bewertung der Zusammenstellung und Einschätzung aller relevanten Datenschutz-Risiken sowie der Festlegung von technischen und organisatorischen Maßnahmen,

- eine Methode zur Bewertung der Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Nachweis erbracht wird, dass die gesetzlichen Anforderungen erfüllt werden.

Die Zertifizierungsstelle kann im Verlaufe des Zertifizierungsverfahrens weitere aus ihrer Sicht für die Zertifizierung notwendige Informationen anfordern. Sie kann das Zertifizierungsverfahren abbrechen, sofern die Antragstellerin oder der Antragssteller die Informationen trotz Aufforderung nicht vorlegt.

Die Zertifizierungsstelle muss festlegen, welchen Stellenwert andere Zertifizierungen der Kund*innen, z. B. der IT-Grundschutz, für ihre Evaluierung einnehmen. Es muss feststehen, welche anderen Zertifizierungen wie und in welchem Umfang für eine Evaluierung berücksichtigt werden können und welche Auswirkungen dies konkret auf den verbleibenden Prüfumfang hat.

Beschwerden und Einsprüche

Damit Zertifizierungsstellen erfahren, wenn es in der Praxis Probleme z. B. mit einer zertifizierten Dienstleistung gibt, ist vorgesehen, dass Beschwerden und Einsprüche direkt bei ihr eingelegt werden können. Sie muss festlegen, wer Beschwerden oder Einsprüche einreichen kann, wer diese auf der Seite der Zertifizierungsstelle bearbeitet, welche Überprüfungen in diesem Zusammenhang stattfinden und welche Möglichkeiten der Anhörung für die Beteiligten bestehen. Außerdem sind Fristen für die Beteiligten zu definieren.

Im Falle begründeter Beschwerden ist die zuständige Datenschutzaufsichtsbehörde zu informieren.

Es liegt ein ausführliches Papier der Datenschutzaufsichtsbehörden vor, das die Anforderungen an die Akkreditierung von Stellen beschreibt, die Datenverarbeitungstätigkeiten zertifizieren möchten. Angehende Zertifizierungsstellen können mithilfe dieses Dokuments prüfen, ob sie und ihre Organisation für ein Akkreditierungsverfahren ausreichend vorbereitet sind. Die Aufgabe der Datenschutzaufsichtsbehörden ist damit jedoch nicht abgeschlossen. Im Gegenteil, sie geht gerade dann erst richtig los. Wir werden bei entsprechenden Anträgen das Akkreditierungsverfahren gemeinsam mit der DAkkS durchführen und angehende Zertifizierungsstellen anhand der genannten Kriterien auf Herz und Nieren prüfen. In Berlin liegen uns schon etliche Interessenbekundungen vor.

2 Digitale Verwaltung

Die Corona-Pandemie hat in den verschiedensten Bereichen Defizite bei der Digitalisierung aufgezeigt.[70] Dies gilt auch für den Bereich der Verwaltung. Eingeschränkte Servicezeiten von Bürgerämtern, aber auch das Herunterfahren der Verwaltung mit dem Lockdown im Frühjahr haben gezeigt, wie wichtig es ist, mit der Digitalisierung noch zügiger voranzukommen. Hierbei den Datenschutz von Anfang an mitzudenken, ist uns ein wichtiges Anliegen – nicht nur, damit bei Missachtung dieses Grundsatzes später ggf. notwendig werdende umfassende und teure technische Überarbeitungen vermieden werden können, sondern auch, um das notwendige Vertrauen der Bürger*innen bei der Inanspruchnahme digitaler Leistungen nicht zu verspielen. Wir bringen uns daher sowohl im Land Berlin als auch auf der Ebene der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) sehr aktiv in den Prozess der datenschutzrechtlichen Begleitung der Umsetzung von Digitalisierungsprojekten ein.

2.1 Stand der Digitalisierungsprojekte

Der IKT-Basisdienst „Digitaler Antrag" ist in den Regelbetrieb überführt worden. Mit dem „Digitalen Antrag" werden Antragsprozesse von der Antragstellung bis zur Überführung in das jeweilige Fachverfahren durchgeführt. Verwaltungsdienstleistungen können auf diese Weise – wie vom Onlinezugangsgesetz des Bundes (OZG) vorgegeben – weitestgehend elektronisch erbracht werden. Die Senatsverwaltung für Inneres und Sport hat uns in die Konzeption des Digitalen Antrags eingebunden. Wie im letzten Jahr berichtet, begrüßen wir es, dass mit dem Onlinezugangsgesetz Berlin (OZG Bln)[71] die notwendigen Rechtsgrundlagen geschaffen worden sind, die es der Verwaltung erlauben, die bei der Nutzung der IKT-Basisdienste erforderlichen personenbezogenen Daten zu verarbeiteten, ohne dass hier auf Einwilligungen der Bürger*innen zurückgegriffen werden muss.[72] Im Laufe des

70 Zur Digitalisierung der Schulen siehe 1.4

71 Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen der Berliner Verwaltung – Onlinezugangsgesetz Berlin (OZG Bln) vom 4. März 2020

72 JB 2019, 2.1

Jahres hat die Senatsverwaltung für Inneres und Sport diverse Antragsprozesse in das Verfahren des „Digitalen Antrags“ eingestellt.

Bei der Umsetzung des OZG ist das Land Berlin gemeinsam mit dem Bundesministerium des Innern, für Bau und Heimat und den Ländern Brandenburg, Hamburg und Thüringen für das Themenfeld Querschnittsleistungen verantwortlich. Eine besondere Rolle spielt hierbei die Erbringung digitaler Nachweise. Auch darüber haben wir bereits im letzten Jahr berichtet.[73] Während es ursprünglich darum ging, den digitalen Nachweis einer Geburtsurkunde bei der Erbringung einer elektronischen Verwaltungsleistung abzubilden, ist daraus das Umsetzungsprojekt „Basiskomponente Nachweisabruf“ entstanden, in dem durch das Land Berlin Verfahren entwickelt werden, die eine Erbringung von Nachweisen wie den Melderegisterauszug, die Geburtsurkunde oder das Führungszeugnis elektronisch abbilden sollen. Da es hier um eine enge Verzahnung mit bundesrechtlich geregelten Verfahren geht, wie z. B. bei der Beantragung von Wohn- oder Elterngeld, bedarf es einer Abstimmung mit den zuständigen Bundesressorts. Hier spielen insbesondere Fragen zur Einordnung der datenschutzrechtlichen Verantwortlichkeit zwischen dem Bund und den Ländern eine wichtige Rolle.

2.2 Umsetzung des Onlinezugangsgesetzes in Bund und Ländern

Das OZG verpflichtet Bund, Länder und Kommunen, bis Ende 2022 ihre Verwaltungsdienstleistungen über Verwaltungsportale auch online anzubieten. Dieser Zeitrahmen ist ambitioniert. Zusätzlich erhöht die Corona-Pandemie den Druck, einzelne Leistungen sogar noch schneller zu digitalisieren.

Nach einem sog. „Einer-für-alle-Prinzip“ arbeiten Bund und Länder arbeitsteilig an der Umsetzung der Digitalisierung der verschiedenen Verwaltungsdienstleistungen. Die unter der Verantwortung eines Bundeslandes gemeinsam mit dem jeweiligen Bundesressort digitalisierte Verwaltungsdienstleistung soll dann auch von den übrigen Ländern und Kommunen übernommen und implementiert werden können. Wegen der zahlreichen mit der Umsetzung des OZG verbundenen

73 JB 2019, 2.1

Fragestellungen hat die DSK eine Unterarbeitsgruppe eingerichtet, die die Umsetzung im Hinblick auf die Einhaltung der datenschutzrechtlichen Rahmenbedingungen begleiten soll. Wir beteiligen uns aktiv an dieser Unterarbeitsgruppe.

2.3 Registermodernisierung und Datencockpit

In diesem Jahr hat die Bundesregierung die Planungen für eine Registermodernisierung konkretisiert und einen Entwurf für ein Registermodernisierungsgesetz[74] vorgelegt. Ziel ist, die in der Verwaltung geführten Register grundlegend zu modernisieren, um die Bürger*innen davon zu entlasten, selbst Nachweise bei der Inanspruchnahme digitaler Verwaltungsleistungen erbringen zu müssen. Vielmehr soll es möglich sein, diese bei den jeweils anderen Behörden medienbruchfrei zu beschaffen. Hierfür soll die Steuer-ID als einheitliches Personenkennzeichen und registerübergreifendes Ordnungsmerkmal zur Identifikation eingesetzt werden.

Die Verknüpfung der Datenbestände über die Steuer-ID begegnet jedoch erheblichen verfassungsrechtlichen Bedenken. Auf diese Weise wird ein Abgleich verschiedenster Datenbestände möglich und birgt die Gefahr einer Verknüpfung zu einem Persönlichkeitsprofil.[75] Ebenso möglich und aus Datenschutzsicht sehr viel besser geeignet wären bereichsspezifische Kennzeichen. Diese könnten die Risiken für die informationelle Selbstbestimmung der Bürger*innen deutlich reduzieren. Eine Anpassung der Regelungen des Gesetzentwurfs ist daher dringend notwendig.

Wir haben im vergangenen Jahr über unsere Beteiligung an dem Digitalisierungslabor für ein sog. Datencockpit berichtet.[76] Durch dieses Datencockpit sollen Bürger*innen bei der Inanspruchnahme digitaler Verwaltungsleistungen erfahren können, welche ihrer Daten bei den verschiedenen Behörden gespeichert sind

74 Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG), BR-Drs. 563/20

75 Siehe Entschließung der DSK „Registermodernisierung verfassungskonform umsetzen!" vom 26. August 2020; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

76 JB 2019, 2.1

und zwischen diesen ausgetauscht werden können. Dadurch soll eine für die Nutzer*innen größtmögliche Transparenz geschaffen werden. Da Berlin das Themenfeld der Querschnittsleistungen betreut, zu denen auch das Datencockpit zählt, hat uns die für die Entwicklung und Implementierung verantwortliche Senatsverwaltung für Inneres und Sport hinsichtlich der datenschutzrechtlichen Aspekte einbezogen.

Mit den Planungen des Bundes, die Registermodernisierung und damit die Verknüpfung der Datenbestände aus verschiedenen Registern über ein einheitliches Personenkennzeichen umzusetzen, bekommt das Datencockpit auch in diesem Zusammenhang eine wichtige Bedeutung. Die Zusammenführung verschiedener Datenbestände über die Verwendung eines einheitlichen Personenkennzeichens begegnet wegen der damit verbundenen Gefahr der Schaffung von Persönlichkeitsprofilen auch hier verfassungsrechtlichen Bedenken. Als Ausgleichsmaßnahme hierfür soll das Datencockpit nach den Planungen nunmehr auch in diesem Zusammenhang gewährleisten, dass für die Bürger*innen zumindest jederzeit Transparenz über die über sie gespeicherten und zwischen den Registern ausgetauschten Daten besteht. Das Datencockpit soll mit dem derzeit noch im Entwurfsstadium befindlichen Registermodernisierungsgesetz[77] auf eine gesetzliche Grundlage gestellt werden. Dies begrüßen wir. Es ist wichtig, dass das Datencockpit dann auch als wirksames Instrument zügig technisch implementiert wird und die angestrebte Transparenz gewährleistet.

Eine datenschutzgerechte Digitalisierung der Verwaltung ist mit erheblichen Herausforderungen verbunden. Um hier die richtigen Weichen zu stellen, bringen wir uns sowohl in Berlin als auch auf der Ebene der DSK in die Prozessgestaltung ein. Nur wenn die Datenschutzrechte der Bürger*innen von vornherein Berücksichtigung finden, kann das notwendige Vertrauen in die Inanspruchnahme digitaler Verwaltungsleistungen gesichert werden.

77 Siehe Artikel 2 des Entwurfs für ein Registermodernisierungsgesetz, § 10 OZG – BR-Drs. 563/20

3 Inneres und Justiz

3.1 Mangelhafte Zusammenarbeit der Polizei mit unserer Behörde

Bei der Überprüfung von Abfragen personenbezogener Daten in Polizeidatenbanken, die in einem Zusammenhang mit rechtsextremen Morddrohungen stehen konnten, mussten wir einen Verstoß der Polizei gegen deren gesetzliche Pflicht zur Zusammenarbeit mit uns beanstanden.

Anlass der Überprüfung war die Beschwerde einer Person, an deren Wohnhaus die Drohung „9 mm für [...] Kopfschuss" gesprüht war. Diese Person war nach eigenen Angaben bereits vorher Opfer mutmaßlich rechtsextremer Gewalt gewesen. Zur Aufklärung des Sachverhalts baten wir die Polizei im Mai 2019 um eine Prüfung sämtlicher Zugriffe auf Einträge zur beschwerdeführenden Person und zu deren Wohnanschrift in der Polizeidatenbank POLIKS sowie um Übermittlung der entsprechenden Protokollbanddaten nebst Auswertung für einen bestimmten Zeitraum.

Aus der von der Polizei übermittelten Auswertung ging hervor, dass mehrere Mitarbeitende der Polizei auf personenbezogene Daten der betroffenen Person zugegriffen hatten. Einige Zugriffe wurden in der Auswertung näher begründet, andere nicht. Abschließend wurde in der Auswertung ohne nähere Erläuterung festgestellt, dass keine Anhaltspunkte für dienstlich nicht begründbare Anfragen vorlägen. Der anschließenden Bitte, auch die bislang nicht nachvollziehbaren Datenabrufe zu begründen, kam die Polizei trotz mehrerer Mahnschreiben und einem direkten Schreiben an die Polizeipräsidentin, in dem auch angesichts der politischen Tragweite des Verdachts nochmals eindringlich um die erforderlichen Informationen gebeten wurde, nicht nach.

Die Polizei begründete diese Verweigerung damit, dass zuvor die Verfahrensrechte der beteiligten Mitarbeitenden geklärt werden müssten, da insoweit immer auch der Verdacht im Raum stehe, dass in solchen Fällen Mitarbeitende eine Straftat oder Ordnungswidrigkeit begangen haben könnten. Zudem habe der Beschwerde-

führer keine konkreten Anhaltspunkte für eine rechtswidrige Datenverarbeitung durch die Polizei genannt, sondern lediglich vage Vermutungen vorgetragen, weshalb fraglich sei, ob die Beschwerde ausreichend substanziiert sei.

Zu unseren Aufgaben gehört es u.a., die Anwendung der Vorschriften über den Datenschutz zu überwachen und durchzusetzen, sich mit Beschwerden betroffener Personen zu befassen und Untersuchungen über die Anwendung der Vorschriften über den Datenschutz durchzuführen.[78]

Diese Aufgabenerfüllung ist eine gesetzliche Verpflichtung, die nicht von bestimmten Voraussetzungen wie dem Vorliegen konkreter Anhaltspunkte für einen Verstoß gegen Vorschriften über den Datenschutz abhängig ist. Daher ist die Substanziiertheit von Bürger*innenbeschwerden ohne Relevanz für die Informations- und Zusammenarbeitspflichten der Polizei uns gegenüber.

Im vorliegenden Fall ging es um die unserem gesetzlichen Auftrag entsprechende Untersuchung, ob die Polizei bei Datenabrufen in POLIKS die Vorschriften über den Datenschutz ordnungsgemäß angewendet hat. Im Falle unrechtmäßiger Datenabrufe obliegt es uns, die Anwendung der Vorschriften über den Datenschutz durch die Polizei für die Zukunft durchzusetzen. Dies kann z. B. durch eine Verpflichtung der Polizei geschehen, bestimmte technische und organisatorische Maßnahmen wie bspw. eine bessere Protokollierung der Abfragen in POLIKS oder geeignete interne Stichprobenverfahren zur Kontrolle von Zugriffen auf POLIKS o. Ä. zu ergreifen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten.

Zur Erfüllung dieser Aufgaben benötigen wir zunächst Informationen über die Gründe der durchgeführten Abfragen. Anderenfalls können wir nicht prüfen, ob die Abfragen rechtmäßig waren.

Würden die datenschutzrechtlich verantwortlichen Stellen in Fällen wie dem vorliegenden die Auskunft mit Verweis auf Verfahrensrechte ihrer Mitarbeitenden verweigern können, wäre es in den meisten Fällen für uns unmöglich, die Rechtmäßigkeit einer Datenverarbeitung bei diesen Stellen zu prüfen. Denn die

78 § 11 Abs. 1 Satz 1 Nr. 1, 6, 8 Berliner Datenschutzgesetz (BlnDSG)

jeweilige Datenverarbeitung wird grundsätzlich nicht von der jeweiligen Stelle als Institution, sondern von deren Mitarbeitenden durchgeführt. Man kommt bei der Prüfung der Rechtmäßigkeit einer Datenverarbeitung durch eine verantwortliche Stelle also regelmäßig nicht umhin, auch Informationen über die Mitarbeitenden zu erhalten. Demgemäß weit gefasst sind auch unsere Befugnisse. Sie werden gesetzlich nicht von straf- oder ordnungsrechtlichen Verfahrensrechten der betreffenden Mitarbeitenden der verantwortlichen Stelle abhängig gemacht. Beides ist strikt voneinander zu trennen.

Soweit dann zureichende tatsächliche Anhaltspunkte für ein strafbares oder ordnungswidriges Verhalten einzelner Mitarbeiter*innen der Polizei vorliegen, haben diese ab diesem Zeitpunkt selbstverständlich entsprechende Aussage- bzw. Auskunftsverweigerungsrechte. Solche Anhaltspunkte sind jedoch zum einen derzeit nicht erkennbar. Zum anderen haben auch nur die betreffenden Mitarbeitenden diese Rechte, nicht die Polizei als verantwortliche Stelle. Diese bleibt umfassend auskunftsverpflichtet.

Zur Vermeidung einer vorherigen Selbstbelastung der beteiligten Mitarbeiter*innen hatten wir die Polizei zudem darauf hingewiesen, dass für die Beantwortung unserer Fragen auch Ermittlungen zur Klärung des Sachverhalts unabhängig von der Befragung dieser Personen stattfinden könnten. Insbesondere ist es möglich, deren Vorgesetzte zu befragen und Einsicht in die von den Betroffenen zu bearbeitenden Vorgänge zu nehmen. Hierdurch könnte u.a. geprüft werden, ob die betreffenden Mitarbeiter*innen überhaupt zuständig waren für die Bearbeitung der Vorgänge, in die sie Einsicht genommen haben. Weiterhin könnte geprüft werden, aus welchen Gründen sie genau zu diesem Zeitpunkt in die Dateien Einsicht genommen haben.

Wir haben die beharrliche Verweigerung der Polizei, uns bei unserer Arbeit zu unterstützen, beanstandet.[79] Die Polizei ist gesetzlich verpflichtet, uns alle Informationen, die für die Erfüllung unserer Aufgaben erforderlich sind, bereitzustellen.[80]

79 Siehe § 13 Abs. 2 BlnDSG

80 § 13 Abs. 4 Nr. 2 BlnDSG

Sie hat zudem die Pflicht, mit uns bei der Erfüllung unserer Aufgaben zusammenzuarbeiten.[81]

Zwar ist bis heute ungeklärt, ob die fraglichen Datenabfragen rechtmäßig waren, jedoch hat sich die Polizei nach einem Gespräch unserer Hausleitung mit der Polizeipräsidentin zwischenzeitlich – über ein Jahr nach Beginn der Prüfung – bereit erklärt, uns nunmehr bei unserer Überprüfung umfassend zu unterstützen. Wir hoffen jetzt auf eine verbesserte Zusammenarbeit.

3.2 Änderung des Polizeigesetzes

Die Polizei soll neue rechtliche Befugnisse für ihre Arbeit im Bereich der Gefahrenabwehr erhalten.[82] Hierzu gehören u.a. die Einführung von Bodycams und präventiver Telekommunikationsüberwachung. Wir haben zu dem entsprechenden Gesetzentwurf gegenüber dem Parlament Stellung genommen.[83]

Erfreulich ist, dass die geplanten Regelungen im Hinblick auf den Datenschutz sehr ausdifferenziert sind. Sie entsprechen zwar nicht in allen Formulierungen den datenschutzrechtlichen Bestimmungen, jedoch wird der Anspruch sichtbar, diesen gerecht zu werden.

Gleichzeitig ist es jedoch sehr bedauerlich, dass auch mit dem vorliegenden Gesetzentwurf nicht die seit langem notwendigen gesetzlichen Anpassungen des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) an die Richtlinie (EU) 2016/680 (JI-Richtlinie) vorgenommen werden.[84] Ebenso wenig ist die Anpassung des ASOG an das novellierte Berliner Datenschutzgesetz (BlnDSG) vorgesehen.

81 § 54 BlnDSG

82 Siehe Entwurf des dreiundzwanzigsten Gesetzes zur Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes und anderer Gesetze, Abghs-Drs. 18/2787 vom 12. Juni 2020

83 Gemäß § 11 Abs. 2 BlnDSG

84 Gemäß Art. 63 Abs. 1 Satz 1 JI-Richtlinie mussten die Mitgliedsstaaten bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften erlassen und veröffentlichen, die erforderlich sind, um dieser Richtlinie nachzukommen.

Dies führt zu praktischen Anwendungsproblemen, bspw. hinsichtlich der Betroffenenrechte.[85]

In unserer Stellungnahme zum Gesetzentwurf haben wir u.a. darauf hingewiesen, dass es unrechtmäßig ist, einmal mittels Bodycam begonnene Bild- und Tonaufnahmen durch die Polizei unterschiedslos bis zum Abschluss der polizeilichen Maßnahmen fortzuführen. In der Gesetzesbegründung wird hierzu erläutert, dass nur so das Einsatzgeschehen umfassend beurteilt werden könne, wobei das „Geschehen" insoweit nicht eng zu verstehen sei. Die pauschale Fortführung von Bild- und Tonaufnahmen zur Erfassung des gesamten Einsatzgeschehens, das unter Umständen sehr lange andauern kann, ohne dass die ursprüngliche Gefahr noch besteht und ohne dass dies für eine nachträgliche Überprüfung einer polizeilichen Maßnahme notwendig ist, ist insbesondere im Hinblick auf die Eingriffstiefe von Bild- und Tonaufnahmen für alle Geschehensbeteiligten und auch etwaige unbeteiligte Dritte unverhältnismäßig und somit unzulässig.

Hinsichtlich des Einschaltens einer Bodycam haben wir gefordert, dass zur ausreichenden Gewährleistung der Transparenz einer Datenverarbeitung hierauf immer vorab hingewiesen werden müsste. Denn nur dadurch können Betroffene reagieren und von ihren Rechten Gebrauch machen. Gleichzeitig sollte bei Aktivierung einer Bodycam ein optisches Signal erkennbar sein, z. B. ein rotes Licht, das die Aufnahme anzeigt.

Den geplanten Dauerbetrieb von im Einsatz befindlichen Bodycams mittels einer sog. Pre-Recording-Funktion[86] haben wir als europarechtswidrig kritisiert. Er widerspricht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit, wonach eine Datenverarbeitung nur erlaubt ist, wenn dies konkret für die Aufgabenerfüllung der verantwortlichen Stelle erforderlich ist.[87]

Die Vorabaufnahme unabhängig von einer konkreten Aufgabenerfüllung wird mit einer technischen Erforderlichkeit begründet, die hingegen nicht existiert. Nach

85 Hierzu gibt es derzeit zwei unterschiedliche Regelungen – § 50 ASOG und § 43 BlnDSG.

86 Die Bodycams sollen in einer Endlosschleife alles im Sichtbereich aufzeichnen und nach spätestens 30 Sekunden wieder löschen, unabhängig davon, ob es für die Datenerhebung und -speicherung einen tatsächlichen Anlass gibt.

87 Siehe Art. 8 Abs. 1 JI-Richtlinie, der bereits in § 33 Abs. 1 BlnDSG umgesetzt wurde

der Gesetzesbegründung sollen Verzögerungen nach dem Auslösen der Aufzeichnung durch ein Hochfahren der Kamera verhindert werden. Moderne Kameras können jedoch im Standby-Modus[88] bereitstehen und sofort eingeschaltet werden, ohne dass eine Zeitverzögerung entsteht. Die Kamera ist in diesem Fall nur temporär deaktiviert, ähnlich wie bei einer Pause-Taste, und kann jederzeit ohne zeitliche Verzögerung in den Aktivierungsmodus geschaltet werden. Eine solche Technik verwendet bspw. die Deutsche Bahn. Dass ein Hochfahren einer Kamera vor ihrer Einsatzmöglichkeit nicht mehr dem Stand der Technik entspricht, können zudem alle prüfen, die bei ihrem Smartphone die Kamera einschalten.

Die geplanten Gesetzesänderungen geben der Polizei neue Datenverarbeitungsbefugnisse, die gerade im Hinblick auf ihre tatsächliche Erforderlichkeit zu beobachten sind. Daher ist es begrüßenswert, dass der Nutzen dieser Befugnisse in der Praxis laut Gesetzentwurf unabhängig wissenschaftlich evaluiert werden soll und sich das Parlament danach nochmals hiermit auseinandersetzen wird.

3.3 Einführung einer bzw. eines Bürger- und Polizeibeauftragten

Aus der Praxis

Im Land Berlin ist die Position einer oder eines Bürger- und Polizeibeauftragten eingeführt worden.[89] Ziel war die Schaffung einer externen Ombudsstelle, d. h. einer unparteiischen Schiedsstelle, die behördliche Vorgänge unabhängig im Interesse der Bürgerinnen und Bürger kontrollieren soll.

Vorbild für das neue Amt sind laut Gesetzesbegründung entsprechende Regelungen in Rheinland-Pfalz.[90] Allerdings wurden die dortigen Regelungen an entscheidenden Stellen zunächst nicht im Berliner Gesetzgebungsvorhaben berücksich-

88 Auch Bereitschafts- oder Wartefunktion genannt

89 Bürger- und Polizeibeauftragtengesetz (BürgBG)

90 Landesgesetz über den Bürgerbeauftragten des Landes Rheinland-Pfalz und den Beauftragten für die Landespolizei (BürgBG RP)

tigt. Hierzu haben wir im Rahmen einer Anhörung im Abgeordnetenhaus Stellung genommen.[91]

Nach dem ursprünglichen Gesetzentwurf[92] sollte die bzw. der Bürger- und Polizeibeauftragte die Arbeit des Petitionsausschusses des Abgeordnetenhauses unterstützen und ihre oder seine Aufgabe als Hilfsorgan des Abgeordnetenhauses bei der Ausübung der parlamentarischen Kontrolle wahrnehmen. Gleichzeitig sollte die bzw. der Bürger- und Polizeibeauftragte aber als oberste Landesbehörde eingerichtet werden. Es war nicht erkennbar, ob die Institution Teil der Exekutive oder der Legislative sein sollte. Wir hatten gefordert, dies im Gesetz klarzustellen. Nunmehr ist geregelt, dass die bzw. der Bürger- und Polizeibeauftragte als Hilfsorgan des Abgeordnetenhauses bei der Ausübung parlamentarischer Kontrolle fungiert, jedoch keine oberste Landesbehörde ist.[93] Damit wurde klargestellt, dass die Einrichtung Teil der Legislative ist.

In diesem Zusammenhang war auch anzumerken, dass die anfänglich geplante Organisation der oder des Bürger- und Polizeibeauftragten als oberste Landesbehörde der Behördenstruktur des Landes Berlin zuwiderlaufen würde. In Berlin sind nur der Senat, der Rechnungshof und die/der Berliner Beauftragte für Datenschutz und Informationsfreiheit oberste Landesbehörden. Diese Behörden haben Verfassungsrang.[94] Die Einrichtung des Amtes der oder des Bürger- und Polizeibeauftragten als oberste Landesbehörde hätte nicht dieser verfassungsrechtlichen Struktur entsprochen.

Wie das Beispiel Rheinland-Pfalz zeigte, gab es jedoch auch andere Wege, um eine größtmögliche Unabhängigkeit der Institution zu erreichen. Das Land Rheinland-Pfalz hat seine Bürgerbeauftragte als ständige Beauftragte des Petitionsausschusses organisiert.[95] Die Beauftragte für die Landespolizei nimmt ihre Aufgabe als Hilfsorgan des Landtags bei der Ausübung parlamentarischer Kontrolle

91 Gemäß § 11 Abs. 2 BlnDSG

92 Siehe Entwurf des Gesetzes zur Einführung des oder der Bürgerbeauftragten des Landes Berlin und des oder der Beauftragten für die Polizei Berlin, Abghs-Drs. 18/2426 vom 21. Januar 2020

93 § 1 Abs. 2 und § 3 BürgBG

94 Siehe Art. 47, 67 und 95 der Verfassung von Berlin (VvB)

95 Siehe § 4 Satz 1 BürgBG RP

wahr und ist in der Ausübung ihres Amtes unabhängig, weisungsfrei und nur dem Gesetz unterworfen.[96] Die Beauftragten stehen in einem öffentlich-rechtlichen Amtsverhältnis zum Land Rheinland-Pfalz, sind jedoch nicht als oberste Landesbehörde eingerichtet.[97] Diese Regelungen entsprechen im Übrigen denen zur Wehrbeauftragten des Deutschen Bundestages[98], die als Teil der Legislative gilt.[99] In der letztlich beschlossenen Version des Gesetzes hat sich der Gesetzgeber diesen Beispielen angeschlossen.

Der uns im Rahmen der Anhörung vorgelegte Gesetzentwurf zur Einrichtung der bzw. des Bürger- und Polizeibeauftragten in Berlin enthielt darüber hinaus auch sehr weitgehende Befugnisse hinsichtlich der Datenverarbeitung, die näher bestimmt und eingegrenzt werden mussten. Es fehlten bspw. Bestimmungen zum Umgang mit sensitiven Daten, die regelmäßig im Zusammenhang mit Beschwerden über die Polizei, aber auch über Gesundheits- und Sozialbehörden anfallen. Zudem fehlten Regelungen zu Betroffenenrechten wie etwa Löschpflichten. Auch fehlte für öffentliche Stellen eine Befugnisnorm, die es diesen erlaubt, personenbezogene Daten an die oder den Bürger- und Polizeibeauftragten zu übermitteln. Auch insofern wurden unsere Einwände berücksichtigt: Sensitive Daten dürfen nunmehr nur verarbeitet werden, soweit ein erhebliches öffentliches Interesse dies erfordert.[100] Es wurde eine Datenübermittlungsbefugnis für öffentliche Stellen geschaffen.[101] Im Übrigen wird jetzt auf die Regelungen der Datenschutz-Grundverordnung (DS-GVO) und des BlnDSG verwiesen, sodass die Anwendung der dortigen Betroffenenrechte gewährleistet ist.[102]

Weiterhin sollten alle Landesbehörden verpflichtet werden, der oder dem Bürger- und Polizeibeauftragten bei der Durchführung der erforderlichen Erhebungen Amtshilfe zu leisten. Nach dem Wortlaut wäre hiervon auch die Berliner Beauftragte für Datenschutz und Informationsfreiheit umfasst gewesen. Dies hätte

96 § 16 Abs. 2 BürgBG RP

97 § 10 Abs. 1, § 17 BürgBG RP

98 Siehe § 1 Abs. 1, § 14 Abs. 3, § 15 Abs. 1 des Gesetzes über den Wehrbeauftragten des Deutschen Bundestages (WbeauftrG)

99 Siehe Maunz/Dürig/Klein, Grundgesetz, Art. 45b, Rn. 13, 14 mwNw

100 § 5 Abs. 1 Satz 2 BürgBG

101 § 5 Abs. 2 BürgBG

102 § 5 Abs. 3 BürgBG

aber im Widerspruch zu den datenschutzrechtlichen Vorgaben gestanden, wonach die oder der Beauftragte weder direkter noch indirekter Beeinflussung von außen unterliegt, weder um Weisung ersucht noch Weisungen entgegennimmt und verpflichtet ist, über die ihr oder ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren.[103] Auch insoweit ist nunmehr klargestellt worden, dass die Rechtsstellung unserer Behörde unberührt bleibt.[104]

Die Einführung einer oder eines Bürger- und Polizeibeauftragten ist zu begrüßen, weil sie zur Stärkung der parlamentarischen Kontrolle und der Rechte der Bürgerinnen und Bürger im Verhältnis zur Polizei und zu anderen Behörden führen kann. Es ist sehr erfreulich, dass unsere Bedenken hinsichtlich des ursprünglichen Gesetzentwurfs aufgenommen wurden und die verfassungs- und datenschutzrechtlichen Aspekte nunmehr hinreichend Berücksichtigung finden.

3.4 Eigenes Versammlungsgesetz für Berlin

Mit der Föderalismusreform im Jahr 2006 wurde die Gesetzgebungskompetenz für das Versammlungsrecht auf die Bundesländer verlagert. Bislang hat Berlin nur im Hinblick auf die Anfertigung von Bild- und Tonaufnahmen bei öffentlichen Versammlungen unter freiem Himmel und Aufzügen hiervon Gebrauch gemacht.[105] Nun soll das gesamte Versammlungsrecht in Berlin neu geregelt werden.[106]

Wir haben zu dem Gesetzentwurf gegenüber dem Parlament u.a. wie folgt Stellung genommen:[107]

103 § 10 Abs. 2, Abs. 5 BlnDSG, Art. 52 Abs. 1, 2 DS-GVO

104 § 6 Satz 2 BürgBG

105 Gesetz über Aufnahmen und Aufzeichnungen von Bild und Ton bei Versammlungen unter freiem Himmel und Aufzügen (VersAufn/AufzG)

106 Entwurf des Gesetzes über die Versammlungsfreiheit im Land Berlin (VersFG-E), Abghs-Drs. 18/2764 vom 2. Juni 2020

107 Gemäß § 11 Abs. 2 BlnDSG

Der Europäische Gerichtshof für Menschenrechte (EGMR) misst dem friedlichen, politischen und gewerkschaftlichen Protest für den demokratischen Prozess eine große Bedeutung bei und stellte in einer Entscheidung im Jahr 2019 entsprechend hohe Anforderungen an die Verarbeitung von Daten durch die britische Polizei.[108]

Personenbezogene Daten, die im Zusammenhang mit Versammlungen verarbeitet werden, unterfallen regelmäßig besonders geschützten Kategorien. Sie können insbesondere Auskunft über die ethnische Herkunft, über politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, aber auch über die Gesundheit oder die sexuelle Orientierung geben und haben aufgrund ihrer Sensitivität einen erhöhten Schutzbedarf.

Der EGMR betont in seiner o. g. Entscheidung, dass die Speicherung solcher Daten durch Behörden eine abschreckende Wirkung („chilling effect") haben kann, sich politisch zu beteiligen.[109] Die Mitgliedschaft oder Zugehörigkeit zu einer Gruppe oder Bewegung sollte deshalb nur erfasst werden, wenn dies für eine spezifische Überprüfung notwendig ist.[110] Dabei gesteht der EGMR den nationalen Behörden bei der Beurteilung der Notwendigkeit einen weiten Einschätzungsspielraum zu.[111]

Unter Berücksichtigung dieser europäischen Rechtsprechung ist zu kritisieren, dass im Berliner Gesetzentwurf eine zweckändernde Nutzung der unter engen Voraussetzungen zu Gefahrenabwehrzwecken bei einer Versammlung erhobenen Daten auch zur Durchführung von Bußgeldverfahren zulässig sein soll. Denn hierdurch besteht die Gefahr, dass etwa durch die zusätzliche Nutzung von Bild- und Tonaufnahmen für die Aufklärung minder schwerer Vergehen quasi durch die Hintertür genau die abschreckende Wirkung entstehen könnte, die Personen davon abhält, sich politisch zu beteiligen.

Auch die derzeit vorgesehene Weiterverarbeitung von rechtmäßig erhobenen Versammlungsdaten allein zu Dokumentationszwecken ist zu kritisieren. Das Erfordernis der Datenverarbeitung zu diesem Zweck ist nicht ersichtlich. Wenn eine

108 Siehe EGMR, Urteil vom 24. Januar 2019, CATT v. THE UNITED KINGDOM (Application no. 43514/15)

109 Rn. 123 der Entscheidung

110 Rn. 124 der Entscheidung

111 Rn. 118 der Entscheidung

Gefahr eingetreten, also eine Störung gegeben ist, löst diese regelmäßig nur noch repressives Tätigwerden der Polizei aus. Für diesen konkreten Zweck ist die weitere Datenverarbeitung aber bereits erlaubt.[112]

Geplant ist auch, dass die Versammlungsbehörde Kontaktdaten des Leitungspersonals von Versammlungen gemeinsam mit Informationen zum Verlauf der Versammlung unterschiedslos zwei Jahre nach Abschluss der Versammlung für die Beurteilung einer Gefahrenlage bei zukünftigen Versammlungen weiterverarbeiten kann.[113] Das verstößt in der vorliegenden Form gegen den rechtsstaatlichen Grundsatz der Erforderlichkeit. Die Regelung beachtet zudem nicht, dass personenbezogene Daten, die sich auf Versammlungen beziehen, in der Regel sensitiv und somit besonders schutzbedürftig sind.

Die Versammlungsbehörde erhebt die vorgenannten Kontaktdaten, um Hilfeleistungen während der Versammlung vorbereiten und in Gefahrenfällen schnell und effizient handeln zu können. Dieser Vorsorgebedarf endet grundsätzlich mit dem Ende der jeweiligen Versammlung. Eine längere Speicherung zu Zwecken der Vorbereitung auf die Gefahrenlage bei zukünftigen Versammlungen kann erforderlich sein. Hierfür müssen aber auch konkrete Anhaltspunkte dafür vorliegen, dass die für die stattgefundene Versammlung verantwortlichen Personen in absehbarer Zeit eine ähnliche Versammlung durchführen werden. Ist etwa aufgrund der Thematik einer Versammlung (z. B. „75 Jahre Kriegsende“) klar, dass diese nur einmalig stattfindet, ist eine weitere Speicherung der Daten nicht erforderlich. Andererseits finden bestimmte Versammlungen wie z. B. Mahnwachen möglicherweise auch so häufig statt, dass es bereits ausreicht, das Verhalten von anmeldenden und/oder leitenden Personen der Versammlungen sowie den Verlauf der jeweiligen Versammlung innerhalb eines Jahres zu kennen.

Im Gesetz soll zudem geregelt werden, dass unsere Behörde und die oder der behördliche Datenschutzbeauftragte der Polizei die Einhaltung der polizeilichen Dokumentationspflichten im Zusammenhang mit der Verarbeitung von Versammlungsdaten überprüfen kann.[114] Nach dem BlnDSG sind wir jedoch befugt, sämt-

112 § 18 Abs. 3 Satz 1 Nr. 1 VersFG-E
113 § 30 Abs. 2 VersFG-E
114 § 18 Abs. 6 VersFG-E

liche Datenverarbeitungsvorgänge öffentlicher Stellen in Berlin zu überprüfen.[115] Die Regelung im vorliegenden Gesetzentwurf ist insofern missverständlich und aufgrund der Regelungen im BlnDSG auch überflüssig. Gleiches gilt für die Befugnisse der oder des behördlichen Datenschutzbeauftragten der Polizei.[116] Wir haben daher die Streichung der Regelung gefordert.

Die Verarbeitung personenbezogener Daten im Zusammenhang mit Versammlungen unterliegt aufgrund der Sensitivität dieser Daten i. V. m. der verfassungsrechtlich garantierten Versammlungsfreiheit sehr strengen Voraussetzungen, die bei entsprechenden gesetzlichen Regelungen berücksichtigt werden müssen.

3.5 Unrechtmäßige Datenverarbeitung zu Sinti und Roma

In der Veröffentlichung der Polizeilichen Kriminalstatistik (PKS) 2017 hieß es auf Seite 48: „Im Bereich des Trickdiebstahls waren von 86 Tatverdächtigen 53 Sinti und Roma."[117] Wir haben aufgrund einer Eingabe die Verarbeitung personenbezogener Daten zu den Ethnien Sinti und Roma bei der Polizei geprüft.

Die Polizei erklärte zunächst, die Angabe in der PKS 2017 beruhe auf der fachlich fundierten Einschätzung der Fachdienststelle. Eine systematische Zuordnung Tatverdächtiger zur Bevölkerungsgruppe der Sinti und Roma erfolge grundsätzlich nicht. Allenfalls im Rahmen polizeilicher Sachbearbeitung komme es vereinzelt zur Verarbeitung von Daten über die Ethnie, etwa wenn sich Personen bei Vernehmungen selbst als Sinti, Roma, Jenische oder auch „Zigeuner" bezeichneten. Solche Angaben würden aber nicht systematisch und suchfähig dokumentiert sowie gespeichert, sondern nur im Wortprotokoll erfasst und würden so Teil des Vorgangs.

115 § 11 Abs. 1 Satz 1 Nr. 1, 8 BlnDSG

116 Siehe § 6 Abs. 1 Nr. 2 BlnDSG

117 Diese Passage wurde zwischenzeitlich am 15. Januar 2020 aufgrund einer Weisung des Senators für Inneres und Sport, Andreas Geisel, in der Online-Version der PKS 2017 gestrichen.

Daraufhin führten wir eine Prüfung bei der Polizei durch, um die Verwendung der Begriffe „Jenische", „Roma", „Sinti" und „Zigeuner" in Vorgängen aus dem Jahr 2017 stichprobenartig zu kontrollieren. Es stellte sich heraus, dass von den im Jahr 2017 abgeschlossenen Vorgängen mit der Ereignisbezeichnung „Trickdiebstahl in Wohnung" 31 einen oder mehrere der Begriffe „Roma", „Sinti" und „Zigeuner" enthielten. Die Nennung war größtenteils auf zitierte bzw. wiedergegebene Zeugen- oder Beschuldigtenaussagen zurückzuführen. Doch auch Dokumente ohne unmittelbaren Bezug zu Zeugen- oder Beschuldigtenaussagen, wie etwa die von den ermittelnden Mitarbeiter*innen der Polizei zusammengefassten Sachverhalte in den Strafanzeigen, Durchsuchungs-, Zwischen- oder Schlussberichten an die Staatsanwaltschaft, enthielten o. g. Begriffe ohne erkennbare Erforderlichkeit.

Gemäß § 33 Abs. 1 BlnDSG dürfen Gefahrenabwehr- und Strafverfolgungsbehörden besondere Kategorien personenbezogener Daten nur verarbeiten, wenn dies zu deren Aufgabenerfüllung oder zur Wahrung lebenswichtiger Interessen einer natürlichen Person erforderlich ist oder sich die Verarbeitung auf Daten bezieht, die von der betroffenen Person offensichtlich öffentlich gemacht wurden. Die ethnische Zugehörigkeit gehört zu den besonderen Kategorien personenbezogener Daten.[118]

Für die Erfüllung der Aufgabe „Strafverfolgung" dürfen Strafverfolgungsbehörden personenbezogene Daten in Dateien speichern, verändern und nutzen, soweit dies für die Zwecke des Strafverfahrens erforderlich ist.[119] Für die Aufgabe „Gefahrenabwehr" können Polizei- und Ordnungsbehörden rechtmäßig erhobene personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit das zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist.[120]

Bei der Beurteilung der Erforderlichkeit der Datenverarbeitung zur vorgenannten Aufgabenerfüllung ist danach zu differenzieren, welcher Begriff verwendet wird, auf wen die Verwendung des Begriffs zurückzuführen ist (Polizei oder Dritte, ins-

118 Siehe § 31 Nr. 14 lit. a BlnDSG
119 § 483 Abs. 1 StPO
120 § 42 Abs. 1 ASOG

besondere Zeug*innen und Beschuldigte) und an wen sich der jeweilige Text (Polizei, Staatsanwaltschaft) richtet:

Die Worte „Zigeuner*in“ und „Landfahrer*in“ sind grundsätzlich unzulässig und aus allen Vorgängen zu entfernen. Lediglich als deutlich gekennzeichnete Zitate können sie ausnahmsweise in Vorgängen stehen, sofern sie ermittlungsrelevant sind.

Für die Begriffe Sinti und Roma gilt:

- Ihre Verwendung in Schlussberichten an die Staatsanwaltschaft ist unzulässig, da die Staatsanwaltschaft die Taten, nicht jedoch die verdächtigten Personen bewertet.

- Ihre Verwendung in Sachverhalten in Strafanzeigen, Vermerken, Zwischenberichten ist ausnahmsweise zulässig,

    - wenn das Merkmal konkret ermittlungs- oder fahndungsfördernde Anhaltspunkte liefert, z. B. Aufenthaltsort oder Bandenstruktur. Die Zuordnung sollte immer nur anhand verbindlicher Kriterien bzw. Anleitungen und nur von entsprechend geschulten Beamtinnen und Beamten vorgenommen werden. Ein sog. „Racial Profiling“ muss unbedingt vermieden werden;
    - wenn die Kenntnis der ethnischen Zugehörigkeit der Opfer und/oder Tatverdächtigen bei Verdacht einer aus fremdenfeindlichen oder rassistischen Motiven begangenen Straftat (§ 130 StGB) für deren exakte Beurteilung relevant ist.

- Ihre Verwendung als Selbstzuschreibungen der Betroffenen oder als wörtliche Wiedergabe von Aussagen Dritter, etwa in Vernehmungsprotokollen oder Gutachten, ist zulässig.

Die Kenntnis der ethnischen Zugehörigkeit verdächtiger oder geschädigter Personen ist also regelmäßig für die polizeiliche Arbeit nicht erforderlich und allenfalls in Ausnahmefällen zulässig. Hinsichtlich all dieser Ausnahmetatbestände trägt die Polizei die Beweislast.

Soweit die Polizei die Erforderlichkeit der Datenverarbeitung zu Sinti und Roma für ihre Aufgabenerfüllung in den von uns geprüften Fällen nicht nachweisen konnte, haben wir eine Beanstandung ausgesprochen.[121] Zudem haben wir die Polizei um selbstständige Prüfung der sonstigen polizeilichen Datenbestände auf rechtswidrige Datenverarbeitung im Zusammenhang mit der Ethnie der Sinti und Roma sowie ggfs. um entsprechende Bereinigung dieser Datenbestände gebeten.

3.6 Unerlaubtes Abfotografieren von Personalausweis oder Reisepass durch die Polizei

Ein Bürger hat sich bei uns darüber beschwert, dass bei einer Zeugenaussage im Zusammenhang mit der Anzeige einer Ruhestörung bei der Polizei sein Personalausweis ohne seine Zustimmung mit einem Smartphone abfotografiert wurde.

Die Polizei teilte uns mit, dass die Ausweisdaten für die gerichtsfeste Dokumentation des Einsatzes benötigt würden. Das Abfotografieren des Personalausweises habe die Arbeit vereinfacht. Beim Abschreiben von Ausweisdaten komme es immer wieder zu Fehlern. Durch das Abfotografieren des Personalausweises sollte vermieden werden, dass fehlerhafte Daten in der Polizeidatenbank gespeichert werden. Außerdem habe die Polizei so weniger Zeit für die Datenerfassung benötigt. Eine Rechtsgrundlage für ihr Handeln konnte die Polizei nicht nennen. Das Foto war von der Polizei nach dem Übertragen der Daten in die Polizeidatenbank gelöscht worden.

Die Polizei hat das Recht, zur Erfüllung der ihr übertragen Aufgaben die Identität von Personen festzustellen und die dabei erhobenen personenbezogenen Daten zu speichern.[122] Bürger*innen müssen nach Aufforderung einer zur Identitätsfeststellung berechtigten Behörde wie der Polizei ihren Personalausweis vorlegen.[123]

121 Siehe § 13 Abs. 2 BlnDSG
122 §§ 21 Abs. 1, 42 Abs. 1 ASOG
123 § 1 Abs. 1 S. 1, 2 Personalausweisgesetz (PAuswG)

Das Abfotografieren des Personalausweises ist dabei jedoch nur in engen Grenzen zugelassen. Mitarbeitende der Polizei müssen, bevor sie einen Personalausweis zur Identitätsfeststellung abfotografieren, die Zustimmung der Ausweisinhaberin bzw. des Ausweisinhabers einholen.[124] Die betroffene Person kann zudem verlangen, dass bestimmte Daten nach dem Abfotografieren unkenntlich gemacht werden.[125]

Wir haben gegenüber der Polizei wegen des Abfotografierens des Personalausweises ohne die Zustimmung des Betroffenen eine Mangelfeststellung[126] ausgesprochen. Mitarbeitende der Polizei dürfen den Personalausweis nur mit Zustimmung der Ausweisinhaberin bzw. des Ausweisinhabers abfotografieren. Das Abschreiben der Identitätsdaten vom Personalausweis ist weiterhin auch ohne Zustimmung möglich, soweit dies für polizeiliche Aufgaben erforderlich ist.

3.7 Speicherung von Daten im Melde-, Pass- und Personalausweisregister

Aus der Praxis

Es erreichten uns wieder zahlreiche Beschwerden und Anfragen zu der Speicherung von personenbezogenen Daten in behördlichen Registern, insbesondere im Melde-, Pass- und Personalausweisregister.[127]

Grundsätzlich dürfen die zuständigen Behörden nur dann personenbezogene Daten speichern, wenn eine gesetzliche Regelung dies vorsieht. Je nach Art des Behördenregisters existieren spezifische Gesetze, die die Datenverarbeitung jeweils anordnen. So wird durch das Bundesmeldegesetz (BMG) bestimmt, welche Angaben zu einer Person im Melderegister gespeichert werden dürfen. Der Umfang der im Pass- bzw. Personalausweisregister zu speichernden Daten wird dagegen im Passgesetz (PassG) bzw. Personalausweisgesetz (PAuswG) festgelegt. Diese

124 § 20 Abs. 2 Satz 1 PAuswG
125 § 20 Abs. 2 Satz 3 PAuswG
126 Siehe § 13 Abs. 2 Satz 2 BlnDSG
127 Siehe zur Datenverarbeitung im Melderegister bereits JB 2019, 3.5

drei behördlichen Dateisysteme sind keine öffentlichen Register, sondern für behördliche Zwecke bestimmt.[128]

Die Melderegister werden von den Meldebehörden geführt, deren Aufgabe es ist, die in ihrem Zuständigkeitsbereich wohnenden Personen zu registrieren, um deren Identität und Wohnungen feststellen sowie nachweisen zu können.[129] Welche personenbezogenen Daten die Meldebehörden zur Erfüllung ihrer Aufgaben im Melderegister speichern dürfen, wird durch § 3 BMG abschließend festgelegt.[130] Die zu speichernden Melderegisterdaten lassen sich in drei Gruppen aufteilen: Die Grunddaten[131], die Spezialdaten[132] sowie die Hinweisdaten, die zum Nachweis der Richtigkeit der Grund- und Spezialdaten verarbeitet werden.

Grunddaten im Zuständigkeitsbereich der Meldebehörde sind u.a. Familienname, Doktorgrad, Geburtsdatum und Geburtsort, Geschlecht, Angaben zum gesetzlichen Vertreter, derzeitige Staatsangehörigkeit(en) und derzeitige sowie frühere Anschrift(en). Diese Daten dürfen zur Durchführung der den Meldebehörden zugewiesenen Aufgaben[133] gespeichert und nach Maßgabe spezifischer Melderechtsvorschriften verwendet werden. Demgegenüber ist die Verarbeitung der Spezialdaten an die im Gesetz genannten konkreten Unterstützungsaufgaben der Meldebehörde gebunden (z. B. im Zusammenhang mit der Vorbereitung und Durchführung von Wahlen und Abstimmungen). Eine Verarbeitung anderer als der im BMG und den Ausführungsregelungen vorgesehenen Daten im Melderegister ist grundsätzlich unzulässig. Sie sind daher von der Meldebehörde unverzüglich zu löschen.[134]

128 Trotz dieses internen Charakters können bei Vorliegen bestimmter Voraussetzungen Auskünfte an private oder öffentliche Stellen erteilt werden; siehe z. B. §§ 34, 44 BMG.

129 § 2 Abs. 1 BMG

130 Weitere Daten bzw. Hinweise dürfen nur auf der Grundlage von § 55 Abs. 1 BMG i.V.m. § 2 Berliner Ausführungsgesetz zum Bundesmeldegesetz (BlnAGBMG) gespeichert werden.

131 Siehe § 3 Abs. 1 Nummer 1 bis 19 BMG

132 Siehe § 3 Abs. 2 BMG

133 Gemäß § 2 Abs. 1 und 3 BMG sind dies: Identitätsfeststellung und Wohnungsnachweis, Erteilung von Melderegisterauskünften, Datenübermittlungen an andere öffentliche Stellen sowie Mitwirkungstätigkeiten (Annexaufgaben).

134 § 14 Abs. 1 Satz 2 BMG

Die Führung der Passregister ist Aufgabe der Passbehörden.[135] Sie dienen einerseits der Ausstellung der Pässe und der Feststellung ihrer Echtheit und andererseits der Identitätsfeststellung der Person, die den Pass besitzt oder für die er ausgestellt ist.[136] Der Inhalt ist im Gesetz abschließend bestimmt.[137] Demnach dürfen sie neben dem Lichtbild und der Unterschrift der Passinhaberin bzw. des Passinhabers sowie verfahrensbedingten Bearbeitungsvermerken u.a. folgende Daten enthalten: Namen, Doktorgrad, Tag und Ort der Geburt, Geschlecht, Größe sowie Farbe der Augen, gegenwärtige Anschrift, Staatsangehörigkeit, Seriennummer des Passes, Gültigkeitsdatum und Angaben zu gesetzlichen Vertreter*innen. Ähnlich dem Melderegister ist bei den verarbeiteten Daten zwischen den vorgenannten Grunddaten einerseits und Hinweisen bzw. „verfahrensbedingten Bearbeitungsvermerken" andererseits zu unterscheiden. Letztere haben die Funktion von Hilfsdaten, um den Nachweis der Richtigkeit der im Pass enthaltenen Angaben zu ermöglichen. Hierzu zählen insbesondere Aktenzeichen, Urkunden und andere Nachweise, die im Rahmen der Passbeantragung und -ausstellung anfallen.[138]

Passbehörden sind verpflichtet, die Daten im Passregister mindestens bis zur Ausstellung eines neuen Passes, bei verloren gegangenen Dokumenten jedoch darüber hinaus für den Fall aufzubewahren, dass das verlorene Dokument wiederauftaucht und zugeordnet werden muss. Spätestens fünf Jahre nach dem Ablauf der Gültigkeit des Passes sind zumindest bestimmte Angaben wie das Lichtbild, die Unterschrift und die verfahrensbedingten Hinweise zu löschen.[139]

Die Personalausweisregister schließlich werden von den für Ausweisangelegenheiten zuständigen Personalausweisbehörden geführt und dienen der Durchführung des PAuswG, insbesondere der Ausstellung der Ausweise und der Feststellung ihrer Echtheit und der Identitätsfeststellung der Person, die den Ausweis besitzt oder für die er ausgestellt ist.[140] Das Personalausweisregister darf neben

135 § 21 Abs. 1 PassG
136 § 21 Abs. 3 PassG
137 § 21 Abs. 2 Nr. 1 bis 16 PassG
138 Siehe hierzu auch Ziff. 21.2.1 Allgemeine Verwaltungsvorschrift zur Durchführung des Passgesetzes (PassVwV)
139 § 21 Abs. 4 Satz 1 PassG
140 § 23 Abs. 2 PAuswG

dem Lichtbild, der Unterschrift der Ausweisinhaberin oder des Ausweisinhabers sowie verfahrensbedingten Bearbeitungsvermerken ausschließlich die im Gesetz aufgeführten Daten enthalten.[141] Diese sind z. B. Familienname und Geburtsname, Vornamen, Doktorgrad, Tag und Ort der Geburt, Größe, Farbe der Augen, Anschrift, Staatsangehörigkeit, letzter Tag der Gültigkeitsdauer und ausstellende Behörde. Ebenso wie beim Passregister handelt es sich bei den gespeicherten Informationen um Grunddaten und verfahrensbedingte Bearbeitungsvermerke. Die Verwendung der im Personalausweisregister verarbeiteten Daten steht unter dem Vorbehalt einer Erlaubnisnorm.[142] Personenbezogene Daten im Personalausweisregister sind mindestens bis zur Ausstellung eines neuen Ausweises, höchstens jedoch bis zu fünf Jahre nach dem Ablauf der Gültigkeit des Ausweises, auf den sie sich beziehen, zu speichern und dann zu löschen.[143]

Welche Daten in den Melde-, Pass- und Personalausweisregistern gespeichert werden, ist in erster Linie durch bundesgesetzliche Vorschriften geregelt und wird zum Teil durch Landesausführungsbestimmungen ergänzt. Soweit die jeweiligen Fachgesetze keine speziellen Regelungen treffen, gelten für die Führung der Register die Beschränkungen und Vorgaben der Datenschutz-Grundverordnung (DS-GVO), des Bundesdatenschutzgesetzes (BDSG) bzw. des Berliner Datenschutzgesetzes (BlnDSG) über technische und organisatorische Maßnahmen.[144] Die IT-Verfahrensverantwortung für das zentrale elektronische Melde-, Pass- und Personalausweisregister liegt in Berlin beim Landesamt für Bürger- und Ordnungsangelegenheiten.[145] Darüber hinaus werden die Aufgaben des Melde-, Pass- und Personalausweiswesens von den Berliner Bezirksämtern wahrgenommen.[146]

141 § 23 Abs. 3 Nr. 1 bis 19 PAuswG

142 § 24 Abs. 1 PAuswG

143 § 23 Abs. 4 Satz 1 PAuswG

144 Siehe z. B. Art. 24, 25 und 32 DS-GVO

145 Anlage ASOG – Nr. 33 Abs. 1 lit. a, Abs. 2 lit. a und Abs. 3 lit. a Zuständigkeitskatalog Ordnungsaufgaben (ZustKat Ord)

146 Anlage ASOG – Nr. 22a Abs. 1 ZustKat Ord

3.8 Gemeinsames Zentrum für die Telekommunikationsüberwachung – Breiter Dienst auf schmaler Grundlage

Die Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen bauen ein gemeinsames Zentrum für die Telekommunikationsüberwachung auf. Wir haben zu den Planungsunterlagen Stellung genommen. Dabei mussten wir eine Überdehnung des Aufgabenbereichs und das Fehlen der Vorbereitung von Funktionen für die Wahrung von Betroffenenrechten kritisieren.

Das Gemeinsame Kontroll- und Dienstleistungszentrum (GKDZ) für die Telekommunikationsüberwachung wird auf der Grundlage eines Staatsvertrags durch die Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen aufgebaut.[147] Es soll die Systeme ablösen, die bisher in den Ländern betrieben werden, Kompetenzen bündeln und für eine effiziente Unterstützung der präventiven Polizeiarbeit und der Strafverfolgung sorgen.

Nachdem wir bereits die Erarbeitung des Staatsvertrags begleitet hatten, der die rechtliche Grundlage für die Inanspruchnahme des Zentrums durch die Polizeibehörden der Länder bildet, nahmen wir nun auch Stellung zu den uns vorgelegten Planungsunterlagen. Wir koordinierten uns dabei mit den Aufsichtsbehörden der anderen beteiligten Länder.

Ein Mangel stach sofort hervor: Die Planungen des Zentrums überschreiten dessen durch den Staatsvertrag gesetzte Kompetenzen. Der Staatsvertrag beschränkt die Kompetenzen des Zentrums auf die Unterstützung der Polizeibehörden auf dem Gebiet der Telekommunikationsüberwachung. Die Planungen sehen jedoch darüber hinaus auch die Unterstützung bei anderen Überwachungsmaßnahmen vor, bspw. bei der akustischen Überwachung von Wohnräumen. Die Länder können dem Zentrum zwar auch Aufgaben auf diesem Gebiet zuweisen. Dazu muss jedoch der Staatsvertrag unter Beteiligung der Parlamente geändert werden. Darauf haben wir nachdrücklich hingewiesen.

147 Siehe GVBl. 2017, S. 651 ff.

Da die Überwachung der Telekommunikation von verdächtigen Personen ein erheblicher Grundrechtseingriff ist und oft auch Personen erfasst, die nicht Gegenstand der jeweiligen polizeilichen Ermittlung sind, sind in der Strafprozessordnung (StPO) eine Reihe von Maßgaben enthalten, die dem Schutz der Rechte dieser Personen dienen.

So ist die Kommunikation mit Berufsgeheimnisträger*innen (z. B. mit Ärzt*innen oder Anwält*innen) besonders geschützt und soll nicht aufgezeichnet werden, es sei denn, die Ermittlungen richten sich gegen die Berufsgeheimnisträger*innen selbst. Auch der Kernbereich privater Lebensgestaltung – und damit der intimste Teil unseres Lebens – darf von der Telekommunikationsüberwachung nicht erfasst werden.

Das Zentrum wird jedoch die Telekommunikationsdaten zunächst ungefiltert von den Telekommunikationsunternehmen übernehmen, die sie auf polizeiliche Anweisung übergeben. Erst zu einem späteren Zeitpunkt entscheiden Beschäftigte der jeweiligen Polizei, welche Teile der Aufnahmen aufgrund der Schutzvorschriften zu löschen sind. Schon dadurch sind die Betroffenen schlechter gestellt als bei einer Aufzeichnung unter unmittelbarer Steuerung von Polizeibediensteten, die sofort eingreifen können, wenn der Schutzbereich tangiert wird. Die Planungen des GKDZ sahen zudem vor, nur die für die Kenntnisnahme durch die Beschäftigten der Polizeibehörden aufbereiteten Daten zu löschen. Die Originaldaten sollten erhalten bleiben. Wir wiesen nachdrücklich darauf hin, dass eine vollständige Löschung aller Datenkopien vorzusehen sei.

Auch für die Gewährung der sonstigen Rechte der Betroffenen durch die Landespolizeibehörden muss das GKDZ Funktionalitäten bereitstellen. Dazu gehören die Sperrung von Daten, deren Löschung zurückgestellt wurde, und die Auskunft über die verarbeiteten Daten, aber auch die Kennzeichnung der Daten – je nachdem, auf welche Personen sie sich beziehen: Verdächtige, Straftäter*innen, Opfer, Zeug*innen oder andere.

Ferner waren die Planungen für die Protokollierung der Datenverarbeitung im GKDZ defizitär. Es ist von grundlegender Bedeutung, dass die Rechtmäßigkeit der im Zentrum betriebenen Verarbeitung hochsensitiver Daten im Nachgang überprüft werden kann. Dazu muss die Planung vorgeben, welche Angaben mit wel-

cher Technik zu protokollieren sind und wie die Protokolle vor unbeabsichtigtem Verlust und unbefugter Änderung geschützt werden. Darüber hinaus müssen Methoden und Arbeitsplätze zur Auswertung der Protokolle bereitstehen und es muss möglich sein, die Protokolle an die Datenschutzaufsichtsbehörden zu übergeben, um diesen ihrerseits eine eingehende Prüfung zu ermöglichen.

Schließlich haben wir das GKDZ darauf hingewiesen, dass die Polizeibehörden dazu verpflichtet sind, in einem systematischen Prozess, der sog. Datenschutz-Folgenabschätzung (DSFA), die Risiken der zukünftigen Datenverarbeitung für die betroffenen Personen zu analysieren sowie angemessene und effektive Maßnahmen zur ausreichenden Minderung der Risiken festzulegen. Es ist sinnvoll, dass das GKDZ diese Folgenabschätzung gemeinsam für alle Polizeibehörden durchführt. Wir werden sie sorgfältig prüfen, sobald sie vorliegt.

Es liegt im Interesse der Allgemeinheit, dass die Polizei die ihr verfassungskonform durch Gesetz zugewiesenen Aufgaben effizient erfüllen kann. Die dabei eingesetzten Mittel müssen sich in dem durch das Gesetz definierten Rahmen halten. Dies gilt auch für länderübergreifend tätige gemeinsame Einrichtungen wie das GKDZ. Mit der Einbeziehung der Datenschutzaufsichtsbehörden in den Planungsprozess wird die Möglichkeit eröffnet, dies schon frühzeitig sicherzustellen.

3.9 Auskunftsrechte von Prüflingen in der Juristenausbildung

Aus der Praxis

Das Gemeinsame Juristische Prüfungsamt Berlin-Brandenburg (GJPA) bat uns um Einschätzung eines Referentenentwurfs für ein Gesetz zur Änderung von Vorschriften für die Juristenausbildung.

Dieser Entwurf sah u.a. die Neuregelung von Auskunftsrechten von Prüflingen vor, die jedoch das grundlegende Auskunftsrecht von Betroffenen nach der DS-GVO über die Verarbeitung der sie betreffenden Daten[148] unrechtmäßig verkürzte.

148 Art. 15 Abs. 1 DS-GVO

Das Auskunftsrecht nach der DS-GVO bezieht sich auf sämtliche Datenverarbeitungsvorgänge des GJPA, nicht nur auf die automatisierte Speicherung personenbezogener Daten, wie es der Gesetzentwurf vorsah. Im Übrigen besteht aufgrund des eindeutigen Wortlauts der DS-GVO insoweit auch keine gesetzliche Klarstellungserforderlichkeit. Eine Wiederholung des Regelungsinhalts der DS-GVO in einem Landesgesetz wäre rechtlich fragwürdig. Wir haben daher die Streichung der geplanten Regelung empfohlen.

Nach dem Gesetzentwurf sollten die Auskunftsrechte auch im Hinblick auf Kopien der Prüfungsakte inklusive der Prüfungsarbeiten aus Kapazitäts- und Praktikabilitätsgründen beschränkt werden.

Der Auskunftsanspruch sollte dadurch gewährleistet werden, dass den Prüflingen nach Abschluss des Prüfverfahrens in den Räumlichkeiten des GJPA Einsicht in die über sie geführten Prüfungsakten gewährt wird und ihnen während der Einsicht auch gestattet werden sollte, Kopien anzufertigen.

Das GJPA ist nach der DS-GVO hingegen verpflichtet, selbst eine kostenlose Kopie der verarbeiteten personenbezogenen Daten zur Verfügung zu stellen.[149] Eine Einschränkung dieser Pflicht in der geplanten Form würde gegen höherrangiges Europarecht verstoßen. Es ist nicht ersichtlich, weshalb bei der Erstellung und Übersendung bzw. Übergabe solcher Kopien an die Betroffenen „ein erhebliches Risiko der Beschädigung, Veränderung, Vertauschung oder Vernichtung der Prüfungsarbeiten" bestehen soll, was nach der Gesetzesbegründung eine Beschränkung der Auskunftsrechte erlauben sollte.[150] Zur Vermeidung von Verwechslungen oder Beschädigungen der zu kopierenden Unterlagen durch die Mitarbeitenden des GJPA können organisatorische Maßnahmen ergriffen werden. Wir haben daher auch die Streichung dieser geplanten Vorschrift empfohlen.

149 Siehe 15 Abs. 3 i. V. m. Art. 12 Abs. 5 Satz 1 DS-GVO

150 Siehe Art. 23 DS-GVO

Der Umfang der Auskunftsrechte für Prüflinge in der Juristenausbildung ergibt sich aus der DS-GVO. Danach besteht insbesondere ein Anspruch auf eine unentgeltliche Kopie der Prüfungsarbeiten nebst Bewertungsunterlagen. Diese Rechte dürfen nicht unzulässig durch nationale Vorschriften zur Juristenausbildung verkürzt werden.[151]

151 Siehe hierzu auch das sehr ausführliche Urteil des VG Gelsenkirchen vom 27. April 2020 – 20 K 6392/18

4 Jugend und Bildung

4.1 Zum Einsatz von Microsoft 365 in Schulen – Fortsetzung

In unserem letzten Jahresbericht haben wir die beim Einsatz von Microsoft 365 (bisher Office 365) bestehenden datenschutzrechtlichen Probleme dargestellt. Gleichzeitig haben wir über den Abstimmungsprozess zwischen Vertreter*innen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mit dem Unternehmen Microsoft Corp. über die Voraussetzungen eines zulässigen Einsatzes der Microsoft 365 Produkte berichtet.[152] Ein Jahr später müssen wir feststellen, dass die Bedenken fortbestehen.

In diesem Jahr haben wir zahlreiche Anfragen zur Zulässigkeit des Einsatzes von Microsoft 365 im Schulkontext erhalten. Durch die Corona-Pandemie haben viele Schulen Produkte aus dem Microsoft 365-Paket in den Blick genommen und Einsatzmöglichkeiten geprüft. Gerade die für Videokonferenzen einsetzbare Software Microsoft Teams[153] als Teil dieses Pakets kam in verschiedenen Schulen zum Einsatz. Der Einsatz von Microsoft Teams ist insoweit auch Gegenstand mehrerer Beschwerden von Eltern, die uns erreicht haben.

Ein Hauptproblem des Einsatzes von Microsoft 365 besteht darin, dass sich Microsoft vorbehält, die eigentlich im Auftrag für die jeweilige Schule als Verantwortliche verarbeiteten Daten für eigene Zwecke zu verwenden. Diese Konstruktion ist der Auftragsverarbeitung nach der Datenschutz-Grundverordnung (DS-GVO) fremd.[154]

Es ist das wesentliche Merkmal einer Auftragsverarbeitung, dass in ihrem Rahmen der Auftragnehmer die Daten ausschließlich für den Auftraggeber verarbeitet. Eine darüber hinausgehende Verarbeitung durch den Auftragnehmer führt

152 JB 2019, 5.3
153 Zum Einsatz von Videokonferenztechnik ausführlich 1.3
154 Siehe Art. 28 DS-GVO

dazu, dass dieser in der Rolle eines Verantwortlichen handelt. Für die damit verbundene Offenlegung personenbezogener Daten durch den Auftraggeber bedürfte es einer Rechtsgrundlage, die es für Schulen jedoch nicht gibt.

Auch kann die vielfach durch Schulen eingeholte Einwilligung der Eltern in die Nutzung von Microsoft 365 hier keine Lösung bieten. Zunächst muss festgestellt werden, dass es nicht möglich ist, in eine rechtswidrige Verarbeitung einzuwilligen. Selbst für den Fall, dass die jeweilige Verarbeitung nicht rechtswidrig und eine Einwilligung damit grundsätzlich möglich ist, stellt die DS-GVO jedoch strenge Anforderungen an deren Wirksamkeit. Insbesondere muss sie informiert und freiwillig erfolgen. Wegen des zwischen Schüler*innen und Lehrkräften bestehenden Über-/Unterordnungsverhältnisses geht die DS-GVO jedoch davon aus, dass die Einwilligung im Schulkontext grundsätzlich nicht freiwillig sein kann.[155]

Der Schule ist es zudem als Auftraggeberin angesichts der unklaren und widersprüchlichen Regelungen in dem mit Microsoft abzuschließenden Auftragsverarbeitungsvertrag nicht möglich, die mit der Nutzung der Software verbundenen Datenverarbeitungen im Einzelnen auf ihre Datenschutzkonformität nach der DS-GVO zu überprüfen. Dies gilt insbesondere für die Darstellung der technischen und organisatorischen Anforderungen, die nicht ausreicht, um die Schulen in die Lage zu versetzen, darüber zu entscheiden, ob diese angemessen sind. Die Schulen sind damit nicht in der Lage, der ihnen nach der DS-GVO obliegenden Rechenschaftspflicht nachzukommen.[156] Vor diesem Hintergrund können von den Eltern einzuholende Einwilligungserklärungen auch nicht den Anforderungen an die Informiertheit genügen, da die Schule diese gar nicht ausreichend über die im Einzelnen stattfindenden Datenverarbeitungen informieren könnte. Im Ergebnis kann die Nutzung von Microsoft 365 durch Schulen in keinem Fall durch eine Einwilligung gerechtfertigt werden.

Zu unserem Bedauern konnte zwischen den Datenschutzaufsichtsbehörden des Bundes und der Länder in diesem Jahr keine Einigkeit darüber erzielt werden, wie der Einsatz von Microsoft 365 abschließend zu bewerten ist. Zwar haben die Aufsichtsbehörden mehrheitlich die Anforderungen für einen datenschutzkonformen

155 Siehe EG 43 DS-GVO

156 Siehe Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DS-GVO

Einsatz von Microsoft 365 als nicht gegeben angesehen, jedoch hat sich die DSK dafür ausgesprochen, hier weitere Gespräche mit dem Unternehmen zu führen, um Nachbesserungen zu erreichen. Dies hat allerdings keine Auswirkungen auf die Bewertung des derzeit auf dem Markt befindlichen Produkts.

Wir halten einen datenschutzgerechten Einsatz von Microsoft 365 in Schulen derzeit nach wie vor für nicht möglich. Wir sehen Microsoft in der Pflicht, erhebliche Nachbesserungen vorzunehmen. Bis dahin raten wir allen Schulen dringend, von einem Einsatz von Microsoft 365 abzusehen.

4.2 Datenschutz bei Bild-, Ton- und Videoaufnahmen in Kindertageseinrichtungen

Dem Datenschutz kommt im Alltag von Kindertageseinrichtungen eine wichtige Rolle zu. Die uns seit Jahren kontinuierlich erreichenden Anfragen von Eltern und von Einrichtungen zeigen, dass erhebliche Rechtsunsicherheit im Umgang mit datenschutzrechtlichen Fragestellungen in der Praxis besteht. Uns erreichen immer wieder Anfragen, wann und unter welchen Voraussetzungen Film- und Fotoaufnahmen angefertigt und an wen diese weitergegeben werden dürfen.

Wie in unserem letzten Jahresbericht[157] angekündigt, haben wir unsere gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Familie herausgegebene Broschüre „Datenschutz bei Bild-, Ton- und Videoaufnahmen. Was ist in der Kindertageseinrichtung zu beachten?“ in der 2. Auflage grundlegend überarbeitet und an die aktuellen rechtlichen Vorgaben der DS-GVO angepasst.[158] Gerade weil im pädagogischen Alltag häufig Unsicherheit darüber besteht, wie angesichts der zunehmenden Digitalisierung der Schutz der Persönlichkeitsrechte von Kindern gewährleistet werden kann, möchten wir den pädagogischen Fachkräften mit der Broschüre eine Hilfestellung an die Hand geben, wie sie mit den besonders sensi-

157 JB 2019, 5.1

158 Siehe dazu die gemeinsame Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit und der Senatsverwaltung für Bildung, Jugend und Familie vom 14. August 2020; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen

tiven Daten der Kinder, aber auch der Beschäftigten in den Einrichtungen datenschutzgerecht umgehen können. Die Broschüre wurde zum Beginn des Kitajahres von der Senatsverwaltung an alle 2.700 Berliner Kindertageseinrichtungen versandt und kann als gedruckte Broschüre sowohl bei der Senatsverwaltung für Bildung, Jugend und Familie als auch bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit kostenlos angefordert werden. Als PDF steht sie auch zum Download auf unserer Webseite zur Verfügung.[159] Zudem plant die Senatsverwaltung, zu der neuen Datenschutzbroschüre eine Fortbildung zu veranstalten.

Die 44 Seiten starke Broschüre behandelt u.a. folgende Themen im Zusammenhang mit Bild-, Ton- und Videoaufnahmen in Kitas: datenschutzrechtliche Einordnung (Rechtsgrundlagen und Grundsätze), Datenschutz bei Aufnahmen von Kindern (Einwilligungserklärung, Aufnahmen bei Veranstaltungen und im pädagogischen Alltag, wissenschaftliche Projekte, Veröffentlichung durch Externe), Datenschutz von Mitarbeiter*innen (Erforderlichkeit für das Arbeitsverhältnis, Abhängigkeitsverhältnis von der Arbeitgeberin bzw. vom Arbeitgeber) und Medienkompetenz im pädagogischen Alltag.

Kinder stehen unter dem besonderen Schutz der DS-GVO. Wir sehen es als unsere Aufgabe an, in Zeiten zunehmender Digitalisierung von vornherein den Schutz der Daten unserer Jüngsten in den Blick zu nehmen. Die Rückmeldungen zu unserer Broschüre zeigen uns, dass diese für die Fachkräfte eine wertvolle Hilfestellung für ihre Alltagspraxis bietet.

4.3 Fotos von Kindern und Jugendlichen bei Sportveranstaltungen ohne Einwilligung der Eltern

Die kroatische Aufsichtsbehörde hat uns Eingaben zu einem Berliner Fotografenteam übermittelt. Mehrere Eltern in Kroatien hatten sich darüber beschwert, dass die auf Sport- und Eventfotografie spezialisierten Fotografen bei einem in-

159 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/informationsmaterialien/2020-BlnBDI-Datenschutz_Bild_Ton_Video.pdf

ternationalen Kinder- und Jugendturnier im Wasserspringen Bilder der teilnehmenden Minderjährigen angefertigt hatten und diese über eine Webseite zum Kauf anboten. Allein von diesem Wettkampf wurden etwa 18.000 Bilder von den Teilnehmenden auf der Webseite veröffentlicht. Die Kinder und Jugendlichen sind auf den Fotos überwiegend einzeln bei ihren Sprüngen abgebildet. Eine ausdrückliche Einwilligung der Eltern für die Anfertigung, Veröffentlichung und den Verkauf der Bilder hatten die Verantwortlichen nicht eingeholt. Als zuständige Aufsichtsbehörde haben wir die Beschwerde federführend bearbeitet.

Fotografien von Menschen stellen grundsätzlich personenbezogene Daten dar, weil die abgebildeten Personen direkt oder indirekt identifiziert werden können.[160] Für die Verarbeitung dieser personenbezogenen Daten, insbesondere für die Anfertigung der Fotografien und die weitere Verwendung der Aufnahmen, muss eine der in Art. 6 Abs. 1 Satz 1 DS-GVO geregelten Bedingungen erfüllt sein. Die Vorschriften der DS-GVO gelten nur dann ausnahmsweise nicht, wenn die Fotografien ausschließlich für den persönlichen oder familiären Gebrauch bestimmt sind und diesen eigenen Privatbereich nicht verlassen.[161] Angesichts der durch die Berliner Fotografen professionell betriebenen Sport- und Eventfotografie mit dem Ziel, die Fotos anschließend zu verkaufen, handelte es sich im vorliegenden Fall jedoch um eine kommerzielle Tätigkeit.

Die verantwortlichen Fotografen hatten keine rechtswirksame Einwilligung der betroffenen Personen bzw. von deren Erziehungsberechtigten in Bezug auf die Anfertigung und Veröffentlichung der Fotos eingeholt.[162] Eine konkludente Einwilligung der betroffenen Personen bzw. von deren Erziehungsberechtigten durch die bloße Teilnahme an dem Wettkampfturnier scheidet aus, da nach Art. 4 Nr. 11 DS-GVO hierfür eine Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung notwendig ist.

Die Anfertigung und Veröffentlichung der Fotos kann auch nicht auf eine Rechtsgrundlage gestützt werden. Art. 6 Abs. 1 lit. b DS-GVO kommt als Rechtsgrundlage nicht in Betracht, da die Anfertigung der Fotos von den an der Sportveranstaltung

160 Siehe Art. 4 Nr. 1 DS-GVO

161 Sog. „Haushaltsprivileg" gemäß Art. 2 Abs. 2 lit. c DS-GVO

162 Siehe hierzu Art. 4 Nr. 11 sowie Art. 7 i. V. m. Art. 8 DS-GVO

teilnehmenden Kindern und Jugendlichen nicht Gegenstand eines Vertrags mit den betroffenen Personen bzw. deren Eltern war. Ein Vertragsverhältnis in Form der Beauftragung bestand lediglich zwischen den Fotografen und dem Veranstalter des Turniers.

Die Anfertigung der Fotografien während der Veranstaltung kann auch nicht auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden. Zwar unterliegt die Betätigung der Fotografen im Bereich der Sport- und Eventfotografie generell der Berufs- sowie Kunstfreiheit[163] und stellt ein berechtigtes Interesse dar. Aufgrund der offiziellen Einladung bzw. Akkreditierung bei der Sportveranstaltung ist zudem von einem Interesse des Veranstalters des Kinder- und Jugendturniers an der Dokumentation des Wettbewerbs und somit von einem berechtigen Interesse eines Dritten auszugehen. Diese Interessen sind jedoch nachrangig gegenüber den schutzwürdigen Interessen der fotografierten Minderjährigen. Insbesondere bei Kindern unter 16 Jahren geht die DS-GVO von einer besonderen Schutzbedürftigkeit aus, die es erforderlich macht, die elterlichen Vertreter mit einzubinden.[164] Hieraus folgt auch für die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO, dass regelmäßig die schutzwürdigen Interessen des betroffenen Kindes überwiegen.[165]

Bei der Interessenabwägung war zudem zu berücksichtigen, dass nicht nur die Eltern der betroffenen Kinder und Jugendlichen die Bilder über eine Webseite käuflich erwerben können, sondern grundsätzlich jedermann. Die Bilder waren und sind nicht in einem internen bzw. geschlossenen Portal hinterlegt, sondern weltweit frei abrufbar. Die Fotos sollen somit vorrangig einem kommerziellen Interesse und nicht nur den Interessen der Kinder und Jugendlichen an einer Darstellung ihrer Leistung bzw. der Sportart dienen.

Wir haben der kroatischen Aufsichtsbehörde nunmehr mitgeteilt, dass wir aufgrund der großen Anzahl der betroffenen Personen ein Sanktionsverfahren einleiten und die Beseitigung der Fotos von der Webseite verlangen werden.

163 Siehe Art. 15 und 13 Charta der Grundrechte der Europäischen Union (GRCh)

164 Siehe Art. 8 Abs. 1 DS-GVO

165 Siehe Kühling/Buchner/Buchner/Petri, DS-GVO, Art. 6, Rn. 155

Ohne eine Einwilligung der betroffenen Personen bzw. von deren Erziehungsberechtigten darf keine Veröffentlichung und kein Verkauf der Fotos erfolgen. Auch wenn die Bilder bei einer öffentlichen Veranstaltung mit internationaler Bedeutung im Leistungssportbereich gemacht wurden, ist die Vermarktung von Fotos der Kinder und Jugendlichen in vorliegendem Fall im Ergebnis nicht mit den Persönlichkeitsrechten der Betroffenen zu vereinbaren.

4.4 Nachweis der Masernimpfpflicht in Schulen und Kindertageseinrichtungen

Seit dem 1. März 2020 gilt in Deutschland in bestimmten Zusammenhängen eine Masernimpfpflicht: Nach dem Infektionsschutzgesetz (IfSG) muss für alle Kinder und Beschäftigten in Schulen, Kitas und anderen Gemeinschaftseinrichtungen ein ausreichender Impfschutz nachgewiesen werden. Wir haben Anfragen von Eltern, aber auch Einrichtungen selbst erhalten, die zeigen, dass das Verfahren zum Nachweis der Impfpflicht im Praxisalltag Fragen aufwirft. Immer wieder haben uns Eltern gefragt, ob die Schule oder Kita ihrer Kinder Kopien des Masernimpfnachweises einsammeln darf.

Bei den in den Impfausweisen enthaltenen personenbezogenen Daten handelt es sich um Gesundheitsdaten, die zu den besonders geschützten Kategorien personenbezogener Daten gehören.[166] Ihre Verarbeitung ist ausnahmsweise erlaubt, soweit dies aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich ist. Im IfSG ist geregelt, dass Gemeinschaftseinrichtungen befugt sind, sich einen Nachweis des Masernimpfschutzes[167] vorlegen zu lassen, und verpflichtet sind, das Gesundheitsamt zu informieren, wenn kein ausreichender Nachweis vorgelegt wurde.[168] Auch wenn der Wortlaut des IfSG die Vorlage an die „Leitung der jeweiligen Einrichtung"[169] vorsieht, stellt es auch nicht von vornherein einen Verstoß dar, wenn der Masernimpfnachweis bspw. den Klassen-

166 Siehe Art. 9 Abs. 1 DS-GVO i. V. m. Art. 4 Nr. 15 DS-GVO
167 Nachweisalternativen sind in § 20 Abs. 9 Satz 1 Nr. 1–3 IfSG aufgeführt.
168 § 20 Abs. 9 Satz 1, Satz 4 bzw. Abs. 10 Satz 1 und Satz 2 IfSG
169 § 20 Abs. 9 Satz 1 bzw. Abs. 10 Satz 1 und Satz 2 IfSG

lehrer*innen vorgelegt wird. Sinn und Zweck der Regelung ist nicht, dass die Leitung die Datenerhebung im Einzelnen persönlich ausführt, sondern dass sie den Vorgang verantwortet. Die Praxis mancher Einrichtungen, die vorgelegten Impfausweise zu kopieren und die Kopien aufzubewahren, ist allerdings in der Regel nicht zulässig. Denn die kopierte Seite eines Impfausweises enthält regelmäßig Informationen über weitere Impfungen, die für den Zweck des Nachweises eines ausreichenden Masernimpfschutzes nicht erforderlich sind. Stattdessen sollte die Einrichtung die Bestätigung, ob ein vollständiger Nachweis erbracht wurde oder nicht, eigenständig in einem separaten Dokument vermerken.

Gemeinschaftseinrichtungen wie Schulen und Kitas sind dazu befugt, sich einen Nachweis des Masernimpfschutzes vorlegen zu lassen. Allerdings muss die Verarbeitung dieser sensitiven Daten datenschutzkonform erfolgen. Die Praxis mancher Schulen und Kitas, Kopien des Impfausweises einzusammeln und aufzubewahren, ist nicht erforderlich und daher unzulässig.

4.5 Childhood-Haus an der Charité – Nachbesserung erforderlich

Kurz vor der geplanten Eröffnung des sog. Childhood-Hauses an der Charité-Universitätsmedizin Berlin hat uns die Charité gebeten, die Konzeption aus datenschutzrechtlicher Sicht zu betrachten. Angesichts der erheblichen datenschutzrechtlichen Relevanz war dies leider viel zu kurzfristig, um die Datenschutzanforderungen noch rechtzeitig vor der geplanten Eröffnung umsetzen zu können. Sinnvoll wäre es gewesen, uns gleich zu Beginn in das Projekt einzubeziehen, da es auf diese Weise möglich gewesen wäre, die datenschutzrechtlichen Anforderungen gleich bei der Konzeption zu berücksichtigen.

Mit dem sog. Childhood-Haus (wörtlich übersetzt: Kinderhaus) soll das skandinavische Modell eines interdisziplinären und behördenübergreifenden Zentrums für Kinder, die Gewalt erfahren haben, umgesetzt und eine zentrale Anlaufstelle geschaffen werden. Ziel soll es sein, ein Kompetenzzentrum für von Gewalt und/oder Missbrauch betroffene Kinder und Jugendliche, bei denen bereits ein Ermittlungsverfahren anhängig ist, zu schaffen. Die Versorgung der Kinder und Jugendlichen, die Beweissicherung und weitere Unterstützung soll in diesem Haus ge-

bündelt werden. Es handelt sich hier um ein fachlich sicher unterstützenswertes Anliegen. Allerdings wirft die Kooperation verschiedener mit einem Fall befasster Institutionen, wie Kinderschutz-Ambulanzen, Trauma-Ambulanz, Polizei, Staatsanwaltschaft und Ermittlungsrichter*innen sowie Jugendämter und Familiengerichte, datenschutzrechtliche Fragen auf, sofern – wie im Childhood-Haus – ein interdisziplinärer Informationsaustausch geplant ist.

Wir haben die Charité auf das Problem der Fallkonferenzen zwischen verschiedenen Institutionen, die unterschiedliche gesetzliche Aufgaben wahrnehmen, aufmerksam gemacht. Datenübermittlungen zwischen allen Beteiligten können nur dann in Betracht kommen, wenn Befugnisse für den Datenaustausch zwischen allen beteiligten Institutionen vorliegen. Dies ist jedoch angesichts der sehr unterschiedlichen Aufgaben der Beteiligten (Strafverfolgung, Kinder- und Jugendhilfe, medizinische Diagnostik) und jeweils unterschiedlichen gesetzlichen Grundlagen für die Datenverarbeitung nicht der Fall. Jede Institution darf nur diejenigen Daten zur Kenntnis bekommen, die für ihre spezielle Aufgabe notwendig sind. Dies sind z. B. für die Jugendhilfe andere Daten als für die Polizei. So benötigt die Polizei für ihre Ermittlungsarbeit nicht die dem Jugendamt für die sozialpädagogische Betreuung einer Familie vorliegenden sensitiven Daten über bestimmte Familienverhältnisse oder möglicherweise im Rahmen medizinischer Diagnostik bekannt gewordenen Erkenntnisse. Der Austausch zwischen verschiedenen Beteiligten muss daher auf das Nötigste begrenzt werden. Dies wird im Rahmen von Fallkonferenzen schwerlich gelingen.

Fallkonferenzen lassen sich in diesem Zusammenhang auch meist nicht auf der Grundlage von Einwilligungen durchführen. Einwilligungen müssen freiwillig und informiert erfolgen. Es muss den Personensorgeberechtigten bzw. den Jugendlichen transparent gemacht werden, welche konkreten Daten für welche möglichst genau beschriebenen Zwecke an alle anderen Beteiligten an der Fallkonferenz weitergegeben werden und welche Konsequenzen sich daraus ergeben können. Dies wird in der Praxis zumeist nicht möglich sein, da nicht von vornherein bekannt ist, welche Informationen im Verlauf einer Fallkonferenz zusammengeführt werden und welche Folgen sich daraus ergeben können. Auch sind der Einwilligung hinsichtlich der Datenverarbeitung von Strafverfolgungsbehörden sehr enge Grenzen gesetzt.

Die Konzeption des Childhood-Hauses sah vor, eine in dem Projekt bei der Charité beschäftigte Person mit einer koordinierenden Rolle auszustatten, bei der die Informationen zu einem konkreten Fall zusammengeführt werden sollten. Auch hier ergaben sich erhebliche datenschutzrechtliche Fragen, denn die Bündelung sämtlicher Informationen zu einem konkreten Fall an einer Stelle steht ebenfalls im Widerspruch zu den für die beteiligten Institutionen geltenden gesetzlichen Datenverarbeitungsbefugnissen. Diese sehen – aus gutem Grunde – nicht vor, dass z. B. medizinische Informationen aus der Kinderschutz-Ambulanz oder der Trauma-Ambulanz, die bei den Jugendämtern vorliegenden Daten sowie die bei den Strafverfolgungsbehörden bekannten Informationen ohne Weiteres miteinander verknüpft werden dürfen.

Wir haben die Charité darauf hingewiesen, dass grundlegende Änderungen an der Konzeption des sog. Childhood-Hauses notwendig sind, um das Vorhaben datenschutzgerecht umsetzen zu können. In erster Linie geht es darum, dass das mit dem Childhood-Haus verbundene Ziel, die Kinder und Jugendlichen mit Gewalt- und Missbrauchserfahrungen möglichst optimal zu versorgen, sich in einem zulässigen Datenschutzrahmen bewegt. Gerade in solch einem sensitiven Bereich ist es unerlässlich, dass die Betroffenen und ihre Familien darauf vertrauen können, dass es nicht „hinter ihrem Rücken" zu einem umfangreichen Austausch von Daten kommt, auf den sie selbst keinen Einfluss mehr nehmen können und der zu möglicherweise unerwarteten und ungewollten Konsequenzen führen könnte. Die Charité hat uns zwischenzeitlich eine geänderte Konzeption vorgelegt. Auf dieser Grundlage werden wir weitere Beratungen mit den Beteiligten durchführen.

5 Gesundheit und Pflege

5.1 Novellierung des Landeskrankenhausgesetzes

Mit dem Berliner Datenschutz-Anpassungsgesetz-EU[170] hat der Landesgesetzgeber in einem Schwung zahlreiche Landesgesetze an die europarechtlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) angepasst. Zu diesen Gesetzen gehörte auch das Landeskrankenhausgesetz (LKG). Bei dessen Novellierung ist vieles gelungen. Leider ist kurz vor der Schlussabstimmung über das Gesetz eine aus Datenschutzsicht fatale Änderung ohne die erforderliche Beratung eingefügt worden.

Das LKG enthält spezielle datenschutzrechtliche Bestimmungen für die Berliner Krankenhäuser.[171] In ihnen wird u.a. festgelegt, wem die Krankenhäuser Patient*innendaten offenlegen dürfen und unter welchen Bedingungen Krankenhäuser bei der Verarbeitung ihrer Patient*innendaten auf externe Dienstleister, sog. Auftragsverarbeiter, zurückgreifen können.[172]

Wir waren in die Erarbeitung eines Entwurfs der Gesetzesnovelle durch die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung intensiv einbezogen worden. Ziel war es, den Krankenhäusern neue Möglichkeiten für die Verarbeitung von Patient*innendaten zu eröffnen, die sich im Klinikalltag als notwendig erwiesen haben, ohne das Schutzniveau der Daten zu senken. Daher fand auch mehrfach ein Austausch mit Vertreter*innen des Krankenhausbereichs statt.

Die bis Ende 2020 geltende Fassung des Gesetzes sah vor, dass Patient*innendaten grundsätzlich nur im Krankenhaus oder im Auftrag durch ein anderes Krankenhaus verarbeitet werden durften. Eine Verarbeitung durch andere Stellen im Auftrag des Krankenhauses war nur dann zulässig, wenn durch technische

170 BlnDSAnpG-EU; siehe GVBl. 2020, S. 807–828
171 §§ 24, 25 LKG
172 § 24 Abs. 7 LKG

Schutzmaßnahmen sichergestellt war, dass der Auftragnehmer keine Möglichkeit hatte, beim Zugriff auf die Patient*innendaten den Personenbezug herzustellen.[173] Eine mit der Beauftragung verbundene Offenbarung von Patient*innendaten an private Unternehmen, die nicht selbst ein Krankenhaus sind, schied also aus.

Aus datenschutzrechtlicher Sicht war diese Regelung nicht zu beanstanden, trug sie doch in besonderem Maße der hohen Sensitivität der in Rede stehenden Patient*innendaten Rechnung. Auch mit Blick auf die europäischen Entwicklungen, mithin dem Wirksamwerden der DS-GVO, hätte es in diesem Punkt keiner Änderung bedurft. Vielmehr sieht die DS-GVO für die Mitgliedstaaten sogar ausdrücklich die Möglichkeit vor, zusätzliche Bedingungen, einschließlich Beschränkungen, einzuführen oder aufrechtzuerhalten, soweit – wie hier – die Verarbeitung von genetischen Daten oder Gesundheitsdaten betroffen ist.[174]

Aus Sicht vieler Krankenhäuser bestand hingegen der durchaus dringende Wunsch nach einer „Öffnung" der Auftragsverarbeitung, um – natürlich auch aus wirtschaftlichen Erwägungen – zukünftig flexibler bei der Einbindung externer Dienstleister zu sein.

Eine der gewünschten Neuerungen war die Erlaubnis, auch Tochterunternehmen (oder andere Unternehmen der gleichen Unternehmensgruppe) einbeziehen zu dürfen. Eine andere war die Einbeziehung von Dienstleistern für den Betrieb und die Wartung der komplexen Informations- und Medizintechnik der Krankenhäuser.

Gerade hinsichtlich des zweiten Punktes ist nachvollziehbar, dass Krankenhäuser nicht für die gesamte Technik die erforderliche Kompetenz im eigenen Haus vorhalten können. Daher sollte die Heranziehung von externer Expertise ermöglicht werden.

Grundsätzlich aber müssen Patint*innendaten aufgrund ihrer besonderen Sensitivität im Krankenhaus und unter seiner Kontrolle verbleiben. Eine Konzentration von Patient*innendaten in den Händen weniger Cloud-Dienstleister würde erheb-

173 So die alte Fassung des § 24 Abs. 7 LKG

174 Art. 9 Abs. 4 DS-GVO

liche Gefahren bergen. Die Gefahren liegen dabei nicht nur darin, dass die Datensammlungen bei diesen Dienstleistern ein attraktives Angriffsziel darstellen würden. Sie liegen auch in der Natur der Dienstleister, die ein Eigeninteresse an der Auswertung der verarbeiteten Daten haben. Zudem werden viele Cloud-Dienste unmittelbar oder mittelbar durch Dienstleister aus Unternehmensgruppen erbracht, die in den USA ihren Hauptsitz haben und damit dem Zugriff US-amerikanischer Behörden ausgesetzt sind.[175] Eine Auslagerung von Patient*innendaten an Dienstleister ohne direkte Verbindung zum Krankenhausbereich und ohne Einverständnis und Interventionsmöglichkeit der Patient*innen lehnen wir daher ab.

Nach dem mehrere Jahre währenden Abstimmungs- und Diskussionsprozess zwischen der zuständigen Senatsverwaltung, der Senatskanzlei und unserem Haus ist schlussendlich ein Regelungsentwurf entstanden, der den Interessen aller Beteiligten Rechnung trägt. So sieht die Neuregelung insbesondere vor, dass der Auftragnehmer nicht notwendigerweise selbst ein Krankenhaus sein muss. Vielmehr reicht es aus, wenn der beauftragte Dienstleister der Unternehmensgruppe eines Krankenhauses angehört. Auf diese Weise wird den Krankenhäusern ermöglicht, Verarbeitungstätigkeiten auch an eigene oder Tochterunternehmen anderer Krankenhäuser auszulagern.[176] Diese Neuregelungen gehen damit deutlich über die bisherigen Möglichkeiten hinaus, ohne dabei den Schutz der sensitiven Daten der Patient*innen aus dem Blick zu verlieren.

Also Ende gut, alles gut? – Ja, gebe es da nicht einen Haken.

Denn die Neuregelung der Auftragsverarbeitung tritt im Unterschied zu allen anderen Änderungen des LKG erst zwei Jahre nach Verkündung des BlnDSAnpG-EU, d. h. im Oktober des Jahres 2022 in Kraft.[177] Zurückzuführen ist dies auf einen noch in letzter Minute eingebrachten Änderungsantrag der Koalitionsfraktionen.[178]

Nachvollziehbar ist diese Hauruckaktion nicht. In der Konsequenz hat sie dazu geführt, dass das LKG für die nächsten zwei Jahre über keinerlei bereichsspe-

175 Siehe 1.2
176 Siehe § 24 Abs. 7 LKG
177 Art. 57 Abs. 2 BlnDSAnpG-Eu
178 Abghs.-Drs. 18/2598-1 vom 1. Oktober 2020

zifische Regelung zur Auftragsverarbeitung verfügt. Es gelten damit zumindest vorübergehend lediglich die allgemeinen Regelungen der DS-GVO.

Eine konkrete Begründung für diese Änderung wurde uns weder mitgeteilt, noch ist sie uns bekannt. Sollten dahingehende Befürchtungen bestanden haben, dass die Neuregelung einer verstärkten Kooperation der Krankenhäuser im Weg steht, ist diese Annahme jedenfalls völlig unbegründet und nicht nachvollziehbar.

Wir werden in unseren Beratungen der Krankenhäuser darauf hinwirken, dass die Neuregelung zur Auftragsverarbeitung schon vor ihrem Inkrafttreten Beachtung findet. Wir können nur an die Einsicht der Krankenhäuser appellieren, sich klarzumachen, welchen Gefahren ausgerechnet diese, zu den sensitivsten Daten zählenden Patient*innendaten ausgesetzt sind. Sind die Daten erst einmal in unbefugte Hände geraten, können sie – z. B. nach Ablauf der Übergangsfrist – auch nicht mehr zurückgeholt werden. Die Auswirkungen auf die Patient*innen könnten gravierend sein.

5.2 Neue Entwicklungen in der Charité-Saga

Seit mehreren Jahren bemüht sich die Charité um Aufarbeitung von uns festgestellter tiefgehender Defizite. Sie wird dabei von uns eng begleitet. In diesem Jahr kam es zunächst zu langen Verzögerungen. Doch zum Jahresende nahm die Bereinigung der Defizite endlich Fahrt auf.

Wie in den vergangenen Jahren bereits ausführlich berichtet[179], haben Prüfungen in den Jahren 2015 und 2019 bei der Charité tiefgreifende Mängel bei der Einhaltung der datenschutzrechtlichen Vorgaben aufgedeckt. Die Charité stellte in enger Absprache mit uns Pläne zur Mängelbehebung auf und arbeitet diese seitdem systematisch ab. Dabei kam es auch in diesem Jahr zu erheblichen Verzögerungen. Einige davon sind zweifellos der Beanspruchung der Charité durch die Covid-19-Pandemie geschuldet. Aber auch in Zeiten geringer Infektionsraten waren die Fortschritte gering. Dies änderte sich erst im vierten Quartal.

179 JB 2019, 6.2; JB 2018, 6.5; JB 2017, 7.5; JB 2016, 6.1; JB 2015, 8.4.1

Wie alle Verantwortlichen, die in großem Umfang sensitive Daten verarbeiten, muss die Charité in einem systematischen Prozess die Risiken bestimmen, denen einerseits ihre Patientinnen und Patienten bei der Datenverarbeitung zur Unterstützung, Dokumentation und Abrechnung der Behandlung und andererseits ihre Probandinnen und Probanden bei Vorhaben der medizinischen Forschung ausgesetzt sind. Solche Risiken bestehen z. B. in der Offenlegung von Patient*innendaten an Unbefugte oder der unrechtmäßigen Aufdeckung der Identität von Probandinnen und Probanden in Forschungsvorhaben. Für jedes dieser Risiken sind angemessene und effektive Maßnahmen zu bestimmen und umzusetzen, mit denen die Wahrscheinlichkeit gesenkt wird, dass sich die mit der Verarbeitung dieser Daten verbundenen Risiken verwirklichen, und die Auswirkungen abgemildert werden, wenn es doch zu einer Datenpanne kommt.

Der zu absolvierende Prozess wird durch den (europäischen) Gesetzgeber vorgegeben und als Datenschutz-Folgenabschätzung (DSFA) bezeichnet. Im Vorjahr 2019 hatte die Charité die ersten DSFA durchgeführt. Die Ergebnisse blieben jedoch zum Teil weit hinter den gesetzlichen Anforderungen zurück. Wir haben die Charité daher bei der Erstellung einer Muster-DSFA unterstützt und hierfür eine Mustergliederung zur Verfügung gestellt. Ab September begann die Charité auf der Grundlage des Musters und weiterer von uns gegebener Hinweise endlich damit, aussagekräftige DSFA-Berichte zu erstellen.

Zwei große Lücken ließ sie dabei offen:

Zunächst folgte sie dem Muster nur für klinische Verfahren. Erst Anfang Oktober trafen bei uns die ersten halbwegs adäquaten DSFA-Berichte auch für Forschungsvorhaben ein – fünf Jahre, nachdem das Fehlen von Risikoanalysen und Konzepten für die zu ergreifenden technischen und organisatorischen Maßnahmen erstmals von uns festgestellt wurde. Bis Mitte 2021 sollen nunmehr auch im Forschungsbereich dreißig DSFA für diverse Forschungsvorhaben erstellt werden. Sie sollen dabei einen Querschnitt der verschiedenen Typen von Forschungsvorhaben abbilden und als Blaupausen für andere Vorhaben dienen. Das Vorgehen ist sinnvoll, doch ließ der Plan völlig außer Acht, dass auch im Jahr 2021 neue Forschungsvorhaben begonnen werden sollen. Für diese neuen Forschungsverfahren waren keineswegs von vornherein vorgeschaltete DSFA vorgesehen. Wir mussten die Charité daher darauf hinweisen, dass neue Vorhaben nicht ohne Er-

füllung der gesetzlichen Anforderungen in Angriff genommen werden dürfen. Es wird nicht möglich sein, Versäumnisse der Vergangenheit aufzuarbeiten, wenn nicht für gegenwärtige und zukünftige Datenverarbeitungen von vornherein die gesetzlichen Vorgaben beachtet werden.

Die zweite große Lücke erstreckt sich auf die Risiken, die aus der Nutzung der technischen Infrastruktur der Charité entstehen, und auf die Funktionalitäten, die diese Infrastruktur bereitstellen muss, um in den einzelnen Verarbeitungstätigkeiten die Rechte der betroffenen Personen wahren und die Datenschutzgrundsätze einhalten zu können.[180] Weder gelang der Charité eine Analyse der für die einzelnen Verarbeitungstätigkeiten relevanten, aus der Infrastruktur herrührenden Risiken noch die Bestimmung der zentral bereitzustellenden Funktionalitäten, wie sie z. B. für das Auffinden aller Kopien von Daten nötig sind, die sich auf eine Person beziehen, die ihre Datenschutzrechte geltend macht. Wir haben hierzu einen separaten Prüfvorgang aufgenommen.

Einige wesentliche Fortschritte erzielte die Charité dagegen in Bezug auf den mangelhaften Schutz der Daten über Patientinnen und Patienten, deren Behandlung bereits längere Zeit abgeschlossen ist. Nunmehr werden Beschäftigte zumindest davor gewarnt, auf derartige Daten zuzugreifen. Ein vollständiger Ausschluss der Zugriffsmöglichkeit wird erst dann greifen, wenn durch geeignete technische und organisatorische Regeln sichergestellt ist, dass bei einer erneuten stationären Aufnahme, ambulanten Behandlung oder Nachfrage von nachbehandelnden Einrichtungen die dann benötigten Daten der Patientinnen und Patienten verzögerungsfrei zur Verfügung stehen. Schließlich hat die Charité zumindest teilweise die Voraussetzungen dafür geschaffen, diejenigen Daten aus der ambulanten Behandlung zu löschen, deren Aufbewahrungsfrist abgelaufen ist. Erste Löschungen wurden vorgenommen.

Vor der Charité steht nach wie vor die Aufgabe, jahrelang aufgebaute Datenschutzmängel abzubauen. Weitere Verzögerungen, soweit sie nicht aus einer medizinischen Notlage herrühren, sind nicht hinnehmbar.

180 Siehe 17.3

5.3 (Un-)Sichere Wege für Patientenakten

Wir wurden durch ein Krankenhaus auf ein Verfahren hingewiesen, mit dem ein Dienstleister für die Medizinischen Dienste der Krankenkassen (MDK) in einem Massenverfahren Patient*innendaten von Krankenhäusern entgegennimmt. Wir haben daraufhin die Sicherheit des Verfahrens überprüft.

Krankenhäuser verarbeiten im Zuge der Behandlung ihrer Patientinnen und Patienten in großem Umfang Gesundheitsdaten. Dies ist erforderlich, um die Behandlung bestmöglich durchführen zu können. Diese streng vertraulich zu behandelnden Patient*innendaten können Informationen beinhalten, deren Offenlegung zu schweren Konsequenzen für die Betroffenen führen kann.

Die MDK überprüfen im Rahmen ihres gesetzlichen Auftrags Abrechnungen von medizinischen Leistungen für einen großen Anteil der Behandlungsfälle. Dazu lassen sie sich medizinische Unterlagen über die Behandlung vorlegen. Dies geschah bisher in Papierform. Mit der Verabschiedung des MDK-Reformgesetzes wurde geregelt, dass Krankenhäuser ab dem 1. Januar 2021 diese Datenübermittlung in elektronischer Form vornehmen müssen.

Die MDK haben zur Entgegennahme der übermittelten Daten eine gemeinsame technische Plattform aufgesetzt und ihren Betrieb an ein gemeinsames Tochterunternehmen mit Sitz in Berlin übergeben.[181] Dieses Unternehmen ist für die Sicherheit der von ihm vollzogenen Verarbeitung verantwortlich.

Bei der elektronischen Übermittlung zahlloser personenbezogener Datensätze mit Gesundheitsdaten über das offene Internet entstehen hohe Risiken für die Vertraulichkeit dieser Daten. Daher ist es erforderlich, die Daten hinreichend zu verschlüsseln, um die Kenntnisnahme und einen möglichen Missbrauch durch Dritte auszuschließen.

Das eingesetzte Verfahren sah ausschließlich die Verschlüsselung des Kommunikationskanals zwischen Krankenhaus und Plattform mittels standardisierter Pro-

181 Siehe § 80 SGV X

tokolle vor, wie sie auch genutzt werden, um die Verbindung zwischen einem Webbrowser und einer Webseite zu verschlüsseln. Angesichts der hohen Risiken ist dies nicht ausreichend. Selbst wenn die Verschlüsselung des Kommunikationskanals fehlerfrei gelingt – und in der Vergangenheit wurden mehrfach Schwachstellen aufgedeckt, deren Ausnutzung Dritten den Zugang zu den Kommunikationsinhalten ermöglicht hätte –, liegen die Daten an den Endpunkten der Verbindung dennoch stets unverschlüsselt vor. Damit stellen sie nach wie vor außerordentlich ergiebige und damit attraktive Ziele für Cyber-Angriffe dar.

Ergänzend ist daher eine Ende-zu-Ende-Verschlüsselung einzusetzen. Diese bewirkt, dass die Daten bereits vor dem Versand so verschlüsselt werden, dass nur der Empfänger, also in diesem Fall der zuständige MDK, die Daten entschlüsseln kann. Dies kann er in einem Abschnitt seines Computernetzwerks tun, der nicht unmittelbar mit dem Internet verbunden und besonders geschützt ist. Entsprechend können auch die Krankenhäuser die Verschlüsselung bereits in einem internen Netzwerk vornehmen. Die Übergabe an die Plattform kann dann von einem weniger geschützten, direkt mit dem Internet verbundenen Gerät aus geschehen.

Diese Vorgehensweise entspricht dem Stand der Technik und ist angesichts der bestehenden Risiken verhältnismäßig. Wir haben daher den Betreiber der Plattform aufgefordert, ergänzend zur bereits vorhandenen Transportverschlüsselung eine Ende-zu-Ende-Verschlüsselung einzusetzen.

Bei der Übermittlung sensitiver Gesundheitsdaten ist eine besondere Sorgfalt bei dem Schutz der Vertraulichkeit erforderlich. Dies gilt umso mehr, wenn eine große Zahl von Patientinnen und Patienten betroffen ist. Hierfür ist eine Ende-zu-Ende-Verschlüsselung einzusetzen.

5.4 Weitergabe von Gesundheitsdaten an die Ausländerbehörde

In einer Eingabe wurde vorgetragen, dass ein behandelnder Klinikarzt die Ausländerbehörde kontaktiert und dieser mitgeteilt habe, dass der Beschwerdeführer nach dem Genuss verschiedener Rauschgifte in der dortigen Rettungsstelle aufgenommen worden sei. Der Beschwerdeführer bat uns um Prüfung.

Die Klinik teilte uns auf unsere Anfrage hin mit, dass der Beschwerdeführer bewusstlos im Rettungswagen in die Klinik eingeliefert worden sei. Ein ihn begleitender Bekannter habe angegeben, dass er an dem Abend diverse alkoholische Getränke und Ecstasy zu sich genommen habe. Jedoch sei durch das Vorliegen einer Sprachbarriere bei der Kommunikation mit der Begleitperson nicht zu klären gewesen, ob der Beschwerdeführer an Vorerkrankungen, Allergien oder chronischen Erkrankungen leide. Er sei dann innerhalb der Klinik zur weiteren Behandlung auf die Intensivstation verlegt worden. Aufgrund der Bewusstlosigkeit sei er nicht in der Lage gewesen, Auskünfte über sich selbst zu erteilen. Auch sei seine Begleitperson für Nachfragen nicht mehr erreichbar gewesen. Die Klinik legte uns nachvollziehbar dar, dass die notwendigen Angaben über etwaige Suizidalität, Fremdaggression und psychiatrische Vorerkrankungen notwendig gewesen und nur durch Angaben von Dritten zu erlangen gewesen seien. Ein Abschiebebescheid sei die einzige bei dem Beschwerdeführer auffindbare Unterlage gewesen, sodass Kontakt zur ausstellenden Ausländerbehörde zur Klärung aufgenommen worden sei. Der Ausländerbehörde seien jedoch keine medizinischen Einzelheiten über Drogen- oder Alkoholkonsum mitgeteilt worden. Um Gefahren für den Beschwerdeführer selbst und eine etwaige Fremdgefährdung der Klinikmitarbeitenden abzuwenden, sei es notwendig gewesen, Kontakt zur Ausländerbehörde aufzunehmen.

Diese Argumentation war für uns nachvollziehbar. Die Zulässigkeit der Verarbeitung personenbezogener Daten ließ sich auf Vorschriften der DS-GVO i. V. m. dem LKG stützen.[182]

182 Art. 9 Abs. 2 lit. c DS-GVO i. V. m. § 24 Abs. 5 Nr. 3 LKG in der bis zum 24. Oktober 2020 geltenden Fassung

Mit sensitiven Patient*innendaten ist sorgsam umzugehen. Dies gilt insbesondere für deren Weitergabe an Dritte. Im Rahmen unserer Prüfung stellte sich heraus, dass im konkreten Fall die Weitergabe an die Ausländerbehörde nach einer Abwägung der Interessen als gesetzlich zulässig anzusehen war.

6 Integration, Soziales und Arbeit

6.1 Beschwerdestelle für geflüchtete Menschen braucht Datenschutz

In unserem letzten Jahresbericht[183] haben wir darüber informiert, dass die Senatsverwaltung für Integration, Arbeit und Soziales plane, eine unabhängige Beschwerdestelle für geflüchtete Menschen zu schaffen, die „niedrigschwellig" Beschwerden über Einrichtungen bzw. über Vorgänge im Zusammenhang mit der Unterbringung entgegennehmen solle. In erster Linie stellte sich in datenschutzrechtlicher Hinsicht das Problem, dass die Beschwerdestelle nach der Planung zwar umfangreiche personenbezogene Daten verarbeiten sollte, eine gesetzliche Aufgabenzuweisung an diese Stelle jedoch nicht besteht. Die Verarbeitung der Daten kann insoweit mangels Rechtsgrundlage lediglich auf der Grundlage einer Einwilligung der Beschwerdeführenden erfolgen.

Die Verarbeitung personenbezogener Daten auf eine Einwilligung zu stützen, wirft in der Praxis schwierige Fragen auf. Eine Einwilligung kann nur dann wirksam sein, wenn sie informiert erfolgt. Dies ist der Fall, wenn die Beschwerdeführenden einordnen können, welche Auswirkungen für sie mit der Erteilung der Einwilligung verbunden sind. Dazu gehört, dass die Umstände der Datenverarbeitung aus der Einwilligungserklärung vollständig und konkret erkennbar sein müssen. Eine Einwilligungserklärung kann als Grundlage für eine Datenverarbeitung nur herangezogen werden, wenn diese Anforderungen erfüllt sind. Für die Datenverarbeitung durch die Beschwerdestelle bedeutet dies, dass in der Erklärung sämtliche Datenverarbeitungsprozesse im Einzelnen benannt werden müssen.

Wir haben diese Problematik eingehend mit der Senatsverwaltung für Integration, Arbeit und Soziales erörtert. Unsere Empfehlung lautete von Beginn an, die Befugnisse der Beschwerdestelle auf eine gesetzliche Grundlage zu stellen und die

183 JB 2019, 7.1

Einwilligung lediglich als eine Übergangslösung zu betrachten. Da geplant war, die Beschwerdestelle möglichst zeitnah in Betrieb zu nehmen, wurden die Vordrucke für die Einwilligungserklärungen sowie die begleitenden Informationsschreiben in einem intensiven Beratungsprozess zwischen der Senatsverwaltung und uns abgestimmt. Die strengen Anforderungen an die Einwilligung sind nunmehr erfüllt. Aufgrund der Corona-Pandemie wird sich die ursprünglich für 2020 geplante Inbetriebnahme der Beschwerdestelle zwar noch verzögern, jedoch stehen die datenschutzrechtlichen Voraussetzungen dem Start nicht mehr entgegen.

Wir begrüßen es ausdrücklich, dass die Senatsverwaltung für Integration, Arbeit und Soziales die Einwilligungslösung lediglich für eine Übergangszeit anwenden möchte und beabsichtigt, die Beschwerdestelle, unserer Empfehlung folgend, zeitnah im Landesrecht zu verankern. Es ist sehr erfreulich, dass uns die Senatsverwaltung einen ersten Entwurf für eine entsprechende Regelung sehr frühzeitig zur Kenntnis gegeben hat, damit die datenschutzrechtlichen Belange von vornherein Berücksichtigung finden können. Wir werden den Entwurf prüfen und die Senatsverwaltung im weiteren Prozess konstruktiv beraten.

6.2 Unterbringung Wohnungsloser – Nicht ohne Datenschutz

Das Projekt „Gesamtstädtische Steuerung der Unterbringung“ (GStU) ist ein wichtiges Projekt des Senats im Bereich Soziales. Mit dem Projekt, das von der Senatsverwaltung für Integration, Arbeit und Soziales realisiert wird, soll die Unterbringungssituation wohnungsloser Menschen verbessert werden. Künftig sollen diesen über die Bezirksgrenzen hinweg Plätze in Unterkünften zugewiesen werden, die konkret auf ihre Bedürfnisse zugeschnitten sind. Hierbei soll die gesamtstädtische Kapazitätsplanung und Belegungssteuerung mithilfe eines zentralen IT-Fachverfahrens realisiert werden. Zudem soll eine zentrale Datenbasis geschaffen werden, um statistische Auswertungen vorzunehmen. Das Ziel, die bedarfsgerechte Unterbringung wohnungsloser Menschen gesamtstädtisch zu steuern und „auf Knopfdruck“ zu organisieren, ist nachvollziehbar. Da hierbei jedoch auch umfangreiche Verarbeitungen besonders sensitiver Daten erfolgen sollen, wie z. B. Informationen über Krankheiten oder Behinderungen oder die

sexuelle Orientierung, ist bei der Umsetzung des Projektes ein besonderes Augenmerk auf die Einhaltung der Datenschutzanforderungen zu richten.

Leider ist unsere Behörde erst im Sommer in dieses bedeutsame Projekt eingebunden worden. Dies verwundert vor dem Hintergrund, dass der Senat die Senatsverwaltung für Integration, Arbeit und Soziales bereits 2016 mit der Entwicklung eines geeigneten Instrumentariums betraut und den Projektauftrag im Juli 2018 beschlossen hat. Erst im September 2020 hat uns die Senatsverwaltung die für unsere Prüfung notwendigen Unterlagen zur Verfügung gestellt. Es stellte sich dann in vielen Punkten noch grundsätzlicher Klärungsbedarf heraus, insbesondere zu den Rollen der Beteiligten. Die Betreuung der wohnungslosen Menschen und deren Zuweisung in geeignete Unterkünfte erfolgt – abhängig von den aufenthaltsrechtlichen Verhältnissen – entweder durch die Sozialen Wohnhilfen der Bezirke oder durch das Landesamt für Flüchtlingsangelegenheiten. Daneben soll später eine „Zentrale Serviceeinheit GStU" eingerichtet werden, die sowohl für das Vertrags- und Unterkunftsmanagement als auch für die Abrechnung und die Qualitätssicherung verantwortlich sein soll. Die Entscheidung über die organisatorische Verortung dieser Serviceeinheit ist jedoch noch nicht getroffen. Zunächst soll die Senatsverwaltung für Integration, Arbeit und Soziales diese Rolle einnehmen.

Die Senatsverwaltung plant, Anfang 2021 ein Pilotprojekt mit zwei Bezirksämtern und dem Landesamt für Flüchtlingsangelegenheiten zu starten. Es soll damit begonnen werden, die Unterkünfte unter Nutzung eines bereits im Land Berlin für einen anderen Zweck verwendeten IT-Fachverfahrens[184] zu vergeben. Die Verantwortung für dieses Verfahren wird die Senatsverwaltung für Integration, Arbeit und Soziales übernehmen.

Aus datenschutzrechtlicher Sicht stellen sich komplexe Fragen: Zum einen ist zu berücksichtigen, dass die Beteiligten jeweils unterschiedliche gesetzliche Aufgaben nach dem Asylrecht, dem Sozialrecht sowie dem Sicherheits- und Ordnungsrecht wahrnehmen. Dies führt dazu, dass auch verschiedene Rechtsgrundlagen für die Zulässigkeit der Verarbeitung personenbezogener Daten in den Blick ge-

184 Es handelt sich hierbei um ein von der Senatsverwaltung für Bildung, Jugend und Familie für die Unterbringung unbegleiteter minderjähriger Ausländer*innen genutztes IT-Verfahren.

nommen werden müssen. Es ist insbesondere zu berücksichtigen, dass es für die bedarfsgerechte Unterbringung auch relevant sein kann, sensitive Daten, z. B. über Erkrankungen oder Behinderungen etc., zu verarbeiten. An die Zulässigkeit der Verarbeitung derartiger Daten sind strenge Anforderungen zu stellen. Zum anderen ist im Hinblick auf das genutzte IT-Fachverfahren durch mehrere Beteiligte genau festzulegen, wer auf welche Daten zugreifen darf, wie die Verantwortlichkeit der Beteiligten untereinander geregelt ist und für welche Verarbeitungen Vereinbarungen über die Auftragsverarbeitung zwischen den Beteiligten zu schließen sind.

Alles in allem bedarf es hier umfangreicher datenschutzrechtlicher Bewertungen. Wir stehen mit der verantwortlichen Senatsverwaltung im Austausch, um die Datenschutzfragen noch vor dem Start des Pilotprojekts zu klären. Auch werden wir die nächsten Projektschritte insbesondere in Bezug auf die mit der geplanten Einrichtung einer „Zentralen Serviceeinheit GStU" verbundenen datenschutzrechtlichen Fragen begleiten und die Senatsverwaltung entsprechend beraten.

6.3 Haushaltsbefragungen und die Sache mit der Anonymität

Aus der Praxis

Durch einen Hinweis wurden wir auf eine geplante Haushaltsbefragung eines Bezirksamts aufmerksam. Der Fragebogen, den nach bestimmten Merkmalen zufällig ausgewählte Bürger*innen freiwillig beantworten sollten, erhielt eine Vielzahl von persönlichen Fragen, deren Detaillierungsgrad eine Identifizierbarkeit der teilnehmenden Bürger*innen für das Bezirksamt zumindest theoretisch möglich machte. Im Anschreiben an die Bürger*innen erweckte das Bezirksamt jedoch den unzutreffenden Eindruck, niemand könne eine Verbindung zwischen den Teilnehmer*innen und deren Antworten herstellen.

Die Befragung richtete sich an Seniorinnen und Senioren und sollte dem Bezirk als Grundlage dafür dienen, seine weiteren Planungen (z. B. zur Wohnraumversorgung, zum Freizeitangebot oder zum Ausbau medizinischer und pflegerischer Dienstleistungen) an den Lebensrealitäten dieser Bevölkerungsgruppe auszurichten. Der beigefügte Fragebogen hatte es dabei allerdings in sich: Abgefragt

wurden z. B. hochgradig detaillierte Angaben zur Person (z. B. Alter, konkrete Höhe des Nettoeinkommens, Jahr des Zuzugs in den Bezirk), zur Wohnsituation (z. B. Zimmer- und Quadratmeteranzahl der Wohnung, Gesamt-, Heiz- und Betriebskosten), zum Gesundheitszustand (z. B. chronische Erkrankungen, Grad einer Behinderung, Pflegegrad) und noch vieles mehr. Eine Identifizierbarkeit der einzelnen Teilnehmer*innen konnte aufgrund dieser Fülle von Informationen daher nicht ausgeschlossen werden. Das ging aus dem begleitenden Anschreiben an die Teilnehmer*innen, mit dem diese über den Hintergrund der Befragung aufgeklärt werden sollten, aber nicht hervor. Vielmehr wurde ursprünglich sogar explizit darauf hingewiesen, dass angeblich niemand eine Verbindung zwischen den Teilnehmer*innen und deren Antworten herstellen könne.

Auf unser Einschreiten hat uns das Bezirksamt mitgeteilt, dass eine Auswertung der Einzelfragebögen durch das Bezirksamt selbst nicht geplant sei. Diese würden zwar an das Be-zirksamt zurückschickt, von diesem aber in verschlossenem Umschlag an einen Dienstleister weitergereicht, der diese maschinell auslese und direkt im Anschluss vernichte. Das Bezirks-amt erhalte lediglich eine nummerische Auswertung. Gleiches gelte für die mit dem Bezirks-amt bei diesem Projekt kooperierende Hochschule, die auf Grundlage dieser Auswertung eine Sozialstudie erstellen solle.

Das Bezirksamt hat das Informationsschreiben für die Bürger*innen sodann geändert und diese Vorgehensweise in einer neuen Version des Anschreibens transparent gemacht. Die Verarbeitung der mit den Fragebögen erhobenen Daten hat sie auf eine Einwilligung der teilnehmenden Bürger*innen gestützt.

Ideal war die Vorgehensweise trotzdem nicht. Zwar hat das Bezirksamt in dem überarbeiteten Anschreiben auf den unzutreffenden Hinweis verzichtet, dass niemand eine Verbindung zwischen den Teilnehmer*innen und deren Antworten herstellen könne. Der Hinweis, dass die Teilnahme an der Studie „anonym“ erfolge, wurde jedoch beibehalten. Dies war bei genauer Betrachtung jedoch weiterhin nicht korrekt. Auch ohne Erhebung der Namen ist die Möglichkeit der Identifizierung einzelner Personen angesichts des Umfangs und des Detaillierungsgrads des Fragebogens keineswegs ausgeschlossen. In diesem Zusammenhang stellte sich daher durchaus die Frage, ob die Einwilligung der betroffenen Personen noch

als Basis für die Datenverarbeitung dienen kann, wenn die Sachlage in diesem Punkt nicht korrekt wiedergegeben wird.[185]

Wir haben das Bezirksamt auf das Problem hingewiesen. Da das Bezirksamt aufgrund der gewählten Verfahrensweise jedoch faktisch keine Kenntnis von den Einzeldatensätzen erhält, sondern die Umschläge vielmehr im verschlossenen Umschlag weiterreicht, haben wir in diesem konkreten Einzelfall unter zwei Bedingungen von weiteren Maßnahmen abgesehen: Das Bezirksamt hat zum einen sicherzustellen, dass auch in tatsächlicher Hinsicht keine Einsicht in die Einzelfragebögen möglich ist. Zum anderen war sicherzustellen, dass die dem Bezirksamt zur Verfügung gestellte „nummerische Auswertung" in einer Weise zusammengefasst ist, dass ein Rückschluss auf einzelne Personen nicht mehr möglich ist. Denn nur in diesem Fall handelt es sich wirklich um anonyme Daten. Zudem haben wir dem Bezirksamt geraten, uns bei zukünftigen Projekten dieses Umfangs frühzeitig in die Planungen einzubeziehen.

Grundsätzlich empfehlen wir, den Detaillierungsgrad bei ähnlichen Umfragen drastisch zu reduzieren, um eine Personenbeziehbarkeit von Beginn an auszuschließen. Wird hiervon kein oder nicht ausreichend Gebrauch gemacht, darf den betroffenen Personen wiederum nicht suggeriert werden, die Studienteilnahme erfolge anonym. Weiterhin ist bei der Gestaltung des Verfahrens von vornherein zu überlegen, ob das Bezirksamt überhaupt als „Empfänger" der Fragebögen in Betracht kommen sollte. Hierzu besteht regelmäßig keine Notwendigkeit, wenn die Befragung nicht durch das Bezirksamt selbst, sondern durch einen Dritten (z. B. eine Hochschule) wissenschaftlich ausgewertet wird.

Haushaltsbefragungen sind grundsätzlich ein legitimes Mittel, um den Bezirken einen Überblick über die Lebensrealitäten einzelner Bevölkerungsgruppen zu verschaffen und ihnen auf diese Weise zu ermöglichen, ihre Planungen hieran auszurichten. Bei allem Wissendurst sind die datenschutzrechtlichen Aspekte bei derartigen Studien jedoch von Beginn an mitzudenken.

185 Eine Einwilligung muss u.a. in „informierter Weise" abgegeben werden, um eine Datenverarbeitung legitimieren zu können; Art. 4 Nr. 11 DS-GVO.

6.4 Abgabe von Behördenakten bei den Nachbarn

Eine Rechtsanwaltskanzlei machte uns darauf aufmerksam, dass der vom Landesamt für Gesundheit und Soziales beauftragte Paketzusteller das Paket mit den Behördenakten, die sensitive Gesundheitsdaten enthielten, bei den Nachbarn abgegeben hatte, da in der Kanzlei niemand angetroffen wurde.

Es stellte sich heraus, dass es sich hier um ein gängiges Verfahren handelte. Wir haben sowohl gegenüber dem Landesamt für Gesundheit und Soziales als auch gegenüber dem für die Organisation der berlinweiten Paketzustellung verantwortlichen Landesverwaltungsamt deutlich gemacht, dass Pakete, die Unterlagen mit sensitiven Daten wie Gesundheitsdaten enthalten können, nur an die jeweiligen Empfänger*innen persönlich oder an benannte Empfangsbevollmächtigte zugestellt werden dürfen. Uns wurde entgegengehalten, dass die vertraglichen Bedingungen es nicht zuließen, die persönliche Zustellung von Paketen zu gewährleisten. Die persönliche Zustellung sei nur bei Briefen möglich.

Nach einem intensiven Austausch mit den beteiligten Behörden konnten wir erreichen, dass nunmehr durch den Abschluss einer Zusatzvereinbarung gewährleistet wird, dass die vom Landesamt für Gesundheit und Soziales in Paketen versandten Akten stets persönlich an die empfangenden Stellen übergeben werden.

6.5 Pflegedienst veröffentlicht Namen von Pflegebedürftigen

Eine Beschwerdeführerin wunderte sich darüber, ihren Namen auf der Internetseite des sie betreuenden Pflegedienstes zu finden. Sie bat uns um Unterstützung.

Es stellte sich heraus, dass der Pflegedienst seine Pflegekräfte in Gruppen für Fortbildungen eingeteilt hatte. Diese Fortbildungsteams benannte der Pflegedienst nach den von ihnen betreuten Pflegebedürftigen. Da der Pflegedienst die Fortbildungspläne für alle Teams auf seiner Webseite abrufbar machte, kam es

zu der Veröffentlichung des Namens der Beschwerdeführerin. Der Pflegedienst erläuterte uns, zur leichteren Zuordnung würden die Teams nach den Namen der zu pflegenden Personen benannt. Wir haben dem Pflegedienst mitgeteilt, dass es sich hier um eine unzulässige Veröffentlichung sensitiver Daten handele und die Daten zu löschen seien.

Der Pflegedienst zeigte sich sehr einsichtig und verwendet seither andere Bezeichnungen für die Fortbildungsteams. Damit wird den Datenschutzbelangen der Beteiligten jetzt Rechnung getragen.

7 Wissenschaft und Forschung

7.1 Die Polizei, dein Freund und Forscher

Bereits seit einigen Jahren ist die Berliner Polizei dabei, im Rahmen eines Forschungsprojekts herauszufinden, mit welchem Testverfahren man Personen in den eigenen Reihen identifizieren kann, die über außergewöhnliche und für den Polizeieinsatz besonders relevante Fähigkeiten bei der Wiedererkennung von Gesichtern verfügen (sog. „Super Recognizer"). Unterstützung erhält die Polizei hierbei von einer auf diesen Themenbereich spezialisierten Wissenschaftlerin der Universität Freiburg (Schweiz). Wir haben die Polizei über den gesamten Zeitraum des Projekts beraten und darauf hingewirkt, dass bei dem Forschungsvorhaben auch die datenschutzrechtlichen Rahmenbedingungen eingehalten werden.

Treffsicher Personen auf Lichtbildern oder Videoaufnahmen wiederzuerkennen, die man nur einmal – vielleicht sogar Jahre zuvor – flüchtig getroffen hat, ist für den weit überwiegenden Teil der Bevölkerung unmöglich. Nicht so für „Super Recognizer", denen genau das regelmäßig gelingen soll. Wie viele Personen tatsächlich über derartige Fähigkeiten verfügen, lässt sich nicht sicher sagen. Schätzungen zufolge sollen es allenfalls ein bis zwei Prozent der Bevölkerung sein.

Dass gerade die Polizei ein besonderes Interesse daran hat, einen Test zur Identifikation von „Super Recognizern" zu entwickeln, verwundert nicht. Nach ihrer Prognose könnten diese Ausnahmetalente die Polizeiarbeit um einiges voranbringen. Zum Beispiel könnten sie eine gesuchte Person auch dann auf den Aufnahmen einer Überwachungskamera identifizieren, wenn diese sich in einer größeren Menschenmenge aufhält. Dies dürfte nicht zuletzt die Rekonstruktion von Fluchtwegen erleichtern und wäre nach Darstellung der Polizei z. B. auch nach dem Anschlag am Breitscheidplatz im Jahr 2016 eine große Hilfe bei der Fahndung gewesen.

Da mit dem Forschungsprojekt erhebliche datenschutzrechtliche Fragen verbunden sind, ist die Polizei bereits frühzeitig auf uns zugekommen und hat uns ihre Überlegungen zur Konzeption des Testverfahrens vorgestellt. Dieses sah vor, dass die Teilnehmer*innen mehrere Module durchlaufen, die ihre Fähigkeiten der Gesichtswiedererkennung in unterschiedlichen Varianten auf die Probe stellen. Zum Beispiel sah ein Modul vor, dass die Proband*innen 20 Bilder guter Qualität von ähnlich aussehenden Personen präsentiert bekommen und darunter eine Zielperson wiederfinden müssen. Nur Personen, die ein Modul bestehen, sollten zum nächsten „vorgelassen" werden.

Das datenschutzrechtliche Problem dabei? Für die Erstellung der Tests wollte die Polizei zum einen auf „Echtdaten" zurückgreifen, also authentisches Bildmaterial verwenden (z. B. aus der Lichtbildvorzeigedatei der Polizei oder aus Ermittlungsakten der Staatsanwaltschaft). Zum anderen wollte sie sich zunutze machen, dass sie mit rund 24.000 Dienstkräften über einen großen Pool an potenziellen Proband*innen verfügt.

Sowohl die Verwendung von Lichtbildern aus Datenbanken der Polizei als auch aus Akten der Berliner Staatsanwaltschaft für Forschungszwecke ist datenschutzrechtlich auch ohne Einwilligung der betroffenen Personen nicht von vornherein ausgeschlossen. Sie ist aber an konkrete Voraussetzungen geknüpft. Dazu gehört insbesondere, dass der Zweck des Forschungsvorhabens nicht auch auf andere Weise erreicht werden kann. Zudem muss das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der betroffenen Personen erheblich überwiegen.[186]

Vor diesem Hintergrund mussten wir den ersten Planungen die datenschutzrechtliche Unzulässigkeit attestieren. Zwar konnte die Polizei plausibel darlegen, dass der Zweck des Forschungsvorhabens nicht auch auf andere Weise erreicht werden kann. Hier spielte insbesondere eine Rolle, dass es nur schwer möglich ist, eine so große Anzahl an Freiwilligen für die Anfertigung von Lichtbildern oder Videoaufnahmen zu gewinnen, um aus diesem Pool wiederum genügend Testpersonen herausfiltern zu können, die die geforderte Ähnlichkeit zueinander aufweisen. Ebenso spielte eine Rolle, dass der Test den tatsächlichen Polizeialltag abbilden

186 Siehe § 35 BlnDSG und § 476 StPO

sollte, die Bilder also möglichst authentisch aussehen mussten (z. B. durch unterschiedliche Qualitäten).

Allerdings fiel die ebenfalls notwendige Abwägungsentscheidung hier zunächst zulasten der Polizei aus. Dass ein gewichtiges öffentliches Interesse an der Durchführung des Forschungsvorhabens besteht, haben wir zwar nicht in Abrede gestellt. Jedoch war zu berücksichtigen, dass mit den Bildern zugleich die potenziell stigmatisierende Information verbunden war, dass die abgebildeten Personen in der Vergangenheit erkennungsdienstlich behandelt worden waren. Zudem war das schutzwürdige Interesse der betroffenen Personen bei der ursprünglichen Planung insbesondere dadurch in besonderem Maße beeinträchtigt, dass die Lichtbilder bis zu 24.000 Dienstkräften – dies entspricht der Einwohnerzahl einer Kleinstadt – vorgeführt werden sollten.

Wir haben allerdings auch signalisiert, dass die Abwägung zugunsten des Forschungsinteresses ausfallen könnte, wenn weit weniger Proband*innen mit „Echtdaten" konfrontiert würden. Wir haben vorgeschlagen, z. B. einen Vortest in den Studienaufbau zu integrieren, der kein authentisches Material enthält und mit dem von vornherein zumindest diejenigen Teilnehmer*innen herausgefiltert werden können, die definitiv nicht über die gesuchten besonderen Fähigkeiten verfügen.

Von der Polizei entwickelt wurde schließlich folgendes Verfahren: Entscheiden sich die Vollzugskräfte der Polizei für eine Teilnahme, müssen sie jetzt einen aus drei Einzeltests bestehenden Vortest absolvieren, der kein Material aus den Datenbanken der Polizei oder Akten der Staatsanwaltschaft enthält. Nur Personen, die in allen drei Tests ein bestimmtes Niveau erreichen, können dann in der Folge auch das erste Testmodul mit authentischem Bildmaterial absolvieren. Zudem ist die datenschutzrechtliche Eingriffsintensität des ersten Testmoduls reduziert worden. Nunmehr ist vorgesehen, dass in das authentische Bildmaterial auch Bilder von Freiwilligen eingestreut werden. So ist für die Proband*innen nicht ersichtlich, ob die ihnen gezeigten Personen tatsächlich einmal erkennungsdienstlich behandelt worden sind. Die schutzwürdigen Belange der betroffenen Personen sind damit weit weniger beeinträchtigt.

Im Ergebnis haben wir uns mit dieser Vorgehensweise einverstanden erklärt. Diese Bewertung bezieht sich jedoch ausschließlich auf die Verarbeitung der in Rede stehenden Daten für das durchgeführte Forschungsprojekt. Ist das Ziel des Projekts erreicht, also die Entwicklung eines wissenschaftlich validen Testverfahrens zur Identifikation von „Super Recognizern" für den Polizeieinsatz, wird eine neue Bewertung erforderlich. Die im Rahmen des Tests verwendeten personenbezogenen Daten können im Anschluss nicht dafür herangezogen werden, weitere „Super Recognizer" in den Reihen der Berliner Polizei, bei Polizeibehörden anderer Länder oder etwa beim Bundeskriminalamt zu identifizieren. Denn die reine Identifikation von „Super Recognizern" zum Zwecke des Einsatzes im Polizeidienst dient nicht mehr der wissenschaftlichen Forschung.

Auch personenbezogene Daten, die sich in Akten und Datenbanken der Polizei und Staatsanwaltschaft befinden, sind für die Forschung nicht in jedem Fall tabu. Hier ist jedoch von vornherein ein besonderes Augenmerk darauf zu richten, dass die schutzwürdigen Belange der betroffenen Personen besondere Beachtung finden.

7.2 Forschung in Jugendämtern – „Was machen Sie denn da gerade so?"

Aus der Praxis

Die Senatsverwaltung für Bildung, Jugend und Familie hat uns darüber informiert, dass sich eine niedersächsische Hochschule dafür interessiere, eine Studie in Berliner Jugendämtern durchzuführen. Da hierbei auch datenschutzrechtliche Fragestellungen auftraten, hat sie uns um Beratung gebeten.

Zielobjekt der Studie sind nicht Kinder oder Jugendliche, sondern die Mitarbeiter*innen der Jugendämter selbst. So soll analysiert werden, wie die von den Beschäftigten benutzten IT-Anwendungen die Fallbearbeitung und Entscheidungsfindung beeinflussen.

Für die Untersuchung sollten verschiedene Methoden eingesetzt werden. Neben Interviews mit den Beschäftigten sollte ihnen im wahrsten Sinne des Wortes auch über die Schulter geschaut werden. Doch damit nicht genug – auch ein phasenweises Abfilmen der Monitore gehörte zum Studiendesign.

Bei den Daten, die in den Jugendämtern verarbeitet werden, handelt es sich um besonders schützenswerte Sozialdaten. Eine Übermittlung dieser Daten – und dazu zählt auch die Ermöglichung der Kenntnisnahme und des Abfilmens durch Dritte – ist nur unter den engen Voraussetzungen des Sozialgesetzbuchs (SGB)[187] zulässig. Zu diesen Voraussetzungen zählt vor allen anderen, dass die Übermittlung der Daten für ein bestimmtes Vorhaben der wissenschaftlichen Forschung[188] auch tatsächlich erforderlich sein muss. Schon daran scheiterte es hier.

So konnten wir dem Konzept der Forscher*innen entnehmen, dass die Bildschirme abgefilmt werden sollen. Auf Nachfrage stellte sich jedoch heraus, dass es für die Forscher*innen lediglich um die Interaktion der Beschäftigten mit der Software ging; die personenbezogenen Daten selbst waren für sie ohne Bedeutung. Diese sollten nach den Planungen vor der eigentlichen Auswertung ohnehin unkenntlich gemacht werden.

Infolge unseres Hinweises, dass wir das Abfilmen vor diesem Hintergrund für unzulässig halten, hat die Hochschule ihr Konzept geändert. Nunmehr wird auf das Abfilmen der Monitore verzichtet. Stattdessen sollen die Mitarbeiter*innen ihr Handeln verbal kommentieren, also ähnlich einem Selbstgespräch mitteilen, was sie gerade machen.[189]

Unter der Voraussetzung, dass die Beschäftigten im Vorhinein sehr genau instruiert werden, bei ihrer Kommentierung keine Sozialdaten preiszugeben, und die Wissenschaftler*innen auch bei ihren Beobachtungen vor Ort diese Daten nicht zur Kenntnis bekommen, haben wir uns mit dem Vorgehen einverstanden erklärt.

Die Verarbeitung der personenbezogenen Daten der Jugendamtsmitarbeiter*innen (z. B. im Rahmen der Interviews) ist wiederum nur auf Basis ihrer Einwilligung möglich. In diesem Zusammenhang haben wir deutlich gemacht, dass die

187 Siehe insbesondere § 75 SGB X

188 Konkret muss es sich um ein Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich oder der wissenschaftlichen Arbeitsmarkt- und Berufsforschung handeln.

189 Methode „Thinking out loud“. Beispiel: “Ich habe hier einen Fall, der schon einmal als kritisch eingeschätzt wurde. Ich klicke jetzt auf das Feld XY, um nachzusehen, was damals der Meldegrund war.“

Einwilligung nur dann als Grundlage für die Datenverarbeitung dienen kann, wenn diese auch auf einer freien Entscheidung der Mitarbeiter*innen beruht. Gerade im Beschäftigtenkontext ist dabei sicherzustellen, dass die Fachkräfte keine Nachteile ihres Arbeitsgebers befürchten müssen, wenn sie sich gegen eine Teilnahme entscheiden.

Wir begrüßen, dass die Senatsverwaltung für Bildung, Jugend und Familie uns rechtzeitig in das Projekt über die Arbeit der Beschäftigten von Jugendämtern mit IT-Anwendungen eingebunden hat. Auf diese Weise konnte eine sachgerechte Lösung gefunden werden.

8 Beschäftigtendaten-schutz, Gewerkschaften, Personalvermittlungen

8.1 360-Grad-Feedback am Arbeitsplatz

Bei einem sog. 360-Grad-Feedback wird die Arbeitsleistung von Beschäftigten durch mehrere Personen bewertet, die sich teilweise in höheren und teilweise in niedrigeren Positionen befinden. Einer möglicherweise genaueren Einschätzung der Arbeitsleistung steht die Gefahr gegenüber, dass die Verarbeitung personenbezogener Daten unzulässig ausgeweitet wird.

Normalerweise erhalten Beschäftigte in regelmäßigen Abständen Leistungsbeurteilungen durch Vorgesetzte. Bezogen auf Führungskräfte besteht seit einigen Jahrzehnten die Tendenz, verschiedene Sichtweisen auf deren Arbeit einzuholen: Ergänzend zu der Einschätzung durch Vorgesetzte wird eine Selbsteinschätzung der Führungskraft abverlangt; zudem geben Mitarbeiterinnen und Mitarbeiter sowie Kolleginnen und Kollegen aus anderen Teilen des Unternehmens eine Beurteilung zu der jeweiligen Person ab. Abhängig von den angewandten Methoden kann so ein umfassenderes Bild der Tätigkeit der Führungskraft entstehen. Bei Führungskräften ist anerkannt, dass aufgrund ihrer Position diese Art der Leistungsbeurteilung grundsätzlich zulässig ist.

Neuerdings wird dieses Konzept bisweilen auch auf Beschäftigte ohne oder mit nur untergeordneten Führungsaufgaben übertragen. Auch hier wird ein Dreiklang aus Bewertungen eingeholt: Zunächst eine Selbsteinschätzung, dann Einschätzungen von Kolleginnen und Kollegen aus unterschiedlichsten Bereichen und schließlich eine Bewertung durch Vorgesetzte. Die Unternehmen, die dieses Verfahren einsetzen, verfolgen dabei ähnliche Ziele wie auch in Bezug auf Führungskräfte. Das Feedback soll insgesamt umfassender und zutreffender sein, Beschäftigte mit besonderen Fähigkeiten oder Förderbedarfen können im Anschluss gezielt angesprochen und besser ihren Fähigkeiten entsprechend eingesetzt werden.

So vorteilhaft solche Verfahren auf der einen Seite bei der beständigen Entwicklung von Organisationen sein können, so problematisch kann auf der anderen Seite die Bewertung durch mehrere Personen für die einzelnen Beschäftigten sein. Anders gesagt: Eine beschäftigte Person muss im Zweifel nicht nur bei Begegnungen mit der Chefin oder dem Chef jederzeit damit rechnen, dass ihr Verhalten das nächste Zeugnis beeinflusst, sondern auch bei jeder Begegnung mit einer anderen Person des Unternehmens, da auch diese Begegnungen Auswirkungen auf die nächste Beurteilung und damit auch auf das weitere Berufsleben haben könnten. Die Folge kann ein permanenter Überwachungsdruck und Stress sein, der sich aus der Sorge um das berufliche Fortkommen ergibt.

In dem von uns geprüften Verfahren haben Beschäftigte in Absprache mit ihren unmittelbaren Vorgesetzten mitentschieden, wer sie bewerten soll. Die Vorgesetzten konnten vereinzelt Personen ablehnen, wenn sie diese für ungeeignet hielten. Gleichzeitig sollten sie darauf achten, dass die Auswahl möglichst unterschiedliche Personen und Funktionen umfasst. Alle Beschäftigten wurden darin geschult, nur berufliche Kontexte in die Bewertung einzubeziehen und bei der Bewertung insgesamt möglichst rücksichtsvoll und sachlich vorzugehen. Vor allem sollte die Arbeit der zu Bewertenden beschrieben werden. Bei der Einführung des Verfahrens konnten zudem auf einer Skala Punkte für Stärken und Schwächen vergeben werden.

Die auf diese Weise abgegebenen Bewertungen wurden von den Vorgesetzten gesichtet und durch eine eigene zusammenfassende Einschätzung ergänzt, die auch abweichen konnte. Die abschließende Entscheidung über die Bewertung traf ein spezielles Gremium, die der bewerteten Person auch das Ergebnis mitteilte. Bei Unstimmigkeiten konnte ein Schlichtungsgremium eingeschaltet werden. Eine Nichtteilnahme am Verfahren, ob als bewertende oder bewertete Person, hatte bislang keine negativen Auswirkungen.

Ein 360-Grad-Feedback ist nicht grundsätzlich unzulässig, allerdings müssen datenschutzrechtliche Vorgaben eingehalten werden. Das heißt vor allem, dass am Arbeitsplatz kein dauerhafter Überwachungsdruck entstehen darf, dass auf den Grundsatz der Datenminimierung geachtet wird und dass die klassischen Betroffenenrechte, wie z. B. das Recht auf Auskunft, sichergestellt werden müssen.

Auf diese Vorgaben hin haben wir das konkrete System überprüft und das Unternehmen aufgefordert, diverse Veränderungen vorzunehmen. Dieser Aufforderung ist es nachgekommen.

Um einem permanenten Überwachungsdruck der Beschäftigten entgegenzuwirken und die Datenverarbeitung einzuschränken, wurde auf unsere Empfehlung hin die Zahl der Personen, die eine andere Person bewerten, auf drei reduziert. Darüber hinaus muss die zu bewertende Person nunmehr mit den Personen, die sie bewerten, auch einverstanden sein. Die betroffene Person kann die sie Bewertenden nun häufig nicht nur selbst vorschlagen, sondern im Zweifel auch ein Veto gegen ihr unliebsame Personen einlegen.

Bei Inhalt und Umfang der Bewertungen war festzustellen, dass die Bewertenden sich an die Vorgaben gehalten haben und keine unnötigen oder sachfremden Erwägungen in die Bewertungen haben einfließen lassen. Die Punkteskala wurde von dem Unternehmen selbst als wenig zielführend erkannt und abgeschafft. Die Speicherdauer der Bewertungen wurde deutlich reduziert, indem von der Datenspeicherung über mehrere Zyklen hinweg Abstand genommen wurde. Nun kann grundsätzlich nur noch auf die Bewertungen des vorangegangenen Zyklus zurückgegriffen werden, um Entwicklungen und Unstimmigkeiten ggf. nachvollziehen zu können. Hiervon ausgenommen ist das Endergebnis: Dieses darf wie ein reguläres Arbeitszeugnis zur Personalakte genommen und für die Dauer des Beschäftigungsverhältnisses gespeichert werden.

Etwas komplizierter war die Frage, wie mit Auskunftsersuchen der Beschäftigten umzugehen ist. Das Unternehmen hielt es für problematisch, dass Bewertete Einsicht in alle erstellten Bewertungen und ggf. auch in die Kommentare der am Ende beratenden Gremien erhalten. Eine Sorge war, dass sich die Bewertenden bei einem umfassenden Auskunftsrecht unter Umständen nicht mehr trauen würden, die Bewertung ehrlich zu formulieren. Befürchtet wurden auch unliebsame Auswirkungen auf die Persönlichkeitsrechte der Bewertenden. Da die bewertenden Personen jedoch eine Aufgabe des Arbeitgebers wahrnehmen, indem sie Vorarbeiten zu einem Arbeitszeugnis leisten, können ihre Rechte nicht pauschal überwiegen. Wir haben jedoch zwei Einschränkungen als zulässig angesehen: Zum einen ist es möglich, eine vollständige Auskunft erst nach Abschluss des Bewertungszyklus zu erteilen, damit der Bewertungsprozess nicht beeinflusst

wird. Zum anderen muss keine Auskunft über die Bewertungen untergeordneter Personen gegeben werden, da diese sonst Bedenken haben könnten, eine solche Aufgabe zu übernehmen und eine Bewertung abzugeben.

Nach wie vor haben Beschäftigte, die weder als Bewertete noch als Bewerter*innen an dem Bewertungssystem teilnehmen wollen, keine Nachteile zu befürchten.

Aufgrund der Umstrukturierung des Verfahrens halten wir dieses in seiner aktuellen Form nun für zulässig.

Einschätzungen von Kolleginnen und Kollegen dürfen in die Bewertung der Arbeitsleistung von Beschäftigten einfließen, wenn Ablauf und Inhalt den Betroffenen transparent gemacht wird, personenbezogene Daten nur im erforderlichen Umfang erhoben und gespeichert werden und ein dauerhafter Überwachungsdruck vermieden wird.

8.2 Begrenzt das Datenschutzrecht die Kollektivrechte von Beschäftigten?

Aus der Praxis

Eine Gewerkschaft hat mit ihrem Gesamtbetriebsrat eine Betriebsvereinbarung geschlossen, durch die zusätzlich zu den gesetzlich normierten Personalvertretungsgremien die Position einer Frauen- und Gleichstellungsbeauftragten sowohl auf Bezirks- als auch auf Bundesebene geschaffen wurde. Nach Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) war die Gewerkschaft der Auffassung, dass sie diesen Frauen- und Gleichstellungsbeauftragten nicht weiterhin personenbezogene Daten wie bspw. Bewerbungsunterlagen übermitteln dürfe.

Die Gewerkschaft vertrat die Auffassung, dass es für die Übermittlung der Unterlagen keine gesetzliche Grundlage mehr gebe. Nur gesetzlich vorgeschriebene Gremien wie etwa Betriebsräte oder Schwerbehindertenvertretungen dürften diese Unterlagen erhalten.

Sowohl das europäische Datenschutzrecht wie auch das Bundesdatenschutzgesetz (BDSG) erlauben die Verarbeitung von Daten auf der Grundlage von Kollek-

tivvereinbarungen, insbesondere zur Sicherstellung von Gleichheit und Diversität am Arbeitsplatz, zur Wahrung von Kollektivrechten und zur Wahrnehmung der Rechte von Beschäftigtenvertretungen.[190]

Die hier in Rede stehende Betriebsvereinbarung stellt eine solche Kollektivvereinbarung dar. Die Frauen- und Gleichstellungsbeauftragten sind, wenn auch gesetzlich nicht vorgeschrieben, im innerbetrieblichen Kontext mit Rechten ausgestattete Personalvertretungen. In der Betriebsvereinbarung wurden diese wie Betriebsratsmitglieder zur Verschwiegenheit verpflichtet. Damit wird dem Schutz der Persönlichkeitsrechte Betroffener Rechnung getragen. Aus dem Datenschutzrecht ergeben sich weder Begrenzungen für die Rechte von Beschäftigtenvertretungen noch Beschränkungen auf gesetzlich vorgeschriebene Gremien.[191]

Wenn zusätzliche Beschäftigtenvertretungen durch Kollektivvereinbarungen eingerichtet werden, beschränkt das Datenschutzrecht die Arbeit dieser Vertretungen nicht und steht insofern der Teilhabe von Beschäftigten am Betriebsablauf nicht entgegen.

8.3 Datenpanne oder Taktik?

Eine Personalvermittlung versendete im Laufe eines Jahres Daten von Arbeitsuchenden durch unverschlüsselte E-Mails an Dritte und erklärte, dies sei geschehen, weil man die Kontrolle über die Technik verloren habe.

Uns hat eine größere Anzahl von Hinweisen erreicht, wonach Unternehmen ungebeten von einer Personalvermittlung Lebensläufe von Bewerber*innen per E-Mail zugesandt bekommen haben – oft mit Bild, Alter und einer Vielzahl weiterer persönlicher Angaben. Die Empfängerinnen und Empfänger der E-Mails haben die Personalvermittler*innen teilweise mehrfach aufgefordert, keine weiteren E-Mails mehr zu senden, dies hatte jedoch keinen Erfolg. Auf unsere Nachfrage hin konnte die Personalvermittlung diese Datenübermittlungen nicht erklären.

190 Art. 88 Abs. 1 DS-GVO und § 26 Abs. 1 Satz 1 BDSG
191 Siehe § 26 Abs. 6 BDSG

Es stellte sich heraus, dass das Unternehmen die Bewerbungsdaten in einer veralteten Datenbank auf kaum gesicherten Servern gespeichert hatte. Eine aktuelle Dokumentation des Systems konnte nicht vorgelegt werden. Es ließ sich nicht feststellen, ob einzelne Beschäftigte oder Außenstehende dem Unternehmen schaden wollten oder ob das wahllose Versenden dieser E-Mails sogar vom Unternehmen selbst erwünscht war, um einen möglichst großen Kreis an Empfängerinnen und Empfängern auf die Arbeitssuchenden aufmerksam zu machen. Selbst wenn ein technischer Fehler vorgelegen haben sollte, wäre es jedenfalls sehr bedenklich gewesen, dass die Personalvermittlung trotz Kenntnis der Probleme über Monate hinweg ihrer Tätigkeit weiter nachgegangen ist, ohne etwas zu unternehmen.

Bewerbungsunterlagen dürfen von Personalvermittlungen nur unter engen Voraussetzungen an Dritte übermittelt werden. Meist ist die Grundlage eine Einwilligung der Bewerber*innen. Solche Einwilligungserklärungen müssen jedoch genau formulieren, wofür sie abgegeben werden, etwa für die Übermittlung von Unterlagen an ein einzelnes Unternehmen oder an verschiedene Unternehmen einer einzelnen Branche. Da Einwilligungen nur wirksam erteilt werden können, wenn die Betroffenen verstehen, worum es dabei geht, müssen sie immer möglichst konkret gefasst werden. Wer nicht weiß, an wen ihre oder seine Daten übermittelt werden, kann dieser Übermittlung auch nicht wirksam zustimmen.

Es ist empfehlenswert, wenn Personalvermittlungen Bewerbungen in einem zweistufigen Verfahren übermitteln: Zunächst werden an interessierte Unternehmen nur allgemeine und möglichst anonymisierte Informationen zu der Kandidatin oder dem Kandidaten übermittelt. Dies können etwa Angaben zu den Fähigkeiten, zur Berufserfahrung o. Ä. sein. Ist das Unternehmen aufgrund dieser allgemeinen Angaben an einer bestimmten Person interessiert, können in einer zweiten Stufe – i. d. R. auf Basis einer Einwilligung der Betroffenen – die vollständigen Bewerbungsunterlagen übermittelt werden. So kann verhindert werden, dass unnötig viele personenbezogene Daten an Unternehmen verschickt werden, die hieran überhaupt kein Interesse haben.

In diesem Fall bestand darüber hinaus das Problem, dass die Personalvermittlung personenbezogene Daten an Unternehmen verschickt hat, die schon mehrfach mitgeteilt hatten, diese Information nicht erhalten zu wollen. Darüber hinaus ist

es problematisch, derartige Unterlagen unverschlüsselt per E-Mail zu versenden. Eine Personalvermittlung muss sich sicherer Übermittlungswege für diese Unterlagen bedienen. Den Vorgang haben wir zur Prüfung eines Bußgeldverfahrens an unsere Sanktionsstelle abgegeben.

Personalvermittlungen sind in besonderem Maße dazu verpflichtet, sorgfältig mit den Daten von den Personen umzugehen, die sie vermitteln wollen.

8.4 Welcome-Back-Gespräche

An einem Logistikstandort werden Beschäftigte, nachdem sie aufgrund von Krankheit abwesend waren, regelmäßig mit einem sog. „Welcome-Back-Gespräch" begrüßt. Hier war zunächst fraglich, ob von Seiten der Arbeitgeberin Gesundheitsdaten erhoben werden.

Die Gespräche finden immer dann statt, wenn Beschäftigte von einer krankheitsbedingten Abwesenheit zurückkehren. Sie sollen den Beschäftigten unmittelbar nach ihrer Rückkehr angeboten und nur auf freiwilliger Basis geführt werden. Zweck der Gespräche ist es, die Arbeitsfähigkeit der Beschäftigten zu erhalten und den Arbeitsplatz langfristig zu sichern. Bezug genommen werden soll in den Gesprächen aber nicht auf die Krankheit, sondern ausschließlich auf die Arbeitssituation, die Arbeitstätigkeit und das Betriebsklima.

Der Logistikstandort hat mit dem Betriebsrat eine Vereinbarung zu dem genauen Verlauf der Gespräche getroffen. Hiernach gibt es zwei Arten von Gesprächen: Bei einer Abwesenheit von bis zu sieben Tagen begrüßen die Vorgesetzten die Beschäftigten und erkundigen sich nach dem Befinden. Der zweite Gesprächstyp wird bei einer Abwesenheit von mehr als sieben Tagen angeboten und innerhalb der ersten fünf Tage nach Rückkehr geführt. Thema ist hier, ob betriebsbedingte Gründe für die Ausfallzeiten verantwortlich sind. Solche Gründe werden ggf. dokumentiert. Sofern keine betriebsbedingten Gründe für die Abwesenheit verantwortlich sind, wird das Gespräch nicht weitergeführt und auch nicht dokumentiert. Sollten betriebsbedingte Gründe vorliegen, sollen die Vorgesetzten versuchen, diese möglichst zu beseitigen. Alle Vorgesetzten, die diese Gespräche führen, erhalten eine Einweisung für die Gesprächsführung.

Bezüglich Art und Ausgestaltung der Gespräche konnten wir keinen Verstoß gegen das Datenschutzrecht feststellen. Die Betriebsvereinbarung regelt den Verlauf und Zweck der Gespräche eindeutig. Im Rahmen der Fürsorgepflicht im Arbeitsverhältnis ist die beschriebene Datenerhebung zulässig.

Ein*e Arbeitgeber*in ist befugt, sich nach dem allgemeinen Befinden ihrer oder seiner Beschäftigten in Bezug auf das Arbeitsverhältnis zu erkundigen. Gesundheitsdaten dürfen jedoch nur unter engen Voraussetzungen erhoben werden.

8.5 Das Arbeitsverhältnis wurde beendet, weil ...

Aus der Praxis

Immer wieder erreichen uns Beschwerden darüber, dass Arbeitgeber*innen die Gründe für die Beendigung eines Arbeitsverhältnisses Dritten mitteilen. Gerade wenn den Betroffenen gekündigt wurde, führt das Informieren der Belegschaft, der Kund*innen oder dem Unternehmen nahestehender Dritter über die Kündigung zu Unmut.

In einem uns bekannt gewordenen Kündigungsfall ging der Beschäftigte mit einer Kündigungsschutzklage gegen die Kündigung vor. Das Klageverfahren wurde mit einem Vergleich beendet. Kurz darauf versandte die Geschäftsführung an ca. ein Dutzend Angestellte des Unternehmens eine einseitige Stellungnahme zu dem Ausgang des Verfahrens. Das Schreiben enthielt auch die Gründe, weshalb die Person aus Sicht der Arbeitgeberin nicht weiterbeschäftigt werden konnte. Abgeschlossen wurde das Schreiben mit dem Hinweis, dass die Information innerhalb des Betriebs weitergegeben und der Inhalt auch weiteren dem Betrieb verbundenen Personen mitgeteilt werden dürfe. Die Verantwortliche wollte nach ihren Angaben mit der Information den Betriebsfrieden wiederherstellen und Zweifel darüber ausräumen, ob die Kündigung berechtigt war.

Daten von Beschäftigten dürfen nur verarbeitet werden, sofern dies für die Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.[192] Für

192 § 26 Abs. 1 Satz 1 BDSG

die Beendigung eines Beschäftigungsverhältnisses ist es jedoch nicht notwendig, dass andere Personen über die Gründe informiert werden. Die Benachrichtigung der anderen Angestellten ist auch nicht für die Durchführung von deren Beschäftigungsverhältnissen erforderlich.

Das Interesse der Arbeitgeberin bestand vorliegend darin, durch Informationen den Betriebsfrieden wiederherzustellen. Dies ist ein berechtigtes Interesse. Die Information der Belegschaft kann selbstverständlich dazu dienen, Unklarheiten auszuräumen. Dem steht jedoch in aller Regel das überwiegende Interesse der Person entgegen, die das Unternehmen verlassen muss. Scheiden Personen aus einem Unternehmen aus, haben sie in der Regel auch keine Möglichkeit, ihre Sichtweise darzustellen. Gerade wenn das Arbeitsverhältnis nicht einvernehmlich beendet wurde, wird oft jede weitergehende Information über die Beendigung des Arbeitsverhältnisses von den Betroffenen als schwere Verletzung des eigenen Ansehens betrachtet. Einer Kündigung gehen nicht selten längere Konflikte voraus. Eine Veröffentlichung der Kündigungsgründe und grundsätzlich auch der Kündigung ist geeignet, ernsthafte Zweifel an der Integrität der gekündigten Person aufkommen zu lassen.

Somit werden mit solchen Mitteilungen die schutzwürdigen Interessen der Betroffenen regelmäßig schwer beeinträchtigt. Die Arbeitgeberin oder der Arbeitgeber muss daher den Betriebsfrieden auf anderem Wege wiederherstellen. Nur in absoluten Ausnahmefällen wäre die Mitteilung näherer Informationen denkbar. Im vorliegenden Fall wurde das Verfahren zur Prüfung, ob eine Geldbuße verhängt werden soll, an unsere Sanktionsstelle abgegeben.

Aus Sicht der Arbeitgeberin bzw. des Arbeitgebers mag es im Einzelfall sinnvoll sein, Beweggründe für eine Kündigung im Betrieb zu veröffentlichen. Trotzdem ist in aller Regel die Information, dass das Arbeitsverhältnis mit einer oder einem Beschäftigten zu einem bestimmten Zeitpunkt beendet wurde, das Einzige, was ein Arbeitgeber bzw. eine Arbeitgeberin den Beschäftigten mitteilen darf.

9 Wohnen

9.1 Kein Datenschutz bei Zweckentfremdung?

Aus der Praxis

Von einem Bezirksverordneten sind wir darauf aufmerksam gemacht worden, dass Defizite beim Schutz der Daten derjenigen Personen bestehen, die nach dem Zweckentfremdungsverbot-Gesetz (ZwVbG) verbotene Wohnungsnutzungen anzeigen.

Das Gesetz wendet sich gegen die Wohnungsknappheit in Berlin und verbietet es z. B. unter bestimmten Umständen, eine Wohnung als Ferienwohnung zu nutzen und so dem regulären Wohnungsmarkt zu entziehen. Zuständig für die Durchführung dieses Gesetzes sind die Bezirksämter. Diese nehmen auch Hinweise etwa aus der Nachbarschaft entgegen, wenn es Anzeichen für die verbotene Nutzung einer Wohnung als Ferienwohnung gibt. Eine solche Anzeige kann entweder direkt beim Bezirksamt oder über ein von der Senatsverwaltung für Stadtentwicklung und Wohnen angebotenes Internetportal erfolgen.

In dem von dem Bezirksverordneten geschilderten Fall hatte ein Mieter von dieser Möglichkeit Gebrauch gemacht und eine mutmaßliche Ferienwohnung in seinem Mietshaus angezeigt. Im Rahmen des nun folgenden Verfahrens soll das Bezirksamt dem Eigentümer der mutmaßlichen Ferienwohnung im Rahmen der Akteneinsicht den Namen des Anzeigeerstatters offenbart haben. Das war für diesen höchst problematisch, da es sich bei dem Eigentümer gleichzeitig um seinen eigenen Vermieter handelte. Außerdem sei er bei seiner Anzeige nicht darauf hingewiesen worden, dass seine Daten möglicherweise an den Vermieter weitergegeben würden, sonst hätte er womöglich auf eine Anzeige verzichtet.

Wir haben uns in den Fall eingeschaltet und konnten feststellen, dass die geschilderte Vorgehensweise eine gängige Praxis in dem Bezirksamt war. Auf unser Einschreiten hin hat das Bezirksamt zugesagt, dass Personen, die eine Anzeige erstatten, künftig über die Datenverarbeitung ordnungsgemäß aufgeklärt werden.[193]

193 Siehe Art. 13 Datenschutz-Grundverordnung (DS-GVO)

Dazu gehören insbesondere auch Informationen darüber, an welchen Empfängerkreis ihre Daten übermittelt werden.[194] Ebenso muss darüber aufgeklärt werden, dass man einer Datenübermittlung auch widersprechen kann.[195]

Falls die Anzeige erstattende Person in Kenntnis dieser Sachlage dennoch ihre Daten angibt, muss sie unter Umständen damit rechnen, dass diese auch im Rahmen von Akteneinsichtsanträgen an Verfahrensbeteiligte und Dritte weitergegeben werden. Die einschlägigen Be-stimmungen über die Akteneinsicht sehen eine Abwägung zwischen dem Informationsinteresse eine*r Antragsteller*in auf Akteneinsicht auf der einen und den Geheimhaltungsinteressen der betroffenen Person auf der anderen Seite vor.[196] Diese Abwägung ist in jedem Einzelfall durch das Bezirksamt durchzuführen. Dabei muss das Bezirksamt auf der einen Seite berücksichtigen, ob Anzeigeerstattende ggf. Repressalien befürchten müssen, insbesondere falls sie sich gegen ihre eigenen Vermieter*innen wenden. Auf der anderen Seite enthält das hier anzuwendende Informationsfreiheitsgesetz (IFG) eine Regelvermutung, nach welcher über Namen und Anschrift von Anzeigeerstattenden im Zweifel Auskunft zu erteilen ist.[197]

Das Bezirksamt hat uns versichert, dass diese Abwägung zukünftig durchgeführt wird. Zusätzlich soll in dem von der Senatsverwaltung für Stadtentwicklung und Wohnen angebotenen Internetportal die Möglichkeit eingeführt werden, Anzeigen auch anonym zu erstatten.

Personen, die eine Ferienwohnung anzeigen, sollte bewusst sein, dass ihre Daten im Rahmen der Akteneinsicht ggf. an Verfahrensbeteiligte weitergegeben werden müssen. Das Bezirksamt ist verpflichtet, darüber aufzuklären und im Falle einer Akteneinsicht eine Abwägung zwischen dem Geheimhaltungsinteresse der Anzeige erstattenden Person und dem Informationsinteresse Dritter durchzuführen. Auch andere Bezirksämter sollten überprüfen, ob die Erstatter*innen von Anzeigen ordnungsgemäß nach Art. 13 DS-GVO aufgeklärt werden.

194 Art. 13 Abs. 1 lit. e DS-GVO
195 Art. 21 DS-GVO
196 § 6 Abs. 2 VwVfG Bln i. V. m. § 6 Abs. 2 Informationsfreiheitsgesetz (IFG)
197 § 6 Abs. 2 Nr. 1 lit. b IFG Bln

9.2 Haushaltsbefragungen zu Milieuschutzgebieten

Aus der Praxis

Seit einiger Zeit haben die Bezirke die Möglichkeit, sog. Milieuschutzgebiete zu bestimmen. Dadurch soll sichergestellt werden, dass die Bewohner*innen dort bleiben können, wo die Infrastruktur vorhanden ist, die sie im Alltag brauchen. So soll verhindert werden, dass sich durch teure Modernisierungsmaßnahmen, durch Veränderungen der Struktur einer Wohnung, durch die Umnutzung von Wohnungen in Gewerbe oder die Umwandlung von Miet- in Eigentumswohnungen die Zusammensetzung der Wohnbevölkerung durch Verdrängung verändert.

Um zu prüfen, ob ein bestimmtes Wohngebiet als Milieuschutzgebiet eingestuft werden kann,[198] führen die Bezirksämter Haushaltsbefragungen durch. Dabei wird eine Vielzahl von Einzelangaben erhoben, wie z. B. Alter, Geschlecht, Nationalität, Beruf, höchster Bildungsstand, monatliches Haushaltseinkommen sowie Angaben zur Wohnsituation und den in der Wohnung lebenden Personen (allein, Wohngemeinschaft, Paar, volljährige oder minderjährige Kinder). Die Teilnahme an einer solchen Haushaltsbefragung ist zwar freiwillig, allerdings müssen trotzdem die datenschutzrechtlichen Voraussetzungen eingehalten werden.

In dieser Hinsicht haben wir bei einer Haushaltsbefragung durch ein Bezirksamt mehrere Mängel festgestellt. Am schwersten wog dabei, dass die Betroffenen nicht korrekt über die Datenverarbeitung aufgeklärt wurden.[199] So wurde den Betroffenen insbesondere unzutreffend mitgeteilt, dass die Angaben anonym erfasst werden. Dabei waren aufgrund der detaillierten Abfragen durchaus Rückschlüsse auf die Betroffenen möglich, zumal die Erhebung hausblockweise erfolgte. Außerdem hat sich das Bezirksamt eines privaten Unternehmens bedient, das die Umfrage durchgeführt hat. Dies ist zwar grundsätzlich zulässig, allerdings muss dann mit dem Unternehmen ein Auftragsverarbeitungsvertrag abgeschlossen werden, der den sicheren Umgang mit den Daten regelt.[200] An einem solchen fehlte es hier.

198 Siehe § 172 Abs. 1 Nr. 2 Baugesetzbuch (BauGB)
199 Siehe Art. 13 DS-GVO
200 Siehe Art. 28 DS-GVO

Wir haben das Bezirksamt auf diese Mängel hingewiesen. Es zeigte sich kooperativ und hatte die in Rede stehenden Daten bereits so zusammengefasst, dass keine Rückschlüsse auf die betroffenen Personen mehr möglich waren. Außerdem wurde uns versichert, dass zukünftig die Betroffenen korrekt über die Datenverarbeitung aufgeklärt und entsprechende Auftragsverarbeitungsverträge abgeschlossen würden. Dazu werde das zuständige Fachamt bei künftigen Vorhaben enger mit dem Rechtsamt und dem Datenschutzbeauftragten des Bezirks zusammenarbeiten, um eine Wiederholung eines solchen Vorfalls auszuschließen. Wir haben uns daher entschlossen, es in diesem Fall bei einer Verwarnung zu belassen.

Bei Haushaltsbefragungen ist stets sorgfältig zu prüfen, ob sich aus den Einzelangaben Rückschlüsse auf die Betroffenen ziehen lassen. Soweit dies möglich ist, handelt es sich um personenbezogene Daten, sodass die datenschutzrechtlichen Verpflichtungen zu beachten sind. Alle Bezirke sollten vor entsprechenden Befragungen stets genau prüfen, ob diese eingehalten werden.

9.3 Wer kommt wann nach Hause? – Chipkarten als Schlüssel

Bewohner*innen eines Mehrparteienhauses beschwerten sich bei uns darüber, dass für den Zugang zu der Liegenschaft zunehmend digitale Schlüsselkarten eingesetzt würden und der Zugang mit physischen Schlüsseln dementsprechend eingeschränkt werde. Sie befürchteten eine Überwachung ihrer Aufenthaltszeiten und berichteten von Zugangsproblemen.

Die Bewohner*innen monierten, dass an einigen Zugängen des Hauses überhaupt keine Möglichkeit zur Verwendung physischer Schlüssel mehr gegeben sei. Neben der Unzuverlässigkeit des Systems bei Strom- oder Internetausfällen beklagten sie zudem die mangelnde Transparenz des Unternehmens hinsichtlich des Umgangs mit den durch das digitale Schließsystem erhobenen Daten.

Die betreffende Hausverwaltung war sich zunächst keines Problems bewusst. Die Schließkarten enthielten zwar RFID[201]-Transponder, die die jeweils einer Wohnung zugeordneten Codes an ein entsprechendes Lesegerät sendeten. Die Rechtevergabe werde jedoch auf nur einem PC im Büro des Unternehmens administriert, der durch ein Virenprogramm, eine Firewall und ein nur dem Geschäftsführer bekanntes Passwort geschützt sei. Man habe sich für eine solche Anlage entschieden, um nicht mit datenschutzrechtlichen Problemen konfrontiert zu werden.

Dieser Wunsch erfüllte sich indes nicht. Allein die Erhebung der Nutzungszeiten einzelner Karten oder der zugehörigen Lesegeräte an den jeweiligen Wohneinheiten stellt eine Verarbeitung personenbezogener Daten dar, unabhängig davon, ob diese im Anschluss durch das Unternehmen tatsächlich ausgelesen werden oder nicht. Durch die theoretisch mögliche Erstellung eines Anwesenheitsprofils ließen sich bspw. im Falle eines Einpersonenhaushalts erhebliche Einblicke in die Privatsphäre betroffener Personen gewinnen. Da die Datenverarbeitung zur Durchführung des Mietvertrags nicht erforderlich ist, kann ein derartiges System nur freiwillig eingesetzt werden.

Voraussetzung für die Freiwilligkeit einer Einwilligung durch betroffene Personen ist aber die Möglichkeit, sich alternativ für ein System ohne eine derartige Datenverarbeitung zu entscheiden. Wir haben das Unternehmen daher dazu angehalten, in von ihr betreuten Liegenschaften physische Schließvorrichtungen dauerhaft als Alternative anzubieten und mit Digitallösungen verbundene Datenverarbeitungen ausschließlich einwilligungsbasiert vorzunehmen.

Die Verarbeitung personenbezogener Daten im Rahmen elektronisch organisierter Zugangssysteme zu Wohngebäuden kann datenschutzrechtlich nur dann zulässig sein, wenn sie auf einer freiwilligen Einwilligung der Bewohner*innen basiert. Voraussetzung dafür ist, dass andere Zugangsoptionen bestehen, die unnötige Datenerhebungen und -verarbeitungen vermeiden.

201 RFID-Systeme bestehen aus einem Sender und einem Empfänger, die berührungslos Informationen austauschen können.

9.4 Datenschutz in der Wohnungswirtschaft – Entwicklungen und Probleme

Das Arbeitsgebiet Wohnen und Wohnungswirtschaft nimmt in der aufsichtsbehördlichen Praxis einen immer größeren Anteil ein; über 120 Verfahren wurden bis Ende November in diesem Bereich eingeleitet.

Die überwiegende Anzahl der Verfahren im Bereich Wohnen wird weiterhin durch Beschwerden von Mieter*innen über Vermietungs- oder Hausverwaltungsunternehmen bzw. Privatvermieter*innen ausgelöst. Auch Beratungen sowohl von Privatpersonen als auch von Gewerbetreibenden und Unternehmen aus der Wohnungswirtschaft haben im Berichtszeitraum zahlenmäßig zugenommen. Ein wachsender Teil von Eingaben bezieht sich auch auf eine neue Entwicklung in der Wohnstruktur Berlins: Mehr und mehr Wohnungseigentümer*innen informieren oder beschweren sich über die Datenverarbeitung im Rahmen von Wohnungseigentumsgemeinschaften (WEG).

Gerade in diesem sich neu entwickelnden Bereich der WEG scheinen viele zu unterschätzen, wie eng die vertragliche Bindung der Mitglieder einer WEG untereinander ist und welche Einblicke in die Verbrauchs- und Finanzverhältnisse der unmittelbaren Nachbarschaft innerhalb einer WEG zwangsläufig bestehen. Die gesetzlich zulässige Kontrolle der jährlichen Verbrauchsrechnungen und das Erstellen von Hausgeldübersichten sind in den allermeisten Fällen nur möglich, wenn auch die Zahlen der jeweils mit abgerechneten Wohneinheiten bekannt sind, was nicht unerhebliche und teils unerwünschte Einblicke in die Nachbarschaft ermöglicht. Dies ist aus den genannten Gründen und mit dem Wohnungseigentumsgesetz als Rechtsgrundlage allerdings datenschutzrechtlich nicht zu beanstanden. Auch die Nutzung von Online-Portalen für den Abruf der erforderlichen Unterlagen ist zulässig, solange diese entsprechend zugangsbeschränkt und abgesichert sind. Eine generelle Pflicht zur Bereitstellung von über das erforderliche Maß hinausgehenden Daten innerhalb einer WEG (bspw. die E-Mail-Adressen sämtlicher Eigentümer*innen für alle WEG-Mitglieder) ist nicht zulässig.

Die Beschwerden von Mieter*innen beziehen sich weiterhin hauptsächlich auf exzessive Datenerhebungen im Mietbewerbungsverfahren und auf nicht oder nicht

korrekt bzw. nicht vollständig bearbeitete Auskunfts- oder Löschungsersuchen. Zudem erhöhte sich das Eingabeaufkommen vor allem auch hinsichtlich der ab dem 1. Januar 2021 verpflichtend zum Einbau vorgesehenen Rauchwarnmelder, die häufig per Funk gewartet werden können. Viele Menschen fürchteten hier eine Überwachung mittels der zum Einbau vorgesehenen Geräte, zumal diese über Sensoren verfügen, die bspw. Abstände messen können, um ein Verdecken der Warnmelder erkennen und vermeiden zu können. Diese Sensoren sind jedoch nicht in der Lage, personenbezogene Daten in Form von Bewegungsprofilen oder Tonaufzeichnungen zu erheben, geschweige denn, diese über die in ihnen verbauten wenig leistungsstarken Funksender nach außen zu übertragen.

Ein Personenbezug ist jedoch in der einer bestimmten Wohneinheit zugeordneten Gerätenummer sowie den entsprechenden Wartungsprotokollen anzunehmen. Zu der unberechtigten Verarbeitung dieser Daten erreichten uns indes noch keine Beschwerden.

Unterschieden werden von diesen Fällen des Einbaus von Rauchmeldern muss der Einsatz funkbasierter Geräte zur Erfassung von Heizkosten, da dort durch die Aufzeichnung der Verbrauchsdaten immer ein Personenbezug mit der Möglichkeit der Ausforschung von Lebensverhältnissen besteht.[202]

Wir erwarten einen weiteren Anstieg der Fallzahlen im Arbeitsgebiet Wohnungswirtschaft. Nicht nur, weil das Thema Wohnen angesichts des knappen Angebots und des daraus entstehenden Machtgefälles immer wieder Raum bietet für eine exzessive Verarbeitung personenbezogener Daten. Auch der in Kraft getretene Mietendeckel und die Diskussion darüber, wie die Wohneigentumsverhältnisse in Berlin tatsächlich ausgestaltet sind oder sein sollten, wird zukünftig auch datenschutzrechtliche Aspekte berühren.

202 JB 2016, 4.4

9.5 Haben Sie sich getrennt? – Exzessive Datenerhebungen in Mietbewerbungsverfahren

Bei einer Vor-Ort-Prüfung eines Internetportals, das seinen geschäftlichen Schwerpunkt im Schalten von Anzeigen für den Verkauf oder die Vermietung von Wohnungen gesetzt hat, wurden die verschiedenen Prozesse innerhalb der Angebote des Internetportals beleuchtet.

In dem geprüften Portal gibt es verschiedene Angebote für unterschiedliche Nutzungsbedürfnisse. So können Anbieter*innen z. B. bei der Erstellung eines Vermietungsangebots verschiedene Kategorien personenbezogener Daten auswählen, die Mietinteressent*innen ausfüllen sollen. Umgekehrt können auch Wohnungssuchende ein Profil anlegen und darin verschiedenste personenbezogene Daten angeben, die dann bei Interesse an einem bestimmten Angebot übermittelt werden können. Dazu gehörten u.a. auch intimste Angaben als Begründung für den angestrebten Umzug wie z. B. die „Trennung einer Partnerschaft" oder die „Vergrößerung einer Familie", die unter verschiedenen Antwortmöglichkeiten ausgewählt werden sollen. Den Nutzer*innen wird dabei suggeriert, dass sie bei möglichst umfassenden Angaben die besten Chancen auf die Wohnung haben.

Die Betreiberin des Portals war der Ansicht, sie habe innerhalb des mit registrierten Nutzer*innen geschlossenen Nutzungsvertrags das Recht, solche Daten zur Vertragserfüllung zu erheben und zu verarbeiten. Dies ist jedoch nicht der Fall. Zweck des Vertrags ist in dem genannten Beispiel die Förderung des Abschlusses eines Mietvertrags. Für den Abschluss des Mietvertrags dürfen Vermieter*innen z. B. Angaben zur Familienplanung der Mieter*innen jedoch nicht erheben.[203] Folglich können solche Angaben auch nicht zur Durchführung eines Vertrags erforderlich sein, der das Ziel hat, Anbieter*innen und Wohnungssuchende über das Internet zusammenzuführen. Auch von einer wirksamen Einwilligung könnte hier kaum ausgegangen werden, da viele Mietinteressent*innen u.a. aufgrund der all-

203 Siehe Orientierungshilfe der DSK zur „Einholung von Selbstauskünften bei Mietinteressentinnen" vom 30. Januar 2018, S. 4; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/orientierungshilfen

gemein angespannten Situation auf dem Berliner Wohnungsmarkt von der angebotenen Leistung abhängig sind und sich zur Erhöhung ihrer Chancen auf dem Wohnungsmarkt zur Abgabe entsprechender Auskünfte genötigt sehen könnten.

Im Rahmen von Mietbewerbungsverfahren dürfen grundsätzlich nur solche personenbezogenen Daten erhoben werden, die für den Abschluss des Mietvertrags erforderlich sind. Dieser Grundsatz darf nicht dadurch umgangen werden, dass eine Online-Plattform zwischengeschaltet wird.

9.6 Mein Haus – Mein Grundbuchauszug

Aus der Praxis

In einer zivil- bzw. baurechtlichen Streitigkeit hat eine Kanzlei im Auftrag ihrer Mandantschaft die Eigentümer*innen mehrerer Grundstücke einer Reihenhaussiedlung verklagt. Der Klageschrift hat die Kanzlei ein umfangreiches Anlagenkonvolut beigefügt, darunter auch die vollständigen Grundbuchblätter bzw. Grundbuchauszüge zu allen Grundstücken der betreffenden Reihenhaussiedlung. Diese Grundbuchauszüge enthielten personenbezogene Daten zu den 23 Grundstückseigentümer*innen, darunter ihre Namen, Geburtsdaten und Anschriften, bestehende Lasten und Beschränkungen sowie Informationen zu Hypotheken, Grundschulden und Rentenschulden. Nach Zustellung der Klageschrift mit den Anlagen durch das Landgericht Berlin erlangten alle Beklagten Kenntnis von diesen Daten.

Grundbuchblätter sind grundsätzlich in die Aufschrift, das Bestandsverzeichnis und die erste bis dritte Abteilung gegliedert.[204] Als „Abteilungen" werden die verschiedenen, in sich abgeschlossenen Abschnitte eines Grundbuchblatts bezeichnet, in die bestimmte Angaben einzutragen sind.[205] In der ersten Abteilung werden die Eigentumsverhältnisse festgehalten und u.a. Name, Geburtsdatum und Anschrift der Eigentümerin bzw. des Eigentümers sowie die Grundlage für die Eintragung des Eigentums vermerkt. In der zweiten Abteilung werden Eigentumslasten und -beschränkungen (u.a. Dienstbarkeiten, Reallasten) und in der dritten

204 § 4 Grundbuchverfügung (GBV)

205 Die nähere Einrichtung und die Ausfüllung des Grundbuchblatts ergibt sich gemäß § 22 GBV aus dem in Anlage 1 GBV enthaltenen Muster.

Abteilung Grundpfandrechte, wie z. B. Hypotheken, eingetragen. Bei den in den Abteilungen enthaltenen Informationen handelt es sich um personenbezogene Daten. Die Kanzlei hat die Grundbuchblätter im Rahmen des Zivilprozesses als Beweismittel vorgelegt.

Die Datenverarbeitung durch die Kanzlei war allerdings rechtswidrig, da weder Einwilligungen der betroffenen Personen vorlagen, noch eine Rechtsgrundlage ersichtlich war. Die Datenverarbeitung kann insbesondere nicht auf Art. 6 Abs. 1 Satz 1 lit. f DS-GVO gestützt werden. Danach ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und -freiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Zwar ist in der Verarbeitung personenbezogener Daten der gegnerischen Partei zur Durchsetzung von Rechtspositionen der Mandantschaft grundsätzlich ein berechtigtes Interesse in der Berufsausübung einer Rechtsanwältin oder eines Rechtsanwalts zu sehen. Die Vorlage der vollständigen Grundbuchauszüge war jedoch im vorliegenden Fall als Beweismittel im Zivilprozess gegen die Eigentümer*innen nicht erforderlich. Eine datenverarbeitende Stelle kann sich nicht auf berechtigte Interessen berufen, wenn den Daten jegliche Aussagekraft für den konkret verfolgten Verarbeitungszweck fehlt.[206] Die Datenverarbeitung muss vielmehr zur Erreichung des Zwecks objektiv tauglich sein und eine die betroffene Person weniger belastende Alternative darf entweder nicht vorliegen oder muss für den Verantwortlichen nicht zumutbar sein.[207]

Die Kanzlei wollte mit der Vorlage der vollständigen Grundbuchauszüge beweisen, dass die betroffenen Personen die richtigen Klagegegner*innen sind. Zur Beweisführung, dass diese tatsächlich das Eigentum an den Grundstücken besitzen, wäre jedoch lediglich eine Kopie der ersten Abteilung der jeweiligen Grundbuchblätter ausreichend gewesen, da hierin die Eigentumsverhältnisse festgeschrieben sind.[208] Die Informationen der zweiten und dritten Abteilung der Grundbuchauszüge waren im Rahmen der Klagebegründung hingegen nicht erforderlich. Es wäre unproblematisch möglich gewesen, aus den vollständigen Auszügen ledig-

206 Siehe Kühling/Buchner/Buchner/Petri, DS-GVO, Art. 6, Rn. 151
207 Siehe Schulz, in Gola, DS-GVO, Art. 6, Rn. 20
208 Siehe § 9 GBV

lich die Blätter der ersten Abteilung zu kopieren und der Klageschrift beizufügen. Kennzeichnend für die drei Abteilungen der Grundbuchblätter ist gerade, dass sie in sich geschlossen sind. In der Trennung der z. B. vom zuständigen Grundbuchamt oder einer Notarin bzw. einem Notar erhaltenen Grundbuchabdrucke eine „Manipulation" zu sehen, die den Tatbestand der Urkundenfälschung i. S. v. § 267 Strafgesetzbuch (StGB) erfüllt, ist abwegig und muss als Schutzbehauptung der Kanzlei gewertet werden.

Die Kanzlei hat im Rahmen unseres gesamten Prüfverfahrens die Rechtsauffassung vertreten, dass die Einführung der vollständigen Grundbuchauszüge in das Klageverfahren rechtmäßig erfolgte. Vor diesem Hintergrund und angesichts der großen Anzahl an betroffenen Personen haben wir den Datenschutzverstoß als äußerst gravierend bewertet. Daher hat unsere Sanktionsstelle inzwischen ein Bußgeldverfahren eingeleitet.

Rechtsanwältinnen und Rechtsanwälte müssen darauf achten, dass sie im Rahmen von Prozessen nur personenbezogene Daten verarbeiten, die zur Beweisführung erforderlich sind. Eine Kanzlei kann sich nicht darauf berufen, dass die Datenverarbeitung zur Wahrung berechtigter Interessen erforderlich war, sofern den im Rahmen eines Zivilprozesses als Beweis eingeführten personenbezogenen Daten jegliche Aussagekraft für den verfolgten Verarbeitungszweck fehlt.

9.7 Schuldner gesucht

Aus der Praxis

Um den Schuldner eines Mandanten ausfindig zu machen, hatte eine Kanzlei sich mit einem Schreiben an die Bewohnerinnen und Bewohner eines Wohnhauses gewandt. Darin teilte die Kanzlei neben dem Namen der gesuchten Person mit, dass diese in dem Haus offiziell gemeldet sei, der Name sich jedoch nicht am Klingeltableau befinde. Versuche, die Person über die Hausverwaltung ausfindig zu machen, sie vor Ort persönlich anzutreffen und Post zuzustellen, seien gescheitert. Die Kanzlei bat die Nachbarinnen und Nachbarn um Mitteilung, ob der wegen offener Forderungen gesuchte Schuldner bei einer der Mietparteien wohne. In dem Schreiben wurde die Veranlassung einer Zwangsabmeldung bei

der Meldebehörde angedroht, falls keine positive Rückmeldung seitens der Mieterinnen und Mieter zur gesuchten Person eingehen sollte.

Die Offenbarung der Informationen über den Schuldner gegenüber den Hausbewohner*innen war unzulässig. Insbesondere war die Versendung des Schreibens mit den personenbezogenen Daten des gesuchten Schuldners weder zur Wahrung berechtigter Interessen der Kanzlei noch zur Wahrung berechtigter Interessen des Mandanten als Gläubiger der Forderung erforderlich.[209] Erforderlichkeit ist dann anzunehmen, wenn das durch die Datenverarbeitung verfolgte berechtigte Interesse tatsächlich erreicht werden kann und es hierfür kein anderes, gleich wirksames, aber mit Blick auf die Grundrechte und Grundfreiheiten der betroffenen Person weniger einschneidendes Mittel gibt. Dies bedeutet, dass das Vorliegen der Erforderlichkeit nur dann anzunehmen ist, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen, wirtschaftlich und organisatorisch zumutbaren Mittel erreicht werden kann, das weniger in die Rechte der oder des Betroffenen eingreift.

Für die rechtswirksame Geltendmachung der vorliegenden Forderung bzw. die Zustellung des anwaltlichen Forderungsschreibens existieren andere, gleich geeignete und weniger in die Rechte des betroffenen Schuldners eingreifende Mittel. Die Kanzlei hätte ein gerichtliches Mahnverfahren einleiten können. Gemäß § 693 Abs. 1 Zivilprozessordnung (ZPO) wird der Mahnbescheid in einem förmlichen Verfahren oder durch die Geschäftsstelle des Gerichts von Amts wegen zugestellt.[210] Die Gerichtsgeschäftsstelle kann eine*n nach § 33 Abs. 1 des Postgesetzes (PostG) beliehene*n Unternehmer*in oder Justizbedienstete*n mit der Ausführung der Zustellung beauftragen. Ist in Einzelfällen die Zustellung durch die Geschäftsstelle oder die Post nicht möglich, kann die oder der Vorsitzende des Prozessgerichts eine*n Gerichtsvollzieher*in mit der Zustellung beauftragen.[211]

Rechtsanwältinnen und Rechtsanwälte sollten bei der Verarbeitung von Daten der gegnerischen Partei genau prüfen, ob alle gesetzlich zur Verfügung stehenden Möglichkeiten ausgeschöpft worden sind, um z. B. ein Forderungsschrei-

209 Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO
210 Siehe § 168 ZPO und § 166 Abs. 2 ZPO
211 § 168 Abs. 2 ZPO

ben zuzustellen. Es ist hingegen kein zulässiges Mittel, gegenüber Nachbarinnen und Nachbarn Informationen über eine gesuchte Person zu offenbaren, um deren Aufenthaltsort ausfindig zu machen. Vielmehr müssen Kanzleien sich an die für zivile Rechtsverfahren vorgesehenen Zustellungsformen halten, auch wenn zuvor verschiedene Nachforschungsmaßnahmen (z. B. persönlich oder postalische Kontaktaufnahmeversuche) erfolglos waren.

9.8 Datenverarbeitung durch Notariate bei „Wohnungs-Paketverkäufen“

Im Rahmen von Immobilienverkäufen werden durch Notarinnen und Notare nicht nur personenbezogene Daten der Vertragsbeteiligten verarbeitet, sondern regelmäßig auch Daten von Mieter*innen der verkauften Wohnung. Hintergrund ist, dass den notariell zu beurkundenden Immobilienkaufverträgen als Anlage oftmals Unterlagen zur Mietwohnung beigefügt werden. Bei einem sog. Paketverkauf, bei dem mehrere Immobilien gleichzeitig mit einem Kaufvertrag verkauft werden, sind dementsprechend oftmals zahlreiche Mieter*innen betroffen. Im Zusammenhang mit solchen Paketverkäufen von Wohnimmobilien haben uns mehrere Beschwerden über Notare erreicht.

Die Notare hatten im Rahmen der Beurkundung und Abwicklung der Paketverkäufe von großen Wohnkomplexen Kaufvertragsunterlagen mit umfangreichen personenbezogenen Daten an alle Mieterinnen und Mieter der Wohnhäuser übersandt, um diese über das Bestehen eines Vorkaufsrechts zu informieren.[212] Die Kaufvertragsparteien hatten die Notare damit beauftragt, die vorkaufsberechtigte Mieterschaft über den Verkauf der Immobilien zu unterrichten und sie förmlich

212 Wenn für eine Wohnimmobilie ein Vorkaufsrecht besteht, ist ein*e Verkäufer*in beim Abschluss eines Kaufvertrags verpflichtet, diesen schnellstmöglich der bzw. dem Vorkaufsberechtigten vorzulegen. Wenn die zum Vorkauf begünstigte Person das Vorkaufsrecht ausüben will, darf sie den Kaufvertrag anstelle der ursprünglichen Käuferin oder des ursprünglichen Käufers übernehmen, einschließlich aller bereits vereinbarten Konditionen, und wird so zur Kaufvertragspartei der Verkäuferin oder des Verkäufers.

aufzufordern, sich zu ihrem Vorkaufsrecht zu äußern.[213] Zur Erfüllung dieses Auftrags wandten sich die Notare mit einem Schreiben an die Vorkaufsberechtigten und sandten gleichzeitig Ausfertigungen des Kaufvertrags einschließlich zahlreicher Anlagen an die Mieter*innen. Beigefügt waren z. B. Mieter-, Kautions- und Saldenlisten, die u.a. die Namen sowie Kontonummern aller Mieterinnen und Mieter eines Wohnhauses, den jeweils zu zahlenden Mietzins, die Höhe der eingezahlten Kautionen und Informationen über Mietrückstände enthielten. In den Mieter*innenlisten war zum Teil sogar vermerkt, welche Personen unter gesetzlicher Betreuung stehen, sodass Rückschlüsse auf deren Gesundheitszustand gezogen werden konnten. Da die Notare allen vorkaufsberechtigten Personen die gleichen Unterlagen zukommen ließen und sie die Daten zu den jeweils anderen Mieter*innen nicht unkenntlich machten, erlangten die Nachbar*innen zum Teil äußerst sensitive Informationen übereinander.

Die handelnden Notare waren als Verantwortliche der genannten Datenverarbeitungen anzusehen und nicht lediglich als Auftragsverarbeiter.[214] Denn bei der von Gesetzes wegen zwingenden Beauftragung eines Notars im Zusammenhang mit dem Abschluss von Immobilienverträgen handelt es sich nicht um eine weisungsgebundene Verarbeitung, sondern um die Inanspruchnahme fremder Fachleistung bei einer oder einem Verantwortlichen.[215] Notarinnen und Notare haben im Rahmen ihrer Tätigkeit grundsätzlich wesentliche eigene Entscheidungsspielräume in Bezug auf den Zweck und die Mittel der Datenverarbeitung. Auch in den von uns geprüften Fällen erschöpfte sich die Tätigkeit der Notare weder in der bloßen Beurkundungstätigkeit noch lag eine reine Vollzugstätigkeit vor. Vielmehr umfasste die Beauftragung durch die Kaufvertragsparteien darüber hinausgehende Aufgaben im Zusammenhang mit der Vertragsabwicklung.

213 § 577 Abs. 1 Satz 3 i. V. m. § 469 Abs. 1 BGB regelt die Pflicht zur Mitteilung an den Vorkaufsberechtigten über den Inhalt des geschlossenen Vertrags. Die Unterrichtungspflicht über das Vorkaufsrecht ergibt sich aus § 577 Abs. 2 BGB. Beiden Pflichten muss eigentlich die Verkäuferin oder der Verkäufer nachkommen.

214 Siehe Art. 4 Nr. 7 DS-GVO und Art. 4 Nr. 8 DS-GVO

215 Siehe auch das Kurzpapier Nr. 13 der DSK, S. 4; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/kurzpapiere

Für die Übermittlung der Daten der Mieterinnen und Mieter durch die Notare an sämtliche vorkaufsberechtigten Personen gibt es keine Rechtsgrundlage.[216] Insbesondere konnten die Notare sich bei der Datenverarbeitung nicht darauf berufen, dass diese zur Erfüllung einer eigenen rechtlichen Verpflichtung erforderlich war.[217] Des Weiteren konnte nicht davon ausgegangen werden, dass die Datenübermittlung zur Wahrung berechtigter Interessen der Verantwortlichen oder Dritter erforderlich und zugleich als schwerwiegender anzusehen gewesen wäre als die datenschutzbezogenen Interessen, Grundrechte und Grundfreiheiten der davon betroffenen Personen.[218] Die gesetzlich geregelte Pflicht, bei Eintritt des Vorkauffalls die Mieterinnen und Mieter über ihr Vorkaufsrecht zu unterrichten und ihnen den Inhalt des jeweiligen Kaufvertrags mitzuteilen, stellt keinen Grund dar, ihnen auch die sensitiven Daten der anderen Mieter*innen zu übermitteln. Erforderlich ist lediglich, dass die vorkaufsberechtigten Personen Kenntnis von den mit den Drittkäufern vereinbarten Gegenleistungen erhalten.

Daten zu anderen Personen, die für eine sachgerechte Entscheidung über die Ausübung des Vorkaufsrechts keinerlei Bedeutung haben, dürfen nicht übermittelt werden. Notarinnen und Notare müssen im Rahmen der notariellen Begleitung von immobilienrechtlichen Kaufverträgen insoweit Sorge dafür tragen, dass die personenbezogenen Daten der Mieterinnen und Mieter datenschutzkonform verarbeitet werden. Hierzu gehört auch, dass sie bei vertraglicher Übernahme der Unterrichtungs- sowie Mitteilungspflichten[219] die datenschutzgerechte Ausführung dieser Pflichten gewährleisten. Dies kann z. B. durch Übersendung individueller Vertragsausfertigungen an die jeweils vorkaufsberechtigten Mieter*innen erfolgen, bei denen die personenbezogenen Daten der anderen Mieter*innen unkenntlich gemacht werden.

Da die von uns geprüften Fälle weitreichende Bedeutung für die Tätigkeit der Notarinnen und Notare hatten, haben wir uns an die Notarkammer Berlin gewandt, um praktikable Lösungen und Handlungsempfehlungen zu erörtern. Die Kammer hat uns mitgeteilt, dass einige Gutachten des Deutschen Notarinstituts unsere

216 Siehe Art. 6 Abs. 1 Satz 1 lit. a bis f DS-GVO
217 Siehe Art. 6 Abs. 1 Satz 1 lit. c DS-GVO
218 Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO
219 Gemäß § 577 Abs. 1 Satz 3 BGB i. V. m. § 469 BGB sowie § 577 Abs. 2 BGB

Auffassung stützen. Da sie die Rechtslage jedoch für noch nicht abschließend geklärt hielt, hat sie ein eher zurückhaltendes Rundschreiben an die Berliner Notarinnen und Notare formuliert.

Notarinnen und Notare sollten bereits bei der Gestaltung von Immobilienkaufverträgen darauf achten bzw. darauf hinwirken, dass nur solche personenbezogenen Daten dem zu beurkundenden Kaufvertrag hinzugefügt werden, die für die Abwicklung des Vertrags sowie die Wahrnehmung rechtlicher Pflichten tatsächlich erforderlich sind. Sie müssen auch dafür sorgen, dass keine personenbezogenen Daten an vorkaufsberechtigte Mieterinnen und Mieter übermittelt werden, die für die Ausübung des Vorkaufsrechts nicht erforderlich sind. Dies kann bspw. durch die Schwärzung solcher Daten vor der Übersendung von Unterlagen erfolgen.

10 Wirtschaft

10.1 Identitätsmissbrauch bei Internetbestellungen

Aus der Praxis

Auch in diesem Jahr ist weiterhin festzustellen, dass Unternehmen keine ausreichenden Maßnahmen zur Identifizierung von Personen bei Bestellvorgängen ergreifen. Dabei werden nach wie vor entweder komplette Identitäten oder Kontodaten von Betroffenen für Betrugsfälle missbraucht.

Bereits im Jahr 2017 mussten wir uns aufgrund einer großen Zahl an Betrugsfällen intensiv mit dem Thema beschäftigen und hatten Änderungen im Geschäftsgebaren von Online-Händlern gefordert.[220] Nun mussten wir wieder feststellen, dass Online-Händler bei Auffälligkeiten, die auf einen möglichen Betrug hinweisen (z. B. bei einer Abweichung zwischen Rechnungs- und Lieferanschrift), nach wie vor keine ausreichenden Kontrollen ergriffen haben, um Identitätsmissbräuche zu verhindern. Eine Erstbestellung auf Rechnung mit einer von der Rechnungsadresse abweichenden Lieferadresse ist weiterhin bei vielen Unternehmen möglich, ohne dass dies zu genaueren Kontrollen oder zumindest einer risikobewussten Ausgestaltung des Mahn- und Inkassoverfahrens führen würde.

Zwar wurden immerhin in den meisten Beschwerdefällen die Mahnungen nicht ausschließlich per E-Mail versandt. Allerdings kommt es auch vor, dass falsche Rechnungsadressen angegeben werden, sodass die potenziellen Opfer dennoch erst durch das erste Schreiben des Inkassounternehmens nach dessen Adressrecherche von dem Mahnverfahren und letztlich dem Identitätsmissbrauch Kenntnis erlangen.

Von Unternehmen, die Erstbestellungen auf Rechnung mit abweichender Lieferanschrift erlauben und keine Identitätsprüfung vornehmen, wäre daher nicht nur

220 JB 2017, 1.3 und Pressemitteilung unserer Behörde vom 8. September 2017; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen/pressemitteilungen-archiv

zu verlangen, dass diese vor Abgabe an ein Inkassounternehmen zumindest einen eigenen Mahnversuch per Post unternehmen, sondern auch, dass sie Postrückläufe in solchen Fällen zum Anlass nehmen, selbstständig einen Identitätsmissbrauch zu prüfen. Dabei sind auch die langen Laufzeiten von Postrückläufen zu beachten – es darf also in solchen Fällen nicht etwa schon zwei Wochen nach der postalischen Mahnung eine Übergabe an ein Inkassounternehmen erfolgen. Ergibt die Prüfung durch das Unternehmen keinen Hinweis auf einen Identitätsmissbrauch, sollte dennoch das Unternehmen zunächst selbst die richtige Anschrift der betroffenen Person ermitteln und die postalische Mahnung nochmals an die tatsächliche Anschrift senden, um eine Aufklärung des Sachverhalts zu ermöglichen.

Jedenfalls muss ein Widerspruch der betroffenen Person im Mahnverfahren angemessen berücksichtigt werden. Denn die Übermittlung personenbezogener Daten an ein Inkassounternehmen ist zum Zwecke des Forderungseinzugs nicht erforderlich und damit nicht nach Art. 6 Abs. 1 lit. b der Datenschutz-Grundverordnung (DS-GVO) zulässig, wenn die geltend gemachte Forderung überhaupt nicht besteht. In Betracht kommt in solchen Fällen zwar eine Übermittlung an das Inkassounternehmen auf der Grundlage berechtigter Interessen nach Art. 6 Abs. 1 lit. f DS-GVO.[221] Ist aber für das Unternehmen ein Identitätsmissbrauch offensichtlich, fehlt es an einem berechtigten Interesse an der Weitergabe der personenbezogenen Daten bei Einschaltung eines Inkassobüros. Wendet die betroffene Person einen Identitätsmissbrauch ein, darf eine Datenübermittlung an das Inkassounternehmen erst dann erfolgen, wenn die Forderung nach dieser Einwendung genau überprüft wurde. In einem uns vorliegenden Beschwerdefall ist die Überprüfung trotz mehrfachen Widerspruchs unterblieben, sodass wir dieses Verfahren unserer Sanktionsstelle zur Prüfung der Einleitung eines Bußgeldverfahrens vorgelegt haben.

In Fällen von Identitätsmissbrauch stellt sich oftmals auch die Frage, ob die Betroffenen einen Auskunftsanspruch über ihre rechtswidrig verwendeten Bestelldaten haben.

221 Siehe 10.7

Personenbezogene Daten sind nach der gesetzlichen Definition alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen und dieser somit zugeordnet werden können.[222] Die durch einen Dritten erzeugten Daten werden durch das jeweilige Unternehmen der vom Identitätsdiebstahl betroffenen Person zugeordnet und damit verarbeitet. Nach der Auslegung des Begriffs des Personenbezugs in der Rechtsprechung des Europäischen Gerichtshofs (EuGH) ist der Personenbezug eines Datums auch dann gegeben, wenn „die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist".[223] Dies ist bei einem Identitätsmissbrauch ersichtlich der Fall. Es handelt sich somit um personenbezogene Daten der jeweiligen natürlichen Person.

Die Betroffenen müssen bei einem (auch vermuteten) Identitätsdiebstahl über alle zu ihnen gespeicherten Daten ausnahmslos Auskunft erhalten. Davon umfasst sind alle Daten, die das Kundenkonto, Kontenbewegungen und die Bestellhistorie betreffen, da diese Daten der Identität der Betroffenen zugeordnet sind oder zu diesen in Bezug stehen. Daher stellen sie personenbezogene Daten der Betroffenen dar, auch wenn sie von Dritten unter Vorspiegelung der falschen Identität verursacht worden sind.

Dem Auskunftsanspruch der betroffenen Person können auch nicht die Rechte Dritter entgegenhalten werden. Ein Schutzbedürfnis der personenbezogenen Daten Dritter besteht nicht, da diese bewusst die personenbezogenen Daten der betroffenen Person verwendet haben, um ihr Handeln dieser zuzuordnen. Insbesondere haben sie die Situation, dass ihre und die Daten der betroffenen Personen zusammenfallen, selbst herbeigeführt.

Wir sind zur Vermeidung von Identitätsmissbrauch weiterhin im Austausch mit den Unternehmen, um auf eine risikobewusste Ausgestaltung des Bestell- und Mahnverfahrens hinzuwirken. Die Rechtmäßigkeit der Verarbeitung ihrer Daten können betroffene Personen bei einem (vermuteten) Identitätsdiebstahl nur überprüfen, wenn sie über alle Daten Auskunft erhalten, die ihr Kunden-

222 Art. 4 Nr. 1 DS-GVO

223 EuGH, Urteil vom 20. Dezember 2017 – C-434/16, Rn. 34, 35 (Nowak-Fall)

konto bzw. ihre Kundennummer betreffen. Da es sich dabei nach dem Gesetz um personenbezogene Daten des Opfers eines Identitätsmissbrauchs handelt, sind Unternehmen zu einer umfassenden Auskunft verpflichtet.

10.2 Und täglich grüßt der Adresshandel

Über viele Monate hinweg haben uns zahlreiche Schreiben von Bürger*innen erreicht, die sich darüber beschwert haben, dass sie wiederholt Werbung per E-Mail von einem Unternehmen erhielten, ohne hierfür eine entsprechende Werbeeinwilligung oder sonstige Zustimmung gegeben zu haben. Vielen der Betroffenen war der Anbieter der E-Mail-Werbung auch nicht bekannt. Auf Auskunftsersuchen seitens der betroffenen Personen wurde oftmals gar nicht oder erst mit großer Verzögerung reagiert. Ebenso verhielt es sich, wenn die Betroffenen mit Aufforderungen zur Sperrung oder Löschung der eigenen Daten an den Anbieter herangetreten sind. Wir haben den Sachverhalt eingehend untersucht und den Anbieter um Stellungnahme gebeten.

Auf unser Anschreiben teilte uns der Anbieter mit, dass er die E-Mail-Adressen der betroffenen Personen häufig durch deren Teilnahme an Gewinnspielen oder mittels Adressmiete erlangt habe. Nach seinen Angaben geschah dies entweder dadurch, dass er als Co-Sponsor der Gewinnspiele den Teilnahmebedingungen entsprechend auch Zugriff auf die Namen und E-Mail-Adressen der Teilnehmer*innen erhielt oder dies durch die Anmietung großer Datenmengen über sog. Listeneigner*innen erfolgte, insbesondere aus Großbritannien.

Oftmals lagen keine wirksamen Einwilligungen seitens der Betroffenen zum Erhalt werblicher Kommunikation vor. Auffällig war überdies, dass der Anbieter die Erlangung der Daten häufig erst auf beharrlichen Druck durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit hinreichend offenlegte und viele der Gewinnspiele bereits vor mehreren Jahren beendet worden waren, die verantwortliche Stelle die Kund*innen jedoch erst in den letzten zwölf Monaten zu Werbezwecken angeschrieben hatte.

Eine Einwilligung unterliegt zwar grundsätzlich keinem Verfallsdatum. Vor dem Hintergrund des Grundsatzes der transparenten Datenverarbeitung gemäß Art. 5

Abs. 1 lit. a DS-GVO empfiehlt der Europäische Datenschutzausschuss (EDSA) jedoch, die Einwilligung in angemessenen Zeitabständen erneuern zu lassen.[224] Wenn alle mit der Datenverarbeitung verbundenen Hinweise dann erneut erteilt werden, hilft das sicherzustellen, dass die betroffene Person darüber informiert bleibt, wie ihre Daten verwendet werden und wie sie ihre Rechte ausüben kann. Wenn, wie hier, über einen längeren Zeitraum keine Kontaktaufnahme mehr erfolgt ist, kann von einem Weiterbestehen der Einwilligung nicht mehr ohne Weiteres ausgegangen werden. Ein Zeitraum von zehn Jahren oder mehr ohne Kontaktaufnahme kann insoweit nicht mehr als angemessen betrachtet werden.

Hinzu kam im vorliegenden Fall, dass die verantwortliche Stelle oftmals erst nach mehreren Monaten auf Anfragen reagierte. Nach Art. 12 Abs. 3 Satz 1 DS-GVO haben Verantwortliche der betroffenen Person beantragte Informationen unverzüglich zur Verfügung zu stellen, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags. Innerhalb dieser Frist muss die Auskunft erteilt oder es muss zumindest mitgeteilt werden, warum dies innerhalb der Frist nicht möglich ist.

Wir haben den Anbieter darauf hingewiesen, dass sein Verhalten datenschutzrechtlich fragwürdig ist und das Verfahren zu ändern sei. Zu beachten sei dabei insbesondere auch, dass die Rechte der Betroffenen auf Auskunft, Löschung und Sperrung ihrer Daten stets zu wahren und zügig zu realisieren sind. Auch hinsichtlich der Transparenz des Umgangs mit den Daten der Kund*innen haben wir deutliche Verbesserungen angemahnt.

Wenngleich unsere Prüfung noch nicht abgeschlossen ist, haben wir den Anbieter bereits deutlich darauf hingewiesen, dass wir ein derartiges Fehlverhalten nicht dulden und dies unverzüglich abzustellen ist. Der Verantwortliche hat zugesagt, unsere Hinweise zu beachten und umzusetzen.

Wir werden den Anbieter auch in Zukunft weiterhin aufmerksam beobachten. Unbeschadet der bisher bereits erfolgten Maßnahmen behalten wir uns auch die Verhängung entsprechender Bußgelder gegen die verantwortliche Stelle vor.

224 Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 vom 4. Mai 2020, Ziff. 111; siehe https://edpb.europa.eu/our-work-tools/our-documents/nasoki/guidelines-052020-consent-under-regulation-2016679_de

10.3 Automatisierter Abruf aus einem Vermittlerregister

Der Deutsche Industrie- und Handelskammertag e. V. (DIHK) führt für die Industrie- und Handelskammern ein Vermittlerregister, in dem u.a. die Daten von ca. 400.000 Versicherungsvermittler*innen eingetragen sind. Versicherungen erhalten Auskünfte aus dem Register im Wege eines automatisierten Abrufs über das Internet.[225] Sie benötigen diese Informationen, da sie nur mit Versicherungsvermittler*innen zusammenarbeiten dürfen, die eine entsprechende Erlaubnis besitzen.[226] In das Register eingetragen sind u.a. jeweils Name und Vorname der Vermittler*innen, die Registernummer, die Adresse, aber auch der Umfang der Tätigkeit.[227] Der DIHK war besorgt darüber, dass einige Versicherungen mehr als Tausend Abfragen pro Tag durchführten. Zur Sicherung des Datenschutzes der Betroffenen und zur Abwehr von Computerangriffen wurde daher die Zahl der möglichen Abfragen reduziert. Teilweise wurde den Versicherungen nur noch die Möglichkeit gegeben, in einem „Ampelverfahren" zu erkennen, ob ein*e Versicherungsvermittler*in in der Liste aufgeführt ist oder nicht. Die Beschränkungen führten zu einem Streit zwischen der Versicherungswirtschaft und dem DIHK. Da sich der DIHK bei seinen Beschränkungen auf Datenschutzvorgaben berief, wurde unsere Behörde gebeten, den Streit zu schlichten.

Grundsätzlich bestehen beim Abruf der öffentlichen Registerdaten keine rechtlichen Bedenken, wenn er zweckgebunden erfolgt. Hiervon kann man beim Abruf von Versicherungen ausgehen, da diese ein Interesse und sogar eine rechtliche Pflicht haben, die Zulassung sowie den Umfang der zugelassenen Tätigkeit der Eintragungspflichtigen zu überprüfen. Bei großen Versicherungsgesellschaften ist es auch nicht verwunderlich, dass teilweise mehr als Tausend Abfragen pro Tag erfolgen, da Versicherungen bei ihren Vertragsbeziehungen immer den aktuellen Stand, also auch eine etwa gerade erst vorgenommene Gewerbeuntersagung, berücksichtigen müssen.[228] Für eine Reduzierung der abrufbaren Informationen z. B. durch eine Ampelangabe gibt es keine datenschutzrechtliche Notwendig-

225 Siehe § 11a Abs. 1 und 2 Gewerbeordnung (GewO)

226 Siehe § 48 Abs. 1 Gesetz über die Beaufsichtigung von Versicherungsunternehmen (VAG)

227 § 8 Versicherungsvermittlerverordnung (VersVermV)

228 Siehe § 11a Abs. 3 Satz 1 GewO

keit. Es bestehen keine Bedenken dagegen, dass die Versicherungen den vollen Datensatz erhalten, aus dem sich der Umfang der zugelassenen Tätigkeit ergibt und nicht nur ein Ja oder Nein. Der Gesetzgeber hat sich zum Schutz von Versicherungsnehmer*innen dafür entschieden, die Vermittlerregisterdaten öffentlich zugänglich zu machen. Die Überprüfung eines berechtigten Interesses ist nicht erforderlich, es sollte nur sichergestellt werden, dass keine Computerangriffe oder missbräuchliche Abrufe erfolgen. Wir haben empfohlen, dass die großen abfragenden Versicherungen Ansprechpartner*innen zur Verfügung stellen, falls bei der DIHK aufgrund der großen Zahl der Abfragen ein Erklärungsbedarf besteht.

Anders als häufig behauptet, verhindern die Datenschutzaufsichtsbehörden nicht nur, sondern ermöglichen vieles: Durch unsere Vermittlung funktioniert inzwischen die Datenabfrage der Versicherungen beim Vermittlerregister wieder.

10.4 Unwillkommene „Willkommens-E-Mail“

Immer wieder erreichen uns Anfragen von Personen, die per Brief oder E-Mail Werbung von Unternehmen erhalten, mit denen sie schon längere Zeit nicht mehr in einer geschäftlichen Beziehung gestanden haben. Im Rahmen der Anhörung verweisen verantwortliche Stellen dann oft auf ein bestehendes Kundenkonto und vertreten die Auffassung, eine Zusendung von Werbung sei in solchen Fallkonstellationen zeitlich unbeschränkt zulässig. Viele Beschwerden erreichten uns insoweit im Zusammenhang mit der Übernahme eines Online-Modehändlers durch ein Berliner Unternehmen. Dabei wurden in zahlreichen Fällen Daten von ehemaligen Kund*innen des Online-Modehändlers aus inaktiven Kund*innenkonten verarbeitet, um diese mit einer sog. Willkommens-E-Mail auf die Angebote des neuen Unternehmens aufmerksam zu machen. Gleichzeitig wurde für sie ein neues Kund*innenkonto angelegt.

Art. 17 Abs. 1 lit. a 2. Alt. DS-GVO verpflichtet jede für die Verarbeitung personenbezogener Daten verantwortliche Stelle, die Daten unverzüglich zu löschen, sofern diese für die Zwecke, für die sie verarbeitet worden sind, nicht mehr notwendig sind. Ein Antrag oder eine Aufforderung der betroffenen Person ist hierfür nicht erforderlich.

Diese antragsunabhängige Verpflichtung zur Löschung bedingt, dass die verantwortliche Stelle ihre Löschungsverpflichtungen selbstständig und fortlaufend zu überprüfen hat. Dabei enthält die DS-GVO jedoch keine konkreten Festlegungen in zeitlicher Hinsicht. Es obliegt damit dem jeweiligen Unternehmen, je nach Art und Umfang der vorgenommenen Datenverarbeitung ein spezifisches Löschkonzept sowie funktionierende Löschroutinen zu entwickeln und durch geeignete technisch-organisatorische Maßnahmen auch umzusetzen (und die betroffenen Personen im Rahmen der Datenschutzerklärung nach Art. 13 bzw.14 DS-GVO über die konkreten Löschfristen zu informieren). Bei einem Kund*innenkonto ist zur Bestimmung des Zeitraums, nach dem die Löschung erfolgen muss, die regelmäßige Nutzung durch die betroffene Person entscheidend.

Die Verarbeitung von personenbezogenen Daten muss dem Zweck angemessen und zu seiner Erreichung erheblich[229] sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Grundsatz der Datenminimierung).[230] Personenbezogene Daten dürfen nicht länger gespeichert werden, als dies für die Zwecke ihrer Verarbeitung notwendig ist (Grundsatz der Speicherbegrenzung).[231] Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sind verantwortliche Stellen verpflichtet, eigenständig Fristen für die Löschung und die regelmäßige Überprüfung der Daten vorzusehen.[232] Wird also der Zweck durch den Prozess der Datenverarbeitung erreicht oder fällt dieser auf andere Weise fort, so sind die Daten grundsätzlich vollständig zu löschen. Wenn nur ein Teil der Daten für den benannten Zweck nicht mehr erforderlich ist, kann auch eine teilweise Löschung geboten sein.

Entscheidend ist, ob aufgrund der Art der Geschäftsbeziehung von der verantwortlichen Stelle nachvollziehbar dargelegt werden kann, dass die weitere Nut-

229 Dies bedeutet, dass von der verantwortlichen Stelle grundsätzlich nur solche personenbezogenen Daten erhoben und verarbeitet werden dürfen, die für den angegebenen Zweck geeignet sind; siehe BeckOK Datenschutzrecht, Schantz, DS-GVO, Art. 5, Rn. 24.

230 Art. 5 Abs. 1 lit. c DS-GVO

231 Art. 5 Abs. 1 lit. e 1. Hs DS-GVO

232 EG 39 Satz 9 DS-GVO

zung der Daten erforderlich ist. Eine konkrete zeitliche Befristung hat der Gesetzgeber dafür nicht vorgesehen.

Eine Orientierung für Speicher- und Löschfristen enthält die von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) am 7./8. November 2018 beschlossene „Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)".[233] Dabei sind je nach Art und Branche der verantwortlichen Stellen zeitliche Begrenzungen von sechs Monaten bis zu zwei Jahren vertretbar. Innerhalb des durch die verantwortliche Stelle jeweils festgelegten Zeitraums nach dem letzten aktiven Geschäftskontakt zu einer betroffenen Person können deren Daten im Grundsatz für die Kund*innen-Rückgewinnung genutzt werden. Nach Ablauf dieser Frist ist regelmäßig von einer fehlenden Erforderlichkeit der Datenspeicherung auszugehen.

Wenn also eine verantwortliche Stelle Daten verarbeitet, diese jedoch für den ursprünglichen Zweck nicht mehr erforderlich sind und auch keine gesetzlichen oder vertraglichen Aufbewahrungsfristen[234] bestehen, dürfen diese nicht mehr verwendet und müssen gelöscht werden. Nicht genutzte Kund*innenkonten und die darin gespeicherten personenbezogenen Daten müssen daher spätestens nach zwei Jahren Inaktivität gelöscht werden.

Im Falle des Online-Modehändlers hätten die inaktiven Kund*innenkonten längst gelöscht sein müssen. Die Datenübernahme durch das neue Unternehmen und das Anlegen neuer Kund*innenkonten mithilfe dieser alten Daten war daher unzulässig.

Verantwortliche Stellen sind verpflichtet, personenbezogene Daten regelmäßig und ohne gesonderte Aufforderung zu löschen, sobald diese für die Zwecke, für die sie erhoben bzw. verarbeitet worden sind, nicht mehr notwendig sind. Bei nicht genutzten Kund*innenkonten ist dies spätestens nach zwei Jahren der Fall.

233 Siehe https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk, insbesondere Kapitel 4.8

234 Siehe Art. 17 Abs. 3 lit b DS-GVO sowie § 35 Abs. 3 2. Alt. BDSG

10.5 Datenspeicherung nach dem Ende eines Vertragsverhältnisses

Auch nach Vertragsende bzw. nach Beendigung eines Kund*innenverhältnisses sind Verantwortliche gesetzlich verpflichtet, bestimmte Unterlagen weiter aufzubewahren. Bei der Bearbeitung entsprechender Beschwerden hat sich in mehreren Fällen herausgestellt, dass die Ausgestaltung der Aufbewahrung dieser Unterlagen durch Verantwortliche nicht mit den Bestimmungen der DS-GVO vereinbar war.

Grundsätzlich sind personenbezogene Daten zu löschen, wenn sie für die Zwecke, für die sie verarbeitet werden, nicht mehr erforderlich sind.[235] Eine Löschung kann demzufolge u.a. unterbleiben, wenn die weitere Verarbeitung der Daten zur Erfüllung einer rechtlichen Verpflichtung der Verantwortlichen noch erforderlich ist.[236] Dadurch legitimiert sind jedoch nur Datenverarbeitungen, die für die Erfüllung der jeweiligen rechtlichen Verpflichtung auch tatsächlich benötigt werden.

Nach dem Grundsatz der Datenminimierung[237] müssen die personenbezogenen Daten dabei dem Zweck angemessen und zu seiner Erreichung erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Verantwortliche müssen die erforderlichen technischen und organisatorischen Maßnahmen treffen, um die Einhaltung der Anforderungen der DS-GVO zu gewährleisten.[238]

Zu den rechtlichen Verpflichtungen, die eine weitere Speicherung personenbezogener Daten erlauben können, zählen insbesondere die Verpflichtungen zur Aufbewahrung von Unterlagen nach dem Handels- und Steuerrecht. Die dortigen Regelungen zur Aufbewahrung von Unterlagen wie Handelsbriefen und Bu-

235 In der Regel erlischt mit dem Ende des Vertragsverhältnisses die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten; siehe Art. 6 Abs. 1 Satz 1 lit. b DS-GVO.

236 Art. 6 Abs. 1 Satz 1 lit. c DS-GVO

237 Art. 5 Abs. 1 lit. c DS-GVO

238 Art. 24, 25, 32 DS-GVO

chungsbelegen berechtigen bzw. verpflichten Verantwortliche im Einzelnen zur Aufbewahrung folgender Unterlagen über das Vertragsende hinaus:

- die empfangenen Handels- und Geschäftsbriefe für die Dauer von sechs Jahren,[239]
- Wiedergaben der abgesandten Handels- und Geschäftsbriefe für die Dauer von sechs Jahren,[240]
- Buchungsbelege für die Dauer von zehn Jahren[241] sowie
- sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind, für die Dauer von sechs Jahren.[242]

Diese Vorschriften sehen jedoch nur die Aufbewahrung bestimmter Dokumente vor, die dann ggf. personenbezogene Daten von Kund*innen enthalten. Nicht aufzubewahren sind hingegen solche Unterlagen, aus denen diese Dokumente erst erstellt wurden, sowie sonstige Kommunikation, die nicht als Handels- oder Geschäftsbrief gilt, etwa weil sie sich nicht auf die Vorbereitung, Durchführung oder Rückgängigmachung eines Handelsgeschäfts bezieht, oder weil es sich um betriebsinterne Kommunikation oder um Telefonvermerke handelt. Die über das Vertragsende hinausgehende Führung einer Datenbank, in der personenbezogene Daten ehemaliger Kund*innen wie etwa Stamm- oder Kommunikationsdaten gespeichert sind, sehen diese Vorschriften nicht vor. Aus solchen Datenbanken sind die personenbezogenen Daten der Kund*innen daher bei Fehlen einer anderen Rechtsgrundlage nach Vertragsende zu löschen.

Die gesetzlichen Verpflichtungen zur Aufbewahrung bestimmter Dokumente mit personenbezogenen Daten nach Beendigung eines Vertragsverhältnisses berechtigen bzw. verpflichten Verantwortliche nicht, Stamm- oder Kommunikationsdaten ehemaliger Kund*innen auch nach Vertragsende weiterhin in ihren Datenbanken zu speichern. Verantwortliche müssen ihre Datenhaltung entsprechend anpassen.

239 § 257 Abs. 1 Nr. 2, Abs. 4 Handelsgesetzbuch (HGB); § 147 Abs. 1 Nr. 2, Abs. 3 Abgabenordnung (AO)

240 § 257 Abs. 1 Nr. 3, Abs. 4 HGB; § 147 Abs. 1 Nr. 3, Abs. 3 AO

241 § 257 Abs. 1 Nr. 4, Abs. 4 HGB; § 147 Abs. 1 Nr. 4, Abs. 3 AO

242 § 147 Abs. 1 Nr. 5, Abs. 3 AO

10.6 Beauftragung von Inkassounternehmen – Warum erhalte ich von denen Post?!

Viele Bürger*innen, die Mahnschreiben von Inkassounternehmen erhalten haben, wenden sich an uns und erkundigen sich nach der Rechtmäßigkeit der Weitergabe ihrer Daten durch Gläubiger*innen an das Inkassounternehmen.

Soweit mit der betroffenen Person ein Vertrag besteht, können Gläubiger*innen die Forderung entweder selbst eintreiben oder ein Inkassounternehmen damit beauftragen. Im letzteren Fall ist es erforderlich, dass das Inkassounternehmen auch die Informationen erhält, die die Forderung begründen und die einen Einzug durch das Inkassounternehmen ermöglichen.

Wird ein Inkassounternehmen beauftragt, ist die Übermittlung der zur Einziehung der Forderung erforderlichen personenbezogenen Daten auf der Basis von Art. 6 Abs. 1 Satz 1 lit. b DS-GVO zulässig. Denkbar ist auch eine Einwilligung der betroffenen Person,[243] wobei diese Rechtsgrundlage in der Praxis weniger Bedeutung hat, da eine Einwilligung jederzeit widerrufen werden kann. Außerdem kommt als Rechtsgrundlage für die Übermittlung personenbezogener Daten an ein Inkassounternehmen Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in Betracht. Danach ist das Übermitteln personenbezogener Daten rechtmäßig, wenn „die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person … überwiegen". Das berechtigte Interesse des übermittelnden Unternehmens besteht darin, dass die offene Forderung durch die Schuldner*innen beglichen wird.

Sofern eine betroffene Person mit einem Unternehmen die Erbringung einer bestimmten Leistung gegen Bezahlung vereinbart und die daraus resultierende Forderung nicht bzw. nicht vollständig beglichen hat, ist das Unternehmen nach sorgfältiger Prüfung folglich grundsätzlich berechtigt, die Vertragsdaten der betroffenen Person zur Forderungseinziehung an ein Inkassounternehmen weiterzugeben.

243 Siehe Art. 6 Abs. 1 Satz 1 lit. a DS-GVO

Da die Datenübermittlung der Forderungseinziehung dienen soll, ist i. d. R. auch nicht davon auszugehen, dass Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Dies gilt grundsätzlich auch in den Fällen, in denen das Bestehen bzw. die Höhe der geltend gemachten Forderung durch die betroffene Person bestritten wird. Bestand aber von vornherein keine Forderung, etwa weil eine Forderung aus einer sog. Abo-Falle geltend gemacht wird oder ein Identitätsdiebstahl vorliegt, kann eine Datenübermittlung zum Forderungseinzug nicht begründbar sein, da es ja gerade an einer Forderung fehlt. In diesem Fall könnte – neben der typischerweise nicht vorliegenden Einwilligung – nur Art. 6 Abs. 1 Satz 1 lit. f DS-GVO als Rechtsgrundlage in Betracht kommen. Hierzu ist allerdings ein berechtigtes Interesse der oder des Verantwortlichen oder einer dritten Person erforderlich. Ein solches berechtigtes Interesse kann zwar auch darin liegen, die Berechtigung der vermeintlichen Forderung festzustellen. Ist aber für eine*n vermeintliche*n Gläubiger*in erkennbar, dass die Forderung nicht besteht, kann ein berechtigtes Interesse an der Weitergabe der personenbezogenen Daten aufgrund der Einschaltung eines Inkassobüros nicht bejaht werden. Bringt die betroffene Person derartige Einwendungen vor, muss die vermeintliche Gläubigerin oder der vermeintliche Gläubiger daher die Berechtigung der Forderung vor der Einschaltung eines Inkassobüros ganz besonders genau prüfen.[244]

Sofern die Voraussetzungen des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO vorliegen, können die Inkassounternehmen also die für die Erfüllung ihres Auftrags erforderlichen Daten verarbeiten und dürfen darüber hinaus erforderliche weitere Daten erheben.

Gläubiger*innen können Inkassounternehmen auch ohne die Einwilligung der betroffenen Personen mit der Geltendmachung ihrer Forderungen beauftragen und die dazu erforderlichen personenbezogenen Daten übermitteln.

244 Siehe 10.1

10.7 Was dürfen Inkassounternehmen den Auskunfteien mitteilen?

Gegenstand zahlreicher bei uns eingehender Anfragen und Beschwerden ist auch die Rechtmäßigkeit der Einmeldung von Forderungen bei Wirtschaftsauskunfteien durch Inkassounternehmen.

Die Befugnis von Inkassounternehmen, Daten von Schuldner*innen an Wirtschaftsauskunfteien, wie bspw. die SCHUFA Holding AG oder die CRIF Bürgel GmbH, zu übermitteln, richtet sich nach Art. 6 Abs. 1 Satz 1 lit. f sowie Art. 6 Abs. 4 DS-GVO. Ein Einverständnis der betroffenen Personen ist hierfür nicht erforderlich.

Eine Übermittlung personenbezogener Daten an eine andere Stelle bzw. zu einem anderen Zweck ist möglich, soweit diese für die Wahrnehmung eines berechtigten Interesses der übermittelnden Stelle, der Empfängerin bzw. des Empfängers der Daten oder von Dritten erforderlich ist. Die schutzwürdigen Interessen der betroffenen Person dürfen dabei diesem berechtigten Interesse gegenüber nicht überwiegen. Darüber hinaus muss der neue Verarbeitungszweck mit dem ursprünglichen Zweck in einem Zusammenhang stehen.[245]

Von einem berechtigten Interesse an der Datenübermittlung an eine Auskunftei kann bei Inkassounternehmen ausgegangen werden, wenn ein Anlass besteht, Dritte über die negativen Zahlungserfahrungen mit einer betroffenen Person zu informieren, um diese Dritten vor Zahlungsstörungen zu bewahren. Dabei muss der Anlass auf gesicherten Tatsachen beruhen. Rein subjektive Einschätzungen genügen also nicht.

Die DSK hat sich bereits 2018 auf die nachfolgend aufgeführten fünf alternativen Fallgruppen verständigt, die im Rahmen der Interessenabwägung nach Art. 6

245 Art. 6 Abs. 4 lit. a DS-GVO, EG 50 Satz 6 DS-GVO

Abs. 1 Satz 1 lit. f i. V. m. Art. 6 Abs. 4 DS-GVO eine Indizwirkung für die Zulässigkeit einer Einmeldung bei einer Auskunftei entfalten können:[246]

„1. Die Forderung ist durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden oder es liegt ein Schuldtitel nach § 794 der Zivilprozessordnung vor.
2. Die Forderung ist nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden.
3. Der Betroffene hat die Forderung ausdrücklich anerkannt.
4. Der Betroffene ist nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden, die erste Mahnung liegt mindestens vier Wochen zurück, der Betroffene ist zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden und der Betroffene hat die Forderung nicht bestritten.
5. Das der Forderung zugrunde liegende Vertragsverhältnis kann aufgrund von Zahlungsrückständen fristlos gekündigt werden und der Betroffene ist zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden."

Die betroffene Person muss vorab durch das Inkassounternehmen über die Möglichkeit der Einmeldung bei einer Wirtschaftsauskunftei unterrichtet werden, da diese nur erfolgen darf, soweit die betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass eine Verarbeitung für diesen Zweck möglicherweise erfolgen wird.[247]

Zu beachten ist auch, dass es für das Vorliegen von negativen Zahlungserfahrungen keine beitragsmäßige Bagatellgrenze gibt. Es können also auch Kleinstbeträge eingemeldet werden, sofern die vorgenannten Übermittlungsvoraussetzungen erfüllt sind.

246 Beschluss der DSK vom 23. März 2018: „Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei unter Geltung der DS-GVO"; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

247 Siehe EG 47 Satz 3 DS-GVO

Für die inhaltliche Richtigkeit der Einmeldungen und für das Vorliegen der Übermittlungsvoraussetzungen ist das Inkassounternehmen als übermittelnde Stelle verantwortlich.

Soweit die Datenübermittlung unzulässig war oder sich nachträglich als unzulässig erweist, haben betroffene Personen bspw. Ansprüche auf Berichtigung, Löschung und Schadensersatz. Das Inkassounternehmen ist in solchen Fällen außerdem verpflichtet, die Auskunfteien, denen die Daten übermittelt wurden, zu benachrichtigen, um eine Korrektur bzw. Löschung der bei den Auskunfteien gespeicherten Daten herbeizuführen.[248]

Inkassounternehmen dürfen Daten von Schuldner*innen (nur dann) an Wirtschaftsauskunfteien übermitteln, wenn bestimmte Voraussetzungen erfüllt sind. Das Einverständnis der betroffenen Personen ist hierfür grundsätzlich nicht erforderlich. Allerdings sind die betroffenen Personen vorab über die Möglichkeit der Einmeldung bei einer Wirtschaftsauskunftei zu informieren.

10.8 Datenschutzbeauftragte gehören nicht zum Kund*innenservice

In einigen Unternehmen werden Anfragen an die in der Datenschutzerklärung angegebene Datenschutzbeauftragte bzw. den angegebenen Datenschutzbeauftragten nicht direkt oder nicht nur an diese benannte Person weitergeleitet, sondern an andere Stellen, insbesondere an den Kund*innenservice.

Die bzw. der Datenschutzbeauftragte ist bei der Erfüllung ihrer oder seiner Aufgaben zur Wahrung von Geheimhaltung und Vertraulichkeit verpflichtet.[249] Diese Verschwiegenheitspflicht besteht auch gegenüber der sie bzw. ihn benennenden Stelle. Es ist daher nicht zulässig, dass Anfragen, die in dem Vertrauen auf Verschwiegenheit an eine*n Datenschutzbeauftragte*n gesandt werden, an andere Stellen des Unternehmens weitergeleitet werden.

248 Siehe Art. 19 Satz 1 DS-GVO
249 Art. 38 Abs. 5 DS-GVO

Ein Verstoß gegen die gesetzlichen Vertraulichkeitspflichten stellt es daher bspw. dar, wenn die an eine*n Datenschutzbeauftragte*n gerichteten E-Mails an einen Verteiler weitergeleitet werden, dem neben der oder dem Datenschutzbeauftragten auch die IT-Leitung und der Kund*innenservice angehören. Für den Kontakt zu der oder dem Datenschutzbeauftragten darf auch nicht dasselbe Kontaktformular verwendet werden wie für den Kontakt zum Unternehmen. Eingehende Post oder E-Mails an die oder den Datenschutzbeauftragte*n dürfen vom Unternehmen – etwa in der Poststelle oder durch die Administrator*innen – nicht geöffnet oder gelesen werden.

Es ist allerdings möglich und vorgesehen, dass die oder der Datenschutzbeauftragte von Mitarbeiter*innen bei der Aufgabenerfüllung unterstützt wird. Diese dürfen daher nach den Vorgaben der oder des Datenschutzbeauftragten und unter Beachtung der Vertraulichkeitspflichten in deren oder dessen Arbeit einbezogen werden.

Die betroffenen Unternehmen haben wir aufgrund der Nichtwahrung der Vertraulichkeit verwarnt bzw. einen Fall zur weiteren Verfolgung an die Sanktionsstelle abgegeben.

Die Kenntnisnahme von Post und E-Mails an die oder den Datenschutzbeauftragte*n muss in der ausschließlichen Entscheidungshoheit der oder des jeweiligen Datenschutzbeauftragten bleiben. Alles andere widerspricht dem Grundsatz der Vertraulichkeit und Verschwiegenheit von Datenschutzbeauftragten. Daher sind auch getrennte E-Mail-Adressen und Kontaktformulare für Unternehmen und Datenschutzbeauftragte erforderlich.

10.9 Unternehmen: Posteingang kontrollieren und Betroffenenrechte sicherstellen!

Wer von einem Unternehmen keine Werbung oder Auskunft mehr erhalten möchte oder die Löschung eines Kund*innenkontos wünscht, antwortet dafür oft einfach auf eine E-Mail des betreffenden Unternehmens. Doch werden solche Kontaktaufnahmen häufig mit dem Hinweis verweigert, dass es sich um eine

„Keine-Antwort-Adresse" handele oder das Postfach nicht gesichtet werde. Betroffene werden oft auf einen bestimmten Kommunikationskanal verwiesen. Es ist auch allgemein festzustellen, dass die Nachrichteneingänge – insbesondere per E-Mail – bei vielen Unternehmen unzureichend kontrolliert werden.

Verantwortliche haben durch technisch-organisatorische Maßnahmen sicherzustellen, dass alle Datenschutzanfragen, die eingehen, an die zuständige Fachabteilung weitergeleitet und dort bearbeitet werden.[250] Dies schließt ein, dass auch E-Mails, die nicht über die von den Verantwortlichen hierfür vorgesehenen Kanäle eintreffen, zur weiteren Bearbeitung an die richtigen Ansprechpersonen geleitet werden. Es kann den Betroffenen nicht abverlangt werden, zunächst die Datenschutzerklärung zu suchen, um die von den Verantwortlichen für Datenschutzanfragen vorgesehene Kontaktadresse herauszufinden. Betroffene Personen gehen meistens davon aus, dass alle Anliegen, die ihr Kund*innenkonto betreffen, auch über die E-Mail-Adresse zu regeln sind, mit der das Unternehmen mit ihnen in der Vergangenheit in Kontakt getreten ist. Entsprechend lässt es die DS-GVO auch nicht zu, Betroffene auf bestimmte Kommunikationswege zu verweisen.

Im Gegenteil verpflichtet Art. 12 Abs. 2 Satz 1 DS-GVO Verantwortliche sogar, betroffenen Personen die Geltendmachung ihrer Rechte zu erleichtern. Sog. No-Reply-E-Mail-Adressen, bei denen Antworten an die Absender-Adresse nicht gelesen werden, sind somit jedenfalls dann ein datenschutzrechtliches Problem, wenn in ihnen nicht zumindest eine Adresse angegeben wird, an die Kund*innen sich wenden können und bei der eingehende datenschutzrechtliche Anfragen bearbeitet werden. Im Ergebnis müssen Verantwortliche alle Anträge auf Geltendmachung von Betroffenenrechten bearbeiten, egal auf welchem Weg sie eingehen.

Auch E-Mails, die als vermeintlicher Spam zwar vom Mail-Server angenommen, aber in einen Spam-Ordner verschoben und nicht gelesen wurden, sind als zugegangen zu werten.[251] Gleiches gilt für E-Mails an weiterhin technisch aktive, aber nicht (mehr) aktiv genutzte Postfächer. Dort eingegangene E-Mails, durch die Betroffenenrechte geltend gemacht werden, müssen ebenso fristgerecht bearbeitet

250 Art. 24 DS-GVO
251 Siehe JB 2019, 9.7

werden. Auch Spam-Ordner und alle technisch aktiven E-Mail-Adressen müssen daher überwacht werden.

Bei der Nutzung von Ticket- oder sog. Customer-Relationship-Management-(CRM-)Systemen[252] ist darauf zu achten, dass Anfragen nicht etwa automatisch gelöscht werden, wenn sie nicht einem bestehenden Kund*innenkontakt zugeordnet werden können. Ein weiteres Problem kann entstehen, wenn etwa im Verlauf einer E-Mail-Kommunikation mit dem Kund*innenservice ab einem bestimmten Zeitpunkt auch das Datenschutzteam in Kopie genommen wird, das CRM-System aber auf solche Konstellationen nicht eingestellt ist. In einem derartigen Fall wurde eine solche E-Mail nur ins CRM-System eingespielt, aber nicht dem Datenschutzteam zugestellt. Der Kund*innenservice hielt sich für die Beantwortung der datenschutzrechtlichen Anfrage nicht für verantwortlich, leitete die Anfrage aber auch nicht an die zuständige Stelle weiter, da ihm die fehlende Einstellung des CRM-Systems nicht bekannt war.

Bei der Beantwortung von Betroffenenanfragen müssen Verantwortliche schließlich auch sicherstellen, dass die Betroffenen tatsächlich von der Antwort Kenntnis nehmen können. So dürfen Verantwortliche etwa nicht ohne Weiteres davon ausgehen, dass die frühere E-Mail-Adresse noch aktiv und im Besitz der betroffenen Person ist, wenn diese sich z. B. postalisch an das Unternehmen wendet.

Unternehmen müssen sicherstellen, dass alle eingehenden datenschutzrechtlichen Anfragen die zuständige Stelle erreichen und von dieser beantwortet werden.

252 Als CRM-System bezeichnet man eine Software zur Verwaltung der Kundenbeziehungen.

10.10 Identifizierung bei der Geltendmachung von Betroffenenrechten

Obwohl die DS-GVO eine Identitätsprüfung nur bei begründeten Zweifeln an der Identität vorsieht, liegt uns eine Vielzahl von Beschwerden vor, weil Verantwortliche für die Geltendmachung von Betroffenenrechten (insbesondere Löschersuchen) weitere Angaben, Nachweise und Handlungen verlangt haben.

Wir mussten feststellen, dass einige Unternehmen zur Löschung von Kund*innenkonten von den Betroffenen weitere Informationen (wie z. B. Kund*innennummer, Rechnungsadresse, Lieferadresse, [alte] Bestellnummer, [alte] Rechnungsnummer sowie das Geburtsdatum) verlangt haben, obwohl das Anliegen mit derselben E-Mail-Adresse gestellt wurde, die bei dem jeweiligen Unternehmen registriert war. Selbst nach Bereitstellung dieser Informationen musste das Löschersuchen zudem teilweise nochmals bestätigt werden. Manche Unternehmen verlangten für die Löschung von Kundenkonten sogar Personalausweiskopien, obwohl beim Anlegen des Kontos selbst keinerlei Überprüfung der Daten erfolgt war und im Falle kostenloser Konten sogar nur Name und E-Mail-Adresse erhoben wurden.[253] Besonders bizarr war die Forderung eines Unternehmens nach Übersendung einer beglaubigten Fotokopie des Personalausweises zum Nachweis der Identität – als Scan per E-Mail.

Verantwortliche können bei begründeten Zweifeln an der Identität zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.[254] Dabei haben Verantwortliche jedoch das Prinzip der Datenminimierung zu beachten.[255]

Die nur abstrakte Gefahr der Fälschung von Absenderadressen[256] darf nicht dazu führen, dass Anfragen zunächst pauschal für einen weiteren Datenabgleich bzw. eine Bestätigung zurückgewiesen und damit verzögert bearbeitet werden. In den

253 Zur Einholung von Personalausweiskopien siehe bereits JB 2018, 9.2
254 Art. 12 Abs. 6 DS-GVO
255 Siehe Art. 5 Abs. 1 Satz 1 lit. c DS-GVO
256 Sog. „Mail-Spoofing"

uns vorliegenden Fällen gab es keine Anhaltspunkte dafür, dass die jeweiligen E-Mail-Adressen missbräuchlich von Dritten genutzt worden sein könnten. Teilweise waren die E-Mails sogar durch den zuständigen Absende-E-Mail-Server mit einer gültigen elektronischen (DKIM-)Signatur[257] versehen worden, sodass nachgewiesen war, dass die E-Mail tatsächlich aus dem angegebenen Postfach stammte. Teilweise gab es eine „Hin-und-Her-Kommunikation" mit der betroffenen Person, sodass hierdurch der Zugriff auf das E-Mail-Postfach ebenfalls nachgewiesen war. Und manches Mal wurden selbst dann und trotz erforderlichen Logins zusätzliche Nachweise angefordert, wenn die Anfrage unter Nutzung des Kontaktformulars aus dem jeweiligen Kund*innenkonto erfolgte.

In der DS-GVO ist insbesondere die Verpflichtung für Verantwortliche niedergelegt, der betroffenen Person die Ausübung ihrer Betroffenenrechte zu erleichtern.[258] Demzufolge dürfen keine inhaltlichen oder formalen Hürden bei der Geltendmachung von Betroffenenrechten errichtet werden. Durch einen standardmäßigen Datenabgleich bei der Geltendmachung von Betroffenenrechten auch ohne begründete Zweifel an der Identität der Antragstellenden wird die Ausübung der Betroffenenrechte erschwert. Dies ist auch dann der Fall, wenn eine zusätzliche Bestätigung des Anliegens verlangt wird. Dies gilt besonders, wenn eine Auskunft an die im Datensatz gespeicherte Anschrift der anfragenden Person zu senden ist.

Solange keine gegenteiligen Hinweise vorliegen oder ein besonderes Risiko besteht – etwa bei besonders vertraulichen Daten oder gefährdeten Personen –, ist grundsätzlich davon auszugehen, dass eine angeforderte Selbstauskunft an die im Datensatz gespeicherte Anschrift gesendet werden kann, ohne dass ein zusätzlicher Nachweis der Identität erforderlich ist. Bestehen ohnehin Kund*innenkonten, sind diese regelmäßig erste Wahl, um Betroffene zu identifizieren. Neue Online-Dienste ermöglichen die Identifizierung aus der Ferne nicht nur durch die

257 DKIM steht für Domain Keys Identified Mail. Dabei handelt es sich um eine Methode der E-Mail-Authentifizierung. DKIM fügt E-Mails eine digitale Signatur hinzu, die der Absender-Domain zugeordnet ist und bei allen ausgehenden E-Mails genutzt wird. Dies ist eine Technik, die Fälschungen des E-Mail-Absenders oder des Inhalts von E-Mails erkennbar macht. Ver- oder gefälschte E-Mails können so automatisch abgewiesen oder gesondert behandelt werden, unverfälschte E-Mails akzeptiert und als echt behandelt werden.

258 Art. 12 Abs. 2 Satz 1 DS-GVO, sog. Erleichterungsgebot

eID-Funktion des Personalausweises, sondern bspw. auch über das Online-Banking.

Da Unternehmen in etlichen Fällen systematisch und grundlos die Ausübung der Betroffenenrechte erschwert haben, insbesondere indem sie unrechtmäßig weitere Nachweise zur Identität der betroffenen Personen angefordert haben, haben wir diese Fälle zur weiteren Prüfung an unsere Sanktionsstelle abgegeben.

Das Anfordern weiterer identifizierender Angaben, Nachweise und Bestätigungen ohne begründete Zweifel an der Identität stellt für die Betroffenen eine zusätzliche Hürde dar und kann sie davon abhalten, ihre Betroffenenrechte geltend zu machen. Die Geltendmachung von Betroffenenrechten sollte aber möglichst einfach sein. Das Anfordern von weiteren Informationen muss daher Fällen begründeter Zweifel an der Identität betroffener Personen vorbehalten bleiben.

10.11 Der ewige Kampf um Auskunft – Hier: Bonitätsdaten

Bei der Prüfung eines Falls stellte sich heraus, dass das verantwortliche Unternehmen regelmäßig bei Vertragsschluss bei einer Auskunftei Bonitätsauskünfte über die jeweilige Kundin oder den jeweiligen Kunden einholt. Die Bonitätsdaten werden danach für die Vertragslaufzeit gespeichert. Diese Praxis ist im konkreten Fall auch zulässig und in der Datenschutzerklärung entsprechend dargestellt. Allerdings hat das Unternehmen die Betroffenen auf deren Anfrage nicht über die von der Auskunftei erhaltenen Informationen unterrichtet. Konkret handelte es sich in den meisten Fällen um den von der Auskunftei errechneten Score-Wert, die Rating-Stufe,[259] ggf. Voradressen und den jeweiligen Geburtsort der

259 Wirtschaftsauskunfteien sammeln Informationen über Menschen, insbesondere über deren wirtschaftliche Situation und deren Zahlungsverhalten. Daraus errechnen sie einen nummerischen Wert, der die Zahlungsfähigkeit (Bonität) der betreffenden Person abbilden soll, den sog. Score-Wert. Abhängig von diesem Score-Wert wird den betroffenen Personen dann eine Wahrscheinlichkeit zugeordnet, mit der sie offene Forderungen begleichen, die sog. Rating-Stufe. Diese Informationen können Unternehmen abrufen, bevor sie Verträge abschließen, bei denen sie sich auf eine spätere Leistung der Vertragspartner*innen verlassen müssen.

Betroffenen. Auf unsere Nachfrage begründete das Unternehmen diese Praxis mit den Allgemeinen Geschäftsbedingungen der Auskunftei. Danach sei das Unternehmen nicht befugt, die erhaltenen Daten an Dritte weiterzugeben.

Die Verweigerung der Auskunft über die von der Auskunftei mitgeteilten Daten ist rechtswidrig.

Betroffene, in diesem Fall Kund*innen, haben das Recht auf Auskunft über alle personenbezogenen Daten, die ein Unternehmen über sie verarbeitet.[260] Dies umfasst grundsätzlich alle gespeicherten Informationen, egal woher die oder der Verantwortliche diese Informationen hat.

Jede Person soll so die Möglichkeit haben, zu überprüfen, ob die über sie gespeicherten Informationen richtig sind und rechtmäßig verarbeitet werden. Dies ist gerade bei Informationen über die Bonität besonders wichtig. Denn es handelt sich dabei häufig um Daten, die die Betroffenen nicht selbst den Verantwortlichen zur Verfügung gestellt haben, sondern die diese aus externen Quellen (z. B. von Auskunfteien) erhalten haben. Aufgrund dieser Informationen entscheiden Unternehmen, ob und zu welchen Bedingungen sie einen Vertrag mit einer Kundin oder einem Kunden abschließen. Wenn diese Informationen nicht (mehr) zutreffend sind oder in rechtswidriger Weise verarbeitet werden, kann dies zu einer nicht gerechtfertigten Ablehnung von Vertragsabschlüssen oder zu schlechteren Konditionen bei Verträgen führen. Dies kann weitreichende Folgen für die Betroffenen haben.

Das Recht auf vollständige Auskunft ist in der DS-GVO deshalb zwingend vorgeschrieben. Jede Einschränkung dieses Rechts muss in der DS-GVO selbst oder ausnahmsweise in anderen Rechtsvorschriften der Europäischen Union oder der Mitgliedsstaaten, denen die oder der Verantwortliche unterliegt, begründet sein.[261] Private Verträge, die dieses Recht einschränken, stellen einen Verstoß gegen die DS-GVO dar. Im deutschen Zivilrecht sind zudem Vereinbarungen, die die

260 Art. 15 Abs. 1 DS-GVO
261 Art. 23 DS-GVO

Rechte von nicht beteiligten Personen beschränken[262], grundsätzlich unzulässig und damit unwirksam.

Die Allgemeinen Geschäftsbedingungen der Auskunftei konnten das Unternehmen im vorliegenden Fall daher nicht von der Pflicht zur vollständigen Auskunft entbinden.

Auf unsere Ansprache hat das Unternehmen Informationen, die es von Auskunfteien erhalten hat, nunmehr standardmäßig in seine Auskunftserteilung aufgenommen.

Unternehmen sind grundsätzlich verpflichtet, auf Anfrage alle Informationen offenzulegen, die sie zu der betreffenden Person speichern. Dies umfasst auch Informationen, die sie von einer Auskunftei erhalten haben. Eine Einschränkung dieses Rechts durch einen Vertrag mit der Auskunftei ist unzulässig.

262 Sog. Verträge zulasten Dritter

11 Finanzen

11.1 Nicht protokollierte Zugriffe auf Bankkonten

Aus der Praxis

Wir erhielten die Beschwerde eines Bankkunden, der den begründeten Verdacht hatte, dass eine Mitarbeiterin der Bank unbefugt Zugriff auf Inhalte seines Bankkontos genommen hatte. Die Reaktion der Bank auf die Bitte des Kunden um Nachforschung blieb sehr vage und unbestimmt.

Ähnlich erging es uns mit unseren Bitten um Stellungnahmen. In mehreren Schreiben hat das Kreditinstitut es vermieden, unsere konkreten Fragen zu beantworten. Statt einer klaren Aussage, ob und ggf. wer auf die Kontobewegungen des Kunden im fraglichen Zeitraum zugegriffen hatte, wurde allgemein von dem hohen Sicherheitsbewusstsein der Bank und umfangreichen Maßnahmen zur IT-Sicherheit gesprochen. Erst allmählich wurden die Aussagen ein wenig konkreter. So verstieg sich das Kreditinstitut schließlich zu der Aussage, dass im fraglichen Zeitraum keine Zugriffe, abgesehen von „technischen" Zugriffen, auf das betreffende Konto festgestellt werden konnten. Was mit technischen Zugriffen gemeint sei, haben wir natürlich hinterfragt. Es handele sich um die notwendigen algorithmischen Zugriffe, um bspw. Transaktionen auszulösen, teilte man uns mit. Im letzten Antwortschreiben musste das Unternehmen dann zugeben, dass Zugriffe von Mitarbeitenden auf Konto- und Transaktionsdaten überhaupt nicht protokolliert werden.

An diesem Punkt haben wir eine Prüfung des Unternehmens durchgeführt. Bei dieser stellte sich Folgendes heraus: Ein erheblicher Anteil der Mitarbeitenden in höheren Positionen, aber auch der im Kund*innen-Service Beschäftigten, hatten Zugriff auf die Kontostammdaten und die Transaktionsdaten der jeweiligen Konten. Dies ist grundsätzlich nicht unzulässig, wenn die betreffenden Mitarbeitenden die Zugriffsrechte benötigen, um ihre tägliche Arbeit zu erledigen. Im Service ist dies verständlich, wenn Kund*innen bspw. Fragen zu bestimmten Buchungen haben.

Die Daten, auf die zugegriffen werden kann, sind durchaus sensitiv. Anhand der Kontobewegungen kann mittlerweile – insbesondere aufgrund des immer umfangreicheren Einsatzes bargeldloser Zahlungsmittel – ein erheblicher Teil der privaten Lebensführung nachvollzogen werden. Auch nach Art. 9 Datenschutz-Grundverordnung (DS-GVO) besonders zu schützende Daten, wie z. B. Parteimitgliedschaften oder Gewerkschaftszugehörigkeit, wären so leicht ermittelbar.

Um missbräuchliche Datenzugriffe zu vermeiden, ist eine Reihe von Maßnahmen zu ergreifen. Dazu gehört selbstverständlich, dass die Anzahl der Zugriffsberechtigten auf ein Minimum zu reduzieren ist und die betreffenden Mitarbeitenden auf Wahrung des Datengeheimnisses zu verpflichten sind. Diese Verpflichtung hatte das Unternehmen allerdings seinen Mitarbeitenden schon vor unserer Prüfung auferlegt. Neben weiteren denkbaren technischen Maßnahmen zur Zugriffsbeschränkung sind zudem eine Protokollierung derartiger Zugriffe und eine regelmäßige, zumindest stichprobenartige Überprüfung der aufgezeichneten Protokolldaten in einem festgelegten, datenschutzkonformen Verfahren zwingend erforderlich.

Diese Einsicht setzte sich auch während der Prüfung bei den Unternehmensvertreter*innen nur langsam durch. Mittlerweile hat das Kreditinstitut die notwendige Protokollierung von Zugriffen auf Konto- und Transaktionsdaten durch Mitarbeitende umgesetzt. Derzeit prüft unsere Sanktionsstelle, ob und, wenn ja, welche Sanktionen für die jahrelange Missachtung datenschutzrechtlicher Grundprinzipien zu verhängen sind.

Verantwortliche haben die Zugänglichkeit von personenbezogenen Daten auf das für den Regelfall notwendige Mindestmaß zu beschränken. Wer einer großen Zahl von Beschäftigten den Zugriff auf personenbezogene Daten eröffnet, muss die Feststellung unbefugter Zugriffe über eine Zugriffsprotokollierung ermöglichen. Dem Beschwerdeführer konnten wir zwar leider nicht mit einem Nachweis seines Verdachts weiterhelfen, und auch die etwaige missbräuchliche Nutzung von Zugriffsrechten konnte mangels Beweisen nicht verfolgt werden. Aber wir konnten dafür sorgen, dass das Datenschutzbewusstsein gestie-

gen und die technischen und organisatorischen Prozesse des Kreditinstituts nun zumindest in diesem Punkt datenschutzkonform umgestaltet wurden, um derartige Fälle künftig so weit wie möglich zu verhindern.

11.2 Streit um Umfang der Auskunftspflicht

Ein Kunde machte gegenüber seiner Bank von seinem Recht auf Auskunft Gebrauch.[263] Insbesondere wollte er feststellen, ob die Bank seine personenbezogenen Daten rechtswidrig übermittelt hat. Die Bank erteilte zwar eine Auskunft, nannte aber nur die Kategorien von Empfänger*innen (z. B. Dienstleister, Kreditdienstleistungsinstitute, Behörden), nicht jedoch die konkreten Empfänger*innen. Sie begründete dies damit, dass bei einem Auskunftsbegehren der Verantwortliche ein Wahlrecht habe, ob er den Betroffenen die konkreten Empfänger*innen oder nur Empfänger*innenkategorien mitteile. Außerdem betrachtete die Bank die Datenempfänger*innen als Geschäftsgeheimnis; dieses müsse beim Auskunftsanspruch nicht preisgegeben werden. Der Bankkunde war mit dieser Auskunft unzufrieden und beschwerte sich bei uns.

Betroffene Personen haben gegenüber den Verantwortlichen einen Anspruch auf Auskunft über „die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden".[264] Zwar scheint der Wortlaut dieser Vorschrift nahezulegen, dass es sich bei „Empfänger oder Kategorien von Empfängern" um gleichwertige Alternativen handelt und insofern ein Wahlrecht der oder des Verantwortlichen bestehen könnte. Eine Beschränkung der Auskunft auf Kategorien von Empfänger*innen ohne Offenlegung von deren Identität würde jedoch dem Zweck der DS-GVO zuwiderlaufen, betroffene Personen in die Lage zu versetzen, die Rechtmäßigkeit der Verarbeitung ihrer personenbezogenen Daten überprüfen zu können[265] und den Verantwortlichen gegenüber ihre Rechte insbesondere auf Berichtigung, Löschung, Widerspruch und Einschränkung der Bearbeitung der Daten geltend zu machen. Diese Rechte können die betroffenen Personen gegenüber Empfän-

263 Siehe Art. 15 DS-GVO
264 Art. 15 Abs. 1 lit. c DS-GVO
265 Siehe EG 63 Satz 1 DS-GVO

ger*innen ihrer übermittelten personenbezogenen Daten aber nur dann geltend machen, wenn ihnen die Identität der Adressaten bekannt ist. Eine Beschränkung des Auskunftsrechts nur auf Kategorien von Empfänger*innen reicht damit zur Wahrung der Rechte der betroffenen Personen nicht aus. Dies würde sogar einen Verstoß gegen europäisches Primärrecht darstellen.[266] Unsere Auslegung entspricht auch dem gesetzgeberischen Willen, denn danach haben betroffene Personen ein Anrecht darauf zu wissen und zu erfahren, wer die Empfänger*innen der personenbezogenen Daten sind.[267] Demnach ist eine Angabe von Kategorien von Empfänger*innen nur dann ausreichend, wenn Übermittlungen zwar grundsätzlich vorgesehen, aber noch nicht erfolgt sind.

Die Bank kann sich auch nicht erfolgreich darauf berufen, die Empfänger*innen der Daten nicht identifizieren zu müssen, da sie ein Geschäftsgeheimnis darstellten. Geschäftsgeheimnisse des Verantwortlichen können zwar den Auskunftsanspruch der betroffenen Person verringern, das Gesetz hat dies allerdings nur für den Kopieranspruch geregelt.[268] Teilweise wird zwar die Auffassung vertreten, der Gesetzgeber habe das Auskunftsrecht beim Vorliegen von Rechten Dritter nicht nur beim Kopieranspruch beschränken wollen, es liege also eine planwidrige Lücke vor.[269] Dieser Auffassung ist aber nicht zu folgen. Während bei dem Recht auf Kopie die Beeinträchtigung von Rechten und Freiheiten anderer Personen besonders nahe liegt, ist kaum anzunehmen, dass eine Beeinträchtigung Dritter durch die Identifizierung der Datenempfänger*innen zu befürchten ist.[270]

Da die Bank sich auch uns gegenüber weigerte, dem Beschwerdeführer die konkreten Empfänger*innen zu benennen, wurde der Vorgang an unsere Sanktionsstelle zur Prüfung der Einleitung eines Ordnungswidrigkeitenverfahrens weitergeleitet.

266 Siehe Art. 8 Abs. 2 Satz 2 Charta der Grundrechte der Europäischen Union: „Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken."

267 EG 63 Satz 3 DS-GVO

268 Siehe Art. 15 Abs. 3, 4 DS-GVO, EG 63 Satz 5 DS-GVO

269 Siehe Stollhoff in Auernhammer, DS-GVO/BDSG, Art. 15, Rn. 33; Härting, Datenschutz-Grundverordnung, Rn. 684

270 Siehe auch Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 15, Rn. 2

Verantwortliche müssen Betroffenen grundsätzlich sowohl die Kategorien von Empfänger*innen als auch die konkreten Empfänger*innen mitteilen.

11.3 Sperrung der Kreditkarte durch Familienangehörigen

Aus der Praxis

Ein Kreditkarteninhaber wollte seinen Hotelaufenthalt mit seiner Kreditkarte bezahlen, dies war aber nicht möglich, da seine Kreditkarte als gestohlen gemeldet war. Er beantragte und erhielt von seiner Bank eine neue Kreditkarte. Obwohl er der Bank mitteilte, dass er seine Kreditkarte nicht als gestohlen gemeldet hatte, untersuchte die Bank den Vorgang nicht. Drei Wochen später musste der Betroffene bei einem Restaurantbesuch feststellen, dass seine Kreditkarte wieder als gestohlen gemeldet war. Er vermutete, dass ein Dritter sich als Inhaber seiner Kreditkarte ausgegeben (Identitätsdiebstahl) und so die Kartensperrung bewirkt habe.

Der Verdacht des Betroffenen bestätigte sich nicht. Nach unserem Auskunftsersuchen ermittelte die Bank, dass in beiden Fällen die Kreditkarte nicht als gestohlen gemeldet worden war. Die Kartensperrung war ohne eine entsprechende Diebstahlsanzeige von einem Mitarbeiter eines technischen Dienstleisters der Bank veranlasst worden. Dieser konnte ermittelt werden. Es handelte sich um einen Angehörigen des Betroffenen, der auf diese Weise einen Familienstreit austragen wollte. Die Bank hat den Mitarbeiter inzwischen entlassen. Da sich die Bank das Verhalten des Mitarbeiters ihres Auftragsverarbeiters zurechnen lassen muss, haben wir die Bank verwarnt. Banken sollten im Übrigen schon bei einer ersten unberechtigten Kreditkartensperrung den Sachverhalt ermitteln.

Rechtswidrige Eingriffe in Banksysteme drohen nicht nur durch Angriffe von außen, sondern auch von innen.

12 Verkehr, Tourismus und Auskunfteien

12.1 „Ihren Jobcenter-Bescheid bitte“

Bürgerinnen und Bürgern mit geringem oder keinem Einkommen ermöglicht der Berlinpass einen vergünstigten Zugang zu Bildung, Sport, Kultur und dem Öffentlichen Personennahverkehr (ÖPNV) der Stadt. Aufgrund der Corona-Pandemie werden diese Pässe derzeit nicht ausgestellt. Uns erreichten in den vergangenen Monaten Beschwerden von anspruchsberechtigten Bürgerinnen und Bürgern, die mitteilten, im Rahmen von Kontrollen im öffentlichen Personennahverkehr aufgefordert worden zu sein, einen gültigen Leistungsbescheid im Original vorzuzeigen.

Abgelaufene Berlinpässe wurden sowohl von der S-Bahn als auch von der BVG aus Kulanz bis zum 31. Dezember 2020 anerkannt. Jedoch wurden anspruchsberechtigte Personen, die bislang keinen Berlinpass erhalten haben, aufgefordert, ihren Leistungsbescheid im Original mit sich zu führen und ihre Bedarfsgemeinschaftsnummer, das Aktenzeichen oder die Wohngeldnummer auf einem erworbenen Berlin-Ticket „S“ einzutragen.[271] Die Leistungsbescheide im Original dienten als Nachweis der Berechtigung zur Fahrt mit dem Berlin-Ticket „S“. Sie enthalten eine Vielzahl personenbezogener Daten wie Name, Adresse, Geburtsdatum, Familienstand und sensitive Daten wie den zugrunde liegenden Berechtigungsgrund, also bspw. Arbeitslosigkeit, Asylbewerberstatus oder Status als Opfer des SED-Unrechts.

Gegen die Pflicht zum Vorzeigen der Leistungsbescheide im Original bestehen erhebliche Bedenken, weil dies aufgrund der Vielzahl der dabei offengelegten personenbezogenen Daten gegen den Grundsatz der Datenminimierung verstößt.[272] Nach diesem Grundsatz muss die Verarbeitung personenbezogener Daten dem

271 Siehe https://www.berlin.de/sen/soziales/soziale-sicherung/berlinpass/

272 Siehe Art. 5 Abs. 1 lit. c DS-GVO

Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Im vorliegenden Fall geht der Umfang der durch den Leistungsbescheid offenzulegenden Daten über das Maß hinaus, welches für den konkreten Fall, nämlich den Nachweis der Berechtigung, erforderlich ist. Der Zweck, den Nachweis der Berechtigung zur Nutzung eines Berlin-Tickets „S" zu erbringen, kann mit einer deutlich geringeren Menge an Daten erreicht werden. Alternativen mit geringerer Eingriffstiefe wären bspw. das Ausstellen einer entsprechenden Bescheinigung durch die leistungsgewährenden Stellen, die ausschließlich die erforderlichen Daten enthält.

Wir haben die Beschwerden zum Anlass genommen, an die verantwortlichen Stellen heranzutreten, um datenschutzfreundlichere Alternativen zu erörtern. Der Prozess dauert derzeit noch an. Die zuständige Senatsverwaltung und die leistungsgewährenden Stellen sollten ein Verfahren anbieten, welches der Datensparsamkeit Rechnung trägt und trotzdem Kontrollierenden die Möglichkeit gibt, die Leistungsberechtigung zu überprüfen.

12.2 Fahren ohne Fahrschein – Datenweitergabe an Inkassounternehmen

Aus der Praxis

Bei Fahrten im öffentlichen Personennahverkehr ohne gültigen Fahrschein fällt regelmäßig ein erhöhtes Beförderungsentgelt an. Ein Bürger beschwerte sich in diesem Zusammenhang bei uns darüber, dass seine personenbezogenen Daten nach einer Fahrscheinkontrolle an ein Inkassounternehmen weitergegeben wurden und darüber hinaus für die Dauer eines Jahres bei dem Verkehrsunternehmen gespeichert werden.

Der Beschwerdeführer wurde im Rahmen einer Fahrscheinkontrolle in der S-Bahn mit einem Fahrschein, aber ohne dazugehörige Kund*innenkarte angetroffen. Das Fehlen einer Kund*innenkarte zu dem entsprechenden Fahrausweis gilt nach den Beförderungsbedingungen der S-Bahn Berlin GmbH als ungültiger Fahrausweis.[273] Die personenbezogenen Daten des Beschwerdeführers wurden

273 § 8 der Beförderungsbedingungen der S-Bahn GmbH

erfasst und zur Geltendmachung des erhöhten Beförderungsentgelts an ein Inkassounternehmen weitergegeben. Dieses machte das erhöhte Beförderungsentgelt dann gegenüber dem Beschwerdeführer geltend.

Das Fahren ohne vollständig mitgeführten Fahrschein in den Zügen der S-Bahn Berlin GmbH berechtigt Kontrolleur*innen, personenbezogene Daten der betroffenen Personen aufzunehmen. Die Verarbeitung der Daten erfolgt zur Erfüllung des jeweiligen Vertrags,[274] der nach den Beförderungsbedingungen der S-Bahn Berlin GmbH durch die Nutzung des Fahrangebots stillschweigend auch zwischen der S-Bahn Berlin GmbH und Personen ohne gültigen Fahrschein abgeschlossen wird.[275] Auch die Weitergabe der zur Abwicklung des erhöhten Beförderungsentgelts erforderlichen Daten an ein Inkassounternehmen ist zur Wahrung der berechtigten Interessen des Verkehrsunternehmens zulässig.

Die Datenschutz-Grundverordnung (DS-GVO) erlaubt die Verarbeitung von Daten u.a. dann, wenn dies „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen".[276] Auf dieser Grundlage müssen die berechtigten Interessen der oder des Verantwortlichen und die Interessen der jeweils betroffenen Person gegeneinander abgewogen werden. Die S-Bahn Berlin GmbH ist nicht verpflichtet, eine fällige Forderung selbst geltend zu machen, sondern kann damit ein Inkassounternehmen beauftragen. Überwiegende Interessen der betroffenen Person sind insoweit nicht ersichtlich. Dementsprechend dürfen die zum Zwecke der Geltendmachung der fälligen Forderung erforderlichen Daten an das Inkassounternehmen übermittelt werden. Denn ohne die entsprechenden personenbezogenen Daten ließe sich die übertragene Forderung nicht eintreiben.

Eine Speicherung der Daten für die Dauer eines Jahres bei der S-Bahn Berlin GmbH ist ebenso zulässig.[277] Das Verkehrsunternehmen hat ein berechtigtes Interesse, innerhalb eines begrenzten Zeitraums zu überprüfen, ob einzelne Perso-

274 Siehe Art. 6 Abs. 1 Satz 1 lit. b DS-GVO
275 Sog. faktischer Vertrag
276 Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO
277 Siehe Art. 6 Abs. 1 lit. f DS-GVO

nen häufiger ohne gültigen Fahrschein angetroffen werden, um ggf. einen Strafantrag wegen sog. Beförderungserschleichung[278] zu stellen.

Personenbezogene Daten, die der Geltendmachung eines erhöhten Beförderungsentgelts dienen, dürfen an ein Inkassounternehmen übermittelt werden. Das Verkehrsunternehmen, welches ein erhöhtes Beförderungsentgelt erhebt, darf die entsprechenden Daten zudem für einen begrenzten Zeitraum speichern.

12.3 „eTickets“ beim Verkehrsverbund Berlin-Brandenburg – Der Datenschutz kommt nicht in Bewegung

Bereits seit einigen Jahren treibt der Verkehrsverbund Berlin-Brandenburg (VBB) die Umstellung von Papierfahrscheinen auf elektronische Tickets voran. Viele Arten von Fahrscheinen werden schon auf der elektronischen „VBB-fahrCard“ bereitgestellt. Von Beginn an begleiten wir das Projekt durch unsere Aufsichtstätigkeit. Auch in diesem Jahr mussten wir Defizite feststellen.

Bereits seit einigen Jahren betreibt der VBB ein technisches System für seine Mitgliedsunternehmen (u.a. Berliner Verkehrsbetriebe – BVG, S-Bahn Berlin GmbH und Verkehrsbetrieb Potsdam GmbH), um im Raum Berlin–Brandenburg den Umstieg der Verkehrsunternehmen von Papierfahrscheinen und papiergebundenen Abonnementbescheinigungen auf elektronische Tickets zu ermöglichen. Dies umfasst u.a. die VBB-Umweltkarte, die „10-Uhr-Karte“ im Abonnement, das VBB-Abonnement für Auszubildende sowie das VBB-Abonnement 65 plus, die schrittweise auf die „VBB-fahrCard“ (Fahrberechtigung in Form einer Chipkarte) umgestellt worden sind.

Der VBB stützt sich bei dem Betrieb des Systems für das elektronische Fahrgeldmanagement (EFM) auf die Vorarbeiten und Dienstleistungen der VDV eTicket

278 Siehe § 265a Strafgesetzbuch (StGB)

Service GmbH & Co. KG aus Köln.[279] Dieses Tochterunternehmen des Verbands Deutscher Verkehrsunternehmen (VDV) hat mit dem sog. VDV-Kernapplikations-Standard die Grundlage für das elektronische Ticketing in Deutschland entwickelt, pflegt das Gesamtsystem und betreibt seine zentralen Komponenten.

Leider mussten wir bei mehrfachen Nachfragen feststellen, dass trotz der langen Vorgeschichte die datenschutzrechtliche Verantwortung für den Betrieb des EFM-Gesamtsystems und damit auch die Rechtsgrundlage für alle damit verbundenen Datenverarbeitungen nach wie vor nicht geklärt ist.

Ebenso unvollständig sind die Informationen darüber, welche Prozessbeteiligten auf welche Nutzungsdaten Zugriff haben. Dies betrifft insbesondere die Zugriffsmöglichkeiten von Drittanbietern, mit denen der VBB kooperiert. So kann die VBB-fahrCard für das Laden von Elektrofahrzeugen an der Berliner Ladesäuleninfrastruktur eingesetzt werden. Bisher sah sich der VBB nicht in der Lage, uns nachvollziehbar darzustellen, wie derartige Drittanbieter mit den Kundendaten aus dem EFM umgehen, sie speichern, nutzen und wieder löschen.

Wiederholt mussten wir zudem darauf hinweisen, dass den Kundinnen und Kunden die Wahl gelassen werden muss, ob sie ein Foto auf der Chipkarte anbringen lassen möchten oder nicht. Wenn sich die Inhaber*innen der elektronischen Tickets auch anderweitig bei Kontrollen als berechtigte Nutzende ausweisen können, z. B. durch ihren Personalausweis, dann besteht kein Erfordernis für ein Foto auf der fahrCard, wenn die Betroffenen dies nicht möchten.

Als positive Entwicklung konnten wir vermerken, dass der VBB plant, die auf der fahrCard gespeicherten Daten zu reduzieren. Zukünftig soll nur noch die Nummer der Tarifwabe, also des größeren, aggregierten Tarifgebiets, erfasst werden. Dies stärkt den Datenschutz, da die bisher gespeicherten genauen Ortsangaben es je nach technischer Konfiguration ermöglichten, Bewegungsprofile der Kund*innen zu erstellen. Durch diese Neuerung kann demgegenüber künftig nur noch allgemein festgestellt werden, ob die jeweils kontrollierte Person in einem Tarifgebiet unterwegs ist, für das auch eine entsprechende Fahrberechtigung erworben wurde. Und nur dies kann das Ziel einer Fahrscheinkontrolle sein.

279 Siehe https://unternehmen.eticket-deutschland.de

Ebenfalls positiv hervorzuheben ist, dass der VBB eine technische Lösung bereitstellen will, mit deren Hilfe Kund*innen selbst Fahrdaten von den Chipkarten löschen können. Denn auf den Chipkarten sind bis zu zehn Datensätze von Fahrtkontrollen gespeichert. Bisher können Daten von den Chipkarten zwar über Mobilgeräte kostenfrei ausgelesen, aber nur in den Kund*innenzentren der Verkehrsunternehmen (z. B. bei der BVG und S-Bahn Berlin GmbH) an Selbstbedienungsgeräten dauerhaft gelöscht werden. Dies würde durch die neue technische Lösung zumindest zum Teil vereinfacht. Die Löschung durch die Kund*innen selbst wäre nach Auskunft des VBB für alle diejenigen Personen technisch einfach realisierbar, die über ein Smartphone mit NFC-Schnittstelle[280] verfügen. – Wir haben den VBB gebeten, diese Option auch deutlich bekannt zu geben.

Elektronische Tickets bieten den Kundinnen und Kunden erhöhten Komfort. Dies darf jedoch nicht auf Kosten des Datenschutzes gehen. Die anbietenden Unternehmen müssen für Transparenz darüber sorgen, welche Daten unter welcher Verantwortung verarbeitet werden und welche Stellen Zugriff darauf haben. Nur so können die Betroffenen ihre Rechte wahrnehmen. Die zuständigen Datenschutzaufsichtsbehörden der Länder Berlin und Brandenburg werden weiter gemeinsam die Entwicklungen bei der „VBB-fahrCard“ beobachten und auf die Behebung von Defiziten dringen.

12.4 Umgang mit Betroffenenrechten bei der Buchung von privaten Ferienunterkünften

Aus der Praxis

Private Ferienunterkünfte online zu buchen, erfreut sich zunehmender Beliebtheit. Doch werden im Rahmen einer solchen Online-Buchung bei den anbietenden Plattformen personenbezogene Daten erfasst. Die DS-GVO ermöglicht es den Betroffenen, u.a. Auskunft über die Speicherung dieser Daten zu verlangen und sie ggf. berichtigen oder löschen zu lassen. Bei uns eingehende Beschwerden zeigen, dass die Ausübung dieser Rechte, aber auch die Nutzung der Plattformen selbst nicht selten von diesen durch das Anfordern von Ausweiskopien erschwert wird.

280 NFC steht für "Near Field Communication". Hierbei handelt es sich um eine Technik, bei der Geräte über kurze Distanzen (üblicherweise wenige Zentimeter) miteinander per elektromagnetischer Induktion kommunizieren können, um Daten auszutauschen.

Gehäuft treffen bei uns Beschwerden von Bürgerinnen und Bürgern ein, die gegenüber den Online-Plattformen ihren Anspruch auf Auskunft oder Löschung geltend machen wollten und zunächst zum Zwecke einer verlässlichen Identifizierung um eine Kopie ihres Personalausweises oder Führerscheins gebeten wurden. Aber nicht nur, wenn es um die Geltendmachung von Betroffenenrechten im Verlauf der Nutzung derartiger Angebote geht, sondern auch zu Beginn der Nutzung werden Bürgerinnen und Bürger häufig dazu aufgefordert, eine Ausweiskopie bereitzustellen.

Bei der Vermietung oder Buchung privater Ferienunterkünfte über Online-Plattformen mag eine Identitätsprüfung von Gastgeber*innen und Gästen an sich ein legitimes Interesse sein; gleichwohl sind an Identitätsprüfungen mithilfe kopierter amtlicher Lichtbildausweise hohe Anforderungen zu stellen. Eine Verarbeitung einer vollständigen Ausweiskopie ist nur dann rechtmäßig, wenn sie zur Erfüllung eines Vertrags mit der betroffenen Person erforderlich ist.[281] Die bloße Nutzung der Plattform kann nicht von der Vorlage von Ausweisdaten abhängig gemacht werden.

Wenn Bürgerinnen und Bürger ihre Rechte auf Auskunft, Berichtigung oder Löschung geltend machen wollten, ist eine Identitätsprüfung nur dann rechtmäßig, wenn begründete Zweifel an der Identität der oder des Betroffenen bestehen.[282] In diesem Fall dürfen dann aber auch nur solche zusätzlichen Informationen angefordert werden, die zur Bestätigung der Identität der jeweiligen Person erforderlich sind.

Wenn eine Ausweiskopie ausnahmsweise etwa zur Vermeidung eines Identitätsdiebstahls verlangt werden kann, sollten die Kund*innen darauf hingewiesen werden, dass nicht erforderliche Daten wie Ausweisnummer oder Augenfarbe geschwärzt werden können.

Wir empfehlen den Betroffenen daher, sich gegenüber dem jeweiligen Unternehmen gegen die Praxis der pauschalen Anforderung von Ausweiskopien zu wehren.

281 Siehe Art. 6 Abs. 1 Satz 1 lit. b DS-GVO

282 Siehe Art. 12 Abs. 6 DS-GVO

12.5 Ein Mann mit vierzehn Geburtstagen

Eine Auskunftei hatte in ihrer Datenbank eine Vielzahl unrichtiger Daten zu einem Beschwerdeführer gespeichert, darunter vierzehn Geburtsdaten. Von den unrichtigen Daten in der Datenbank der Auskunftei erfuhr der Beschwerdeführer, als er von seinem Recht auf Auskunft Gebrauch machte. Hierzu sah er sich veranlasst, als ein Unternehmen bei ihm die Schulden eines seiner Namensvetter eintreiben wollte. Dieses hatte angegeben, seine Daten von der Auskunftei erhalten zu haben.

Als der Beschwerdeführer sich über die bei der Auskunftei über ihn gespeicherten Daten informieren wollte, teilte diese ihm zunächst mit, dass sie keine Daten über ihn gespeichert hätten. Auf nochmalige Nachfrage stellte sich indes heraus, dass die Auskunftei doch über entsprechende Daten in ihrer Datenbank verfügte. Die dem Beschwerdeführer daraufhin zugesandte Übersicht gab Erstaunliches preis: Die Auskunftei hatte in der Rubrik „Geburtsdatum" insgesamt vierzehn Geburtsdaten gespeichert, die allesamt dem Beschwerdeführer zugeordnet waren. Diese vierzehn Geburtsdaten erstreckten sich über eine Zeitspanne von 1977 bis 1997. Darüber hinaus beinhaltete der Datensatz 26 postalische Adressen, an denen der Beschwerdeführer bislang gelebt haben sollte. Nachdem wir uns der Sache angenommen hatten, erfuhren wir von der Auskunftei, dass diese Daten versehentlich aufgrund eines hausinternen Missverständnisses gespeichert worden seien.

Auskunfteien sind dazu berechtigt, personenbezogene Daten zum Zweck der Auskunftserteilung zu verarbeiten, wenn es zur Wahrung ihrer berechtigten Interessen erforderlich ist und nicht die Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen.[283] Die DS-GVO verlangt an dieser Stelle eine Interessenabwägung im konkreten Einzelfall. Dabei überwiegen die Grundrechte und Grundfreiheiten der betroffenen Personen z. B. regelmäßig dann nicht, wenn die Auskunfteien aktuelle Adressdaten an Gläubiger übermitteln.

Ein entscheidendes Kriterium für die Rechtmäßigkeit der Speicherung ist die Richtigkeit der Daten. Die gespeicherten Daten müssen sachlich richtig sein und

283 Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO

erforderlichenfalls aktualisiert werden.[284] Dementsprechend sind Verfahren vorzusehen, um unrichtige Daten unverzüglich zu berichtigen bzw. zu löschen. Bei einer Ansammlung von vierzehn Geburtsdaten, die einer einzigen Person zugeordnet sind, ergibt sich zwingend, dass dreizehn dieser Daten unrichtig sein müssen. Auch die 26 gespeicherten postalischen Adressen hätten Anlass für Zweifel an der Richtigkeit der Daten begründen müssen.

Dieser Fall zeigt auch plastisch, welche Folgen fehlerhafte Datensätze haben können. Für den Betroffenen war es sicher nicht angenehm, sich gegen Forderungen zu wehren, die ein Namensvetter hätte begleichen müssen.

Die Auskunftei hat uns im Rahmen unserer Untersuchung mitgeteilt, dass die hier betroffenen Daten zwischenzeitlich gesperrt seien und anschließend gelöscht würden. Darüber hinaus wurde uns zugesichert, dass dieser Vorgang zum Anlass genommen werde, die internen Verfahren technisch und organisatorisch nachzubessern.

Auskunfteien dürfen nur sachlich richtige Daten verarbeiten und sind verpflichtet, mithilfe von technisch-organisatorischen Maßnahmen sicherzustellen, dass unrichtige Daten unverzüglich berichtigt oder gelöscht werden.

284 Art. 5 Abs. 1 lit. d DS-GVO

13 Videoüberwachung

13.1 Wichtige Dokumente zur Videoüberwachung verabschiedet

Aus der Praxis

In diesem Jahr wurden gleich zwei wichtige Dokumente zur Videoüberwachung beschlossen: Zum einen verabschiedete bereits Anfang des Jahres der Europäische Datenschutzausschuss (EDSA) seine Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte.[285] Im September zogen dann auch die deutschen Aufsichtsbehörden nach und aktualisierten ihre Orientierungshilfe zur Videoüberwachung durch nicht öffentliche Stellen.[286]

Wie wir bereits im Vorjahr berichtet haben,[287] war unsere Behörde an der Erstellung der Leitlinien des EDSA maßgeblich beteiligt und koordinierte europaweit als Hauptberichterstatterin die Arbeiten. Inhaltlich stellen die Leitlinien u.a. fest, dass jede Videoüberwachung mit einem Eingriff in die Persönlichkeitsrechte verbunden ist. Deshalb muss ihr stets ein berechtigtes Interesse der Kamerabetreiber*innen zugrunde liegen. Dieses Interesse muss objektiv vorliegen, d. h., bei einer Videoüberwachung aus Sicherheitsgründen müssen stets auch tatsächliche Anhaltspunkte für eine Gefahr für Leib, Leben oder Sachgüter vorliegen. Die Leitlinien stellen klar, dass ein rein subjektives Sicherheitsgefühl nicht genügt, um eine Videoüberwachung zu rechtfertigen.

Auch mit Blick auf die Verarbeitung biometrischer Daten schaffen die Leitlinien Klarheit. Gemäß der Datenschutz-Grundverordnung (DS-GVO) ist es privaten Unternehmen ohne ausdrückliche Einwilligung der Betroffenen grundsätzlich verboten, biometrische Daten zum Zwecke der Identifizierung bestimmter Personen zu verarbeiten. Die Leitlinien konkretisieren nunmehr die strengen Anforderungen der DS-GVO an die Wirksamkeit solcher Einwilligungen. Außerdem bieten sie

285 Siehe https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitlinien

286 Siehe https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/orientierungshilfen

287 JB 2019, 14.2.

praktische Hilfestellungen zu Fragen der Transparenz bei Videoüberwachungsmaßnahmen und zur Ausübung der Betroffenenrechte.

Im September verabschiedete dann die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine aktualisierte Fassung der „Orientierungshilfe zur Videoüberwachung durch nicht öffentliche Stellen". Die ursprüngliche, noch unter der früheren Rechtslage erstellte Orientierungshilfe wurde grundlegend überarbeitet und an die rechtlichen Rahmenbedingungen der DS-GVO sowie an die o. g. Leitlinien des EDSA angepasst. Sie enthält auch Teile, die über die europäischen Leitlinien hinausgehen, wie z. B. Abschnitte zur Videoüberwachung von Beschäftigten und zur datenschutzrechtlichen Bewertung von Tür- und Klingelkameras, Drohnen und Wildkameras sowie Dashcams. Darüber hinaus wird eine Checkliste für Kamerabetreiber*innen mit den wichtigsten Prüfungspunkten im Vorfeld einer Videoüberwachung bereitgestellt.

Beide Dokumente zur Videoüberwachung stellen nicht nur wichtige Beiträge zur einheitlichen Anwendung der DS-GVO dar. Sie beinhalten auch praktische Hinweise für Betreiber*innen von Videoanlagen. Anders als die Orientierungshilfe der deutschen Aufsichtsbehörden richten sich aber die europäischen Leitlinien nicht in erster Linie an Kamerabetreiber*innen, sondern enthalten auch ein eigenes Kapitel mit Hinweisen für Betroffene zur Ausübung ihrer Rechte.

13.2 Testbahnhof Südkreuz – „Intelligente" Videoüberwachung doch nicht so schlau

Nachdem die Bundespolizei den Bahnhof Südkreuz jahrelang als Versuchslabor für biometrische Gesichtserkennung genutzt hat, wollte nunmehr auch die Deutsche Bahn den Bahnhof für eigene Tests nutzen.[288] Dabei ging es – anders als bei den Tests der Bundespolizei – nicht um die Verarbeitung biometrischer Daten zum Zwecke der Identifizierung, sondern um die automatisierte Erkennung von Gefahrensituationen.

288 Siehe JB 2018, 4.4 und JB 2019, 11.1

Im Einzelnen waren folgende fünf Szenarien Gegenstand des Tests:

- Liegende Personen (z. B. gestürzte Personen, die medizinische Hilfe benötigen),
- Betreten definierter Zonen (z. B. Personen, die sich zu nah an der Bahnsteigkante befinden),
- Ansammlungen und Personenströme (z. B. Erkennen von Ansammlungen vor Rolltreppen oder dynamische Bewegung von Personengruppen),
- Personenzählung (z. B. Anzahl von Personen in einem definierten Bereich),
- abgestellte Gegenstände (z. B. über längere Zeit unbeaufsichtigte Gepäckstücke).

Für den Test wurde das Videomaterial genutzt, welches ohnehin täglich am Bahnhof Südkreuz aufgenommen wird. Denn wie viele Bahnhöfe der Deutschen Bahn und der Berliner Verkehrsbetriebe (BVG) ist der Bahnhof Südkreuz mit zahlreichen Überwachungskameras ausgestattet. Diese dienen in erster Linie der Wahrung des Hausrechts und der Sicherheit der Fahrgäste sowie bei entsprechenden Vorfällen auch dazu, eventuelle Schadensersatzansprüche geltend machen zu können. Daher sind die Daten, die mit den Videokameras verarbeitet werden, so hochauflösend, dass Personen erkannt und ggf. identifiziert werden können.

Anhand dieses Videomaterials wurden verschiedene Software-Produkte daraufhin getestet, wie zuverlässig sie in einer der oben genannten Situationen reagieren. Für den Test wurde die Technik von drei ausgewählten Anbieter*innen an die herkömmliche Videoüberwachungsanlage am Bahnhof Südkreuz angeschlossen. Die getestete Software sollte nun durch die automatische Auswertung des vorhandenen Videomaterials erkennen, ob Vorfälle der genannten Situationen vorliegen. Darüber sollte dann anschließend das Sicherheitspersonal in der Videoleitstelle automatisch informiert werden. Dieses sollte sich die Situation auf dem Bildschirm anschauen und über weitere Maßnahmen entscheiden.

Ziel des Tests war es, das Personal der Videoleitstelle im Regelbetrieb durch das Erkennen der genannten Szenarien bei seiner täglichen Arbeit zu unterstützen.

Die uns vorliegenden Ergebnisse des Tests führen zu erheblichen Zweifeln an der datenschutzrechtlichen Zulässigkeit des Einsatzes der hier erprobten Technik im

Regelbetrieb. Zwar hat die Deutsche Bahn durchaus ein berechtigtes Interesse, in die o. g. Situationen einzugreifen und für die Sicherheit des Personals und der Fahrgäste zu sorgen bzw. ihr Hausrecht am Bahnhof wahrzunehmen. Allerdings müssen die Maßnahmen, die zur Erreichung dieser Ziele ergriffen werden, stets geeignet, erforderlich und verhältnismäßig sein.[289]

Hier bestehen bereits erhebliche Bedenken hinsichtlich der Eignung der „intelligenten" Videoüberwachung. Nach den uns vorliegenden Informationen ist davon auszugehen, dass die Marktreife für den Regeleinsatz in dem komplexen Umfeld eines Personenbahnhofs zum jetzigen Zeitpunkt nicht gegeben ist. Die Systeme erkannten viele Situationen nicht oder erzeugten Fehlalarme. Als Folge konnte die angestrebte Trefferquote von 95 % erfolgreicher Alarme von keinem System auch nur annähernd erreicht werden. Teilweise betrug die Trefferquote lediglich 27 %. Demzufolge besteht bei allen Systemen Optimierungsbedarf.

Vor diesem Hintergrund stellt sich auch die Frage nach der Verhältnismäßigkeit, da im Regelbetrieb eine Vielzahl unbescholtener Fahrgäste von der Videoüberwachung betroffen wäre, die täglich den Bahnhof nutzen. Aufgrund der Fehlalarme würden sie zu Unrecht zum Gegenstand weiterer Überprüfungen werden. Führt die angesprochene Maßnahme aufgrund der hohen Fehlerquoten faktisch nicht zu einer Verbesserung der Sicherheit der Fahrgäste, so ist diese unverhältnismäßig und damit nicht mit den datenschutzrechtlichen Vorgaben zu vereinbaren.

Umso erstaunlicher ist, dass das Bundesinnenministerium und die Deutsche Bahn Ende des Jahres angekündigt haben, die Möglichkeiten zur intelligenten Videoanalyse in der praktischen Anwendung im Umfeld des Bahnhofs Südkreuz über einen Projektzeitraum von weiteren drei Jahren auszuloten, da sie trotz allem in Videoanalysesystemen vielversprechende Ansätze für die Erkennung und Meldung betriebsrelevanter Situationen sehen.

Wir werden auch künftige Tests eng begleiten und daraufhin kontrollieren, ob dabei die datenschutzrechtlichen Vorgaben eingehalten werden.

289 Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO

Nach Auswertung der uns vorliegenden Testergebnisse gehen wir davon aus, dass ein Einsatz derartiger Systeme aufgrund hoher Fehlerquoten aktuell kein verlässliches Hilfsmittel darstellt, die Deutsche Bahn bei der Wahrnehmung ihrer Aufgaben zu unterstützen. Der Einsatz der getesteten Software im Regelbetrieb ist daher nach derzeitigem Stand nicht zulässig.

13.3 Noch stärker im Fokus: Videoüberwachung im Kleingewerbe

Wir hatten es mit einer Vielzahl von Fällen zur Videoüberwachung im Einzelhandel und im Gaststättengewerbe zu tun. Dies war schon in den vorherigen Jahren ein Schwerpunkt unserer Tätigkeit, da Überwachungskameras immer günstiger werden und überall zu haben sind, sich die Betreiber*innen hingegen oftmals nicht über die datenschutzrechtlichen Vorgaben im Klaren sind. Dieses Jahr kam noch hinzu, dass aufgrund der Corona-Pandemie Kleingewerbetreibende stärker als sonst im Fokus der Polizei und der Ordnungsbehörden standen. Im Rahmen von Überprüfungen kontrollierten diese seit Beginn der Pandemie die Einhaltung der Abstandsregeln und Hygienemaßnahmen in Gewerbeeinheiten im gesamten Stadtgebiet. Dies betraf u.a. gastronomische Einrichtungen, wie Restaurants, Gaststätten, Imbisse und Shisha-Bars, aber auch andere Kleingewerbe, wie Spätkauf-Läden, Friseurgeschäfte, Nagelstudios, Backshops, Spielcasinos, Sport-Bars und Wettbüros. Für unsere Tätigkeit hatte dies den positiven Nebeneffekt, dass die genannten Behörden bei der Kontrolle der Einhaltung der Corona-Maßnahmen des Öfteren auch einen Verdacht auf illegale Videoüberwachungen feststellten und uns die Fälle zur weiteren Bearbeitung übermitteln konnten. Da wir aufgrund unserer geringen personellen Kapazitäten – anders als Polizei und Ordnungsämter – nicht ständig vor Ort sein können, sind wir auf solche Mithilfe sowie auf Hinweise aus der Bevölkerung angewiesen.

Oftmals betrafen diese Fälle Videoüberwachungen, die über die Grenzen des eigenen Ladengeschäfts hinaus das öffentliche Straßenland erfassten. Eine solche Überwachung ist nicht zulässig, da den Betreiber*innen regelmäßig das berechtigte Interesse zur Überwachung des öffentlichen Raums fehlt. Ausnahmen bestehen nur in engen Bereichen und lediglich dann, wenn dies im konkreten Fall erforderlich ist, um z. B. Sachbeschädigungen entgegenzuwirken. So hat die

Rechtsprechung in einem Fall die Erweiterung des Erfassungsbereichs auf maximal einen Meter über die Grundstücksgrenzen hinaus für zulässig erachtet, da nur so Schmierereien an der Hausfassade eingedämmt werden konnten.

Auch die Überwachung der eigenen Gewerberäume ist an strenge Voraussetzungen geknüpft, da die Videoüberwachung regelmäßig einen Eingriff in die Persönlichkeitsrechte der von derartigen Maßnahmen betroffenen Personen darstellt. Insbesondere ist die Erhebung personenbezogener Daten mit Videotechnik nur zulässig, soweit sie u.a. zur Wahrung berechtigter Interessen erforderlich ist und sofern nicht schutzwürdige Interessen der betroffenen Personen überwiegen.[290] Die Videoüberwachung eines Geschäftsraums mit regelmäßigem Kundenverkehr ist z. B. zur Prävention oder zur Beweissicherung von Diebstählen nur dann zulässig, wenn objektiv eine Gefahrenlage besteht. Ein Indiz dafür ist z. B., wenn es in der Vergangenheit tatsächlich zu kriminellen Vorfällen in dem Ladengeschäft oder in der Nachbarschaft gekommen ist. Diese Vorfälle sollten anhand von Anzeigen bei der Polizei mit Aktenzeichen dokumentiert werden. Ein rein subjektives Unsicherheitsgefühl oder Angst vor Diebstählen reicht nicht aus. Besteht eine Gefahrenlage nicht, ist die Videoüberwachung abzuschalten. Ebenfalls nicht zulässig ist eine Videoüberwachung zur Verhaltens- und Leistungskontrolle der dort tätigen Angestellten.

Andere Fälle betrafen – bis zu ihrer Corona-bedingten Schließung – Gaststätten, die besonders zu beurteilen sind, da sie zum längeren Verweilen, Entspannen und Kommunizieren gedacht sind. Das dem Freizeitbereich zuzurechnende Verhalten der Gäste einer Gaststätte geht mit einem besonders hohen Schutzbedarf des Persönlichkeitsrechts der Betroffenen einher. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucher*innen und greift damit besonders intensiv in das Persönlichkeitsrecht der Gäste ein. Ihre schutzwürdigen Interessen überwiegen daher im Normalfall gegenüber dem berechtigten Interesse der Gastronom*innen an einer Überwachung.

In sehr vielen Fällen ging es schließlich um die mangelhafte Umsetzung der Transparenzpflicht. Fehlende oder mangelhafte Hinweise auf die Videoüberwa-

290 Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO

chung sind sogar die häufigsten Verstöße, die im Rahmen der Gewerbekontrollen von Ordnungsämtern und Polizei festgestellt werden. In diesem Zusammenhang verweisen wir stets auf ein Beispiel für ein Hinweisschild, das wir auf unserer Internetseite veröffentlicht haben,[291] und erklären den Betreiber*innen ausführlich, welche Informationen ihren Gästen, Kund*innen und Beschäftigten mitzuteilen sind.[292]

Aufgrund unserer guten Erfahrungen haben wir beschlossen, unsere Kooperation mit der Polizei in diesem Bereich auszubauen. Gemeinsam mit der Polizei haben wir einen Handlungsleitfaden entwickelt, der es Polizeibeamt*innen vor Ort erleichtern soll, eine illegale Videoüberwachung zu erkennen und zu dokumentieren. Wir erhoffen uns davon eine erhebliche Steigerung der Effizienz in der Zusammenarbeit beider Behörden.

Die kooperative Unterstützung der Polizei und der Ordnungsämter ermöglicht uns eine breitgestreute Überprüfung von Videoüberwachungsanlagen im Kleingewerbe des gesamten Stadtgebiets, die wir zuvor in diesem Umfang nicht leisten konnten. Zur Zulässigkeit von Videoüberwachungsanlagen haben wir eine Orientierungshilfe und eine Leitlinie erstellt, die wir auf unserer Internetseite zum Abruf bereithalten.[293]

291 www.datenschutz-berlin.de/themen-videoueberwachung_dsgvo.html
292 Art. 13 DS-GVO
293 Siehe 13.1

14 Sanktionen

14.1 Entwicklungen in der Sanktionsstelle

Im dritten Jahr des Wirksamwerdens der Datenschutz-Grundverordnung (DS-GVO) bearbeiten wir nunmehr weit überwiegend Fälle nach den neuen Bußgeldvorschriften. Daneben beziehen sich nur noch sehr wenige Fälle auf die alte Rechtslage.

Wir haben dieses Jahr 47 Bußgelder in Höhe von insgesamt 77.250,00 Euro festgesetzt.

Daneben wurden 38 Zwangsgeldbescheide erlassen.

In 5 Fällen haben wir einen Strafantrag gestellt.

14.2 Bußgelder wegen unbefugter Nutzung der Polizeidatenbank POLIKS

Ein großer Teil der von der Sanktionsstelle geführten Verfahren richtet sich gegen Polizeibeamtinnen und Polizeibeamte, die unbefugt, d. h. ohne einen dienstlichen Anlass, personenbezogene Daten Dritter aus der polizeiinternen Datenbank POLIKS abrufen.

POLIKS ist eine der wichtigsten elektronischen Arbeitshilfen der Polizei und enthält dementsprechend viele und zum Teil sehr sensitive personenbezogene Daten. In der Datenbank werden u.a. Daten von Beschuldigten, Straftäter*innen, Opfern und Zeug*innen erfasst und gespeichert. Die Polizei nutzt POLIKS als Informationssystem für ihre gesetzlichen Aufgaben im Bereich der Strafverfolgung und der Gefahrenabwehr.

Leider greifen immer wieder einige Polizeibeamt*innen und Polizist*innen unerlaubt zu privaten Zwecken auf den in POLIKS enthaltenen umfangreichen Datenkatalog zu.

In einem Fall nutzte eine Polizistin POLIKS, um die Ex-Freundinnen des neuen Lebensgefährten ausfindig zu machen und sie anschließend zu Gesprächen aufzusuchen.

In einem anderen Fall hatte ein Polizist die Daten sämtlicher Nachbar*innen aus dem eigenen Mehrfamilienhaus abgefragt, um die aus POLIKS gewonnenen Informationen später in nachbarschaftlichen Streitigkeiten gegen die einzelnen Bewohner*innen des Hauses auszuspielen.

In einem weiteren Fall hatte ein Polizeibeamter auf Wunsch diverser Freund*innen Informationen aus POLIKS zusammengetragen und über ein privates Instant Messenger System versendet. Hier ging es um Daten von Lehrer*innen der Kinder, von Nachbar*innen oder gar Lebensgefährt*innen der Anfragenden.

Weiterhin haben wir ein Bußgeld gegen einen Polizeibeamten verhängt, der POLIKS als Suchmaschine für Kontaktdaten eines Verkäufers verwendete. Nachdem er bei der Suche über die Suchmaschine „Google" nicht die richtige Telefonnummer des Verkäufers eines Kartenspiels fand, versuchte er über POLIKS, die entsprechenden Daten herauszubekommen.

In diesem Jahr haben wir insgesamt 33 Verfahren gegen Polizeibeamtinnen und Polizeibeamte eingeleitet und bereits 9 Bußgelder gegen diesen Personenkreis erlassen. Viele Verfahren sind aber noch nicht ausermittelt.

14.3 Der Datenschutz braucht Landgerichte auch erstinstanzlich

Mit dem „Entwurf eines Gesetzes zur Effektivierung des Bußgeldverfahrens"[294] will der Bundesrat die bisher im Bundesdatenschutzgesetz (BDSG) vorgesehene erstinstanzliche Zuständigkeit der Landgerichte für nach der Datenschutz-Grundverordnung (DS-GVO) festgesetzte Geldbußen, die einen Betrag von mehr als 100.000,00 Euro übersteigen,[295] streichen. Würde dies beschlossen werden, müss-

294 BR-Drs. 107/20

295 Siehe § 41 Abs. 1 BDSG

ten künftig Amtsgerichte über Geldbußen in diesen Größenordnungen entscheiden.

Ordnungswidrigkeitenverfahren auf der Grundlage der DS-GVO, die mit sehr hohen Geldbußen abgeschlossen werden, weisen sowohl rechtlich als auch hinsichtlich der wirtschaftlichen und technischen Zusammenhänge eine besondere Komplexität auf und bedürfen daher einer Würdigung durch Spruchkörper eines Kollegialgerichts, wie es sie bei Landgerichten, nicht jedoch bei Amtsgerichten gibt. Solche Verfahren sind mit Wirtschaftsstrafsachen vergleichbar, die ebenfalls den Landgerichten zugewiesen sind. Nicht ohne Grund hat sich der europäische Gesetzgeber bei den Bußgeldvorschriften der DS-GVO am Kartellrecht orientiert.

Das ausgewiesene Ziel des Gesetzentwurfs, Bußgeldverfahren zu effektiveren, würde mit der angestrebten Änderung der gerichtlichen Zuständigkeit nicht erreicht werden. Beim Entwurf des Gesetzes wurde in eklatanter Weise die Vielschichtigkeit von DS-GVO-Geldbußen verkannt. Eine Streichung der landgerichtlichen Zuständigkeit für diese Verfahren würde die Amtsgerichte zudem nicht etwa entlasten, sondern im Gegenteil noch stärker als bisher belasten, weil die Komplexität derartiger Verfahren die Arbeitskapazitäten der Einzelrichter*innen der Amtsgerichte komplett sprengen würde.

Das Sanktionsrecht der DS-GVO ist – anders als der Bundesrat unterstellt – mit der Sanktionierung herkömmlicher deutscher Ordnungswidrigkeiten, wie etwa Geldbußen im Straßenverkehr, in keiner Weise vergleichbar. Anders als dort geht es in den Verfahren nach der europäischen DS-GVO nicht etwa um die Verfolgung von Bagatelldelikten, sondern um unionsweit höchst relevante Verfahren zum Schutz des freien Datenverkehrs und der Privatsphäre der Bürgerinnen und Bürger. Dabei können Millionen von personenbezogenen Daten und weltweit agierende Unternehmen betroffen sein. Für ähnlich komplexe Ordnungswidrigkeiten in Kartellangelegenheiten ist in Deutschland sogar eine Zuständigkeit der Oberlandesgerichte gegeben. Diese Wertung kommt auch in dem insoweit eindeutigen Wortlaut von § 41 Abs. 2 Satz 1 BDSG zum Ausdruck, der eine entsprechende Anwendung der Vorschriften über das Strafverfahren und damit auch eine Besetzung der Strafkammern als sog. große Bußgeldkammern gemäß § 76 Gerichtsverfassungsgesetz (GVG) vorsieht.

Es müsste bei diesen Verfahren nach der DS-GVO also eigentlich nicht um eine Einschränkung einer landgerichtlichen Zuständigkeit gehen, sondern vielmehr um die Überlegung, ob diese Verfahren nicht sogar vollständig in erster Instanz in die Zuständigkeit eines höheren Gerichts verwiesen werden sollten, ggf. auch – zumindest teilweise – an ein Oberlandesgericht in Anlehnung an die kartellrechtlichen Regelungen.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat als Vorsitzende des Arbeitskreises Sanktionen eine Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 22. September 2020 vorbereitet, die die Beibehaltung der landgerichtlichen Zuständigkeit für DS-GVO-Geldbußen über 100.000,00 Euro fordert. Die DSK hat diese Entschließung verabschiedet.[296]

14.4 Erfundene Stellenanzeigen bei der Bundesagentur für Arbeit

Auf der Online-Jobbörse der Bundesagentur für Arbeit wurden mutmaßlich erfundene Stellenanzeigen veröffentlicht, um an Bewerber*innendaten für einen illegalen Weiterverkauf zu gelangen. Nach Medienberichten soll es sich hierbei um etwa 120.000 fingierte Stellenanzeigen handeln.

Wir haben aufgrund eines Hinweises der Bundesagentur für Arbeit hierzu bereits im Jahr 2019 einen Strafantrag bei der Staatsanwaltschaft gestellt.

Nach Ablauf mehrerer Monate wurde uns vonseiten der Staatsanwaltschaft mitgeteilt, dass sie die Einstellung des eingeleiteten Strafverfahrens vorhabe, weil eine rechtswidrige Tat nicht nachgewiesen werden könne. Begründet wurde dies u.a. damit, dass keine konkreten Geschädigten bekannt seien und sowohl gegenüber der Bundesagentur für Arbeit als auch den Betroffenen das betrügerische Handeln transparent gewesen sei.

296 Siehe https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

Die Einstellung des Verfahrens war für uns nicht nachvollziehbar. Angesichts des vorgeworfenen Ausmaßes des Datenmissbrauchs sind aus unserer Sicht weitere Ermittlungen und eine Ahndung des Vorfalls bei Nachweis der Tat dringend notwendig. Dies dient auch der Abschreckung möglicher Nachahmer*innen. In einer Stellungnahme haben wir die Staatsanwaltschaft um weitere Ermittlungen gebeten und sie aufgefordert, uns über die Entwicklungen zu informieren. Dieses Schreiben blieb bis heute unbeantwortet. Aus den Medien haben wir schließlich von der Einstellung des Strafverfahrens durch die Staatsanwaltschaft erfahren. Wenn es bei dieser Entscheidung bleibt und das Verfahren von der Staatsanwaltschaft nicht wieder aufgenommen wird, werden wir deren Akten anfordern und die Einleitung eines Ordnungswidrigkeitsverfahrens in eigener Verantwortung prüfen.

Das Erschleichen von Bewerber*innendaten durch fingierte Stellenanzeigen ist kein Bagatelldelikt.

15 Telekommunikation und Medien

15.1 „Wir wissen, was du letzten Sommer gelesen hast“ – Drittinhalte und Tracking auf Webseiten

Aus der Praxis

Auch in diesem Jahr hat uns die Nachverfolgung von individuellem Verhalten im Internet „auf Trab gehalten“. Neben den bereits laufenden Verfahren im Kontext des Trackings haben wir uns mit neuer Rechtsprechung, neuen Gestaltungsmerkmalen von Einwilligungs-Bannern, weiteren Detailproblemen und dem nächsten Versuch einer europäischen ePrivacy-Verordnung beschäftigt. Auch wenn wir zunehmend kooperativen Verantwortlichen begegnen, bleibt die Thematik eine Gemengelage, deren Überprüfung viel Zeit in Anspruch nimmt.

Seit vielen Jahren stellt es ein wachsendes Problem für die Privatsphäre dar, wenn auf Webseiten Dienste von Drittanbietern[297] sowie Cookies oder ähnliche Tracking-Techniken eingebunden werden, mittels derer personenbezogene Daten von Webseitengästen verarbeitet werden. Insbesondere der Einsatz von Mechanismen, mit denen Webseitengäste und ihre Vorlieben über das einzelne Webangebot hinaus wiedererkannt werden können, führt in der Praxis zur Bildung umfangreicher Verhaltensprofile.

15.1.1 Dauerbaustelle Tracking

Mit mehreren Veröffentlichungen hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits einige The-

297 Solche Inhalte von Dritten können einerseits sichtbar sein, wie z. B. Werbebanner, Landkarten, Videos oder Interaktionselemente von sozialen Netzwerken. Andererseits gibt es auch unsichtbare Elemente, wie winzig kleine Bilder, die einzig dafür existieren, Daten über Webseitengäste bzw. die Nutzung des Webangebots an den jeweiligen Drittdienst weiterzuleiten.

men rund ums Tracking aufgegriffen und Verantwortliche über die rechtlichen Rahmenbedingungen informiert.[298] Bedingt durch die Vielschichtigkeit der Thematik und infolge neuer Rechtsprechung zu einzelnen Aspekten sind die Anforderungen jedoch laufend zu evaluieren. Nach wie vor ist es z. B. nicht gelungen, die EU-Richtlinie für den Schutz der Privatsphäre in der elektronischen Kommunikation (besser bekannt als ePrivacy-Richtlinie)[299] durch eine europäische Verordnung abzulösen, die im Gegensatz zu einer Richtlinie in jedem EU-Mitgliedstaat unmittelbar gelten würde, ohne dass eine Umsetzung ins nationale Recht erforderlich wäre.

Im Raum steht neben den Vorgaben der Datenschutz-Grundverordnung (DS-GVO) daher auch immer noch die bei einer europäischen Richtlinie erforderliche nationale Umsetzung der ePrivacy-Richtlinie.[300] In Deutschland stellt sich in diesem Zusammenhang insbesondere nach wie vor die Frage, ob diese tatsächlich ordnungsgemäß im Telemediengesetz (TMG) erfolgt ist. Nach einer Vorlageentscheidung des Europäischen Gerichtshofs (EuGH) im Verfahren „Planet49"[301] hat sich nunmehr der Bundesgerichtshof (BGH) zumindest zu einem Absatz eines Paragrafen des TMG geäußert.[302] Gegenstand des Verfahrens war ein Streit, in dem das beklagte Unternehmen personenbezogene Daten über das Nutzungsverhalten von Verbraucher*innen mittels Cookies zu pseudonymisierten Nutzungsprofilen verarbeitete und diese für personalisierte Werbung nutzte. Anders als dies zuvor von der DSK bewertet wurde,[303] geht der BGH in seiner Entscheidung davon aus, dass sich § 15 Abs. 3 Satz 1 TMG europarechtskonform auslegen lässt.

Nach dem Wortlaut des § 15 Abs. 3 Satz 1 TMG wäre die Datenverarbeitung dann zulässig, wenn die betroffenen Personen entsprechend informiert wurden und

298 Hinweise der DSK zu Google Analytics, siehe 15.4; Positionsbestimmung sowie Orientierungshilfe der DSK für Telemedienanbieter, siehe JB 2018, 12.3 und JB 2019, 13.3

299 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

300 Primär Art. 5 Abs. 3 der ePrivacy-Richtlinie

301 Siehe hierzu JB 2019, 13.2.

302 BGH, Urteil vom 28. Mai 2020 – I ZR 7/16

303 Siehe Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand März 2019, S. 2 ff.; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/orientierungshilfen

nicht widersprochen haben (sog. Widerspruchslösung). Der BGH nimmt nun an, dass schon in dem Fehlen einer wirksamen Einwilligung ein solcher Widerspruch gesehen werden könne und deshalb eine aktive Einwilligung erforderlich sei. Unter Zugrundelegung dieser Auslegung wendet er die TMG-Vorschrift neben der DS-GVO an. Diese europarechtskonforme Auslegung des TMG ist allerdings rechtsdogmatisch nur schwer nachzuvollziehen.

Allein die Tatsache, dass die nationalen Datenschutzaufsichtsbehörden und das deutsche Zivilgericht der höchsten Instanz bei einer sehr praxisrelevanten Rechtsfrage zwar im Ergebnis darin übereinstimmen, dass eine Verarbeitung, wie sie den Gerichten zur Entscheidung vorlag, einwilligungsbedürftig ist, jedoch bei der Herleitung dieses Ergebnisses voneinander abweichende Auffassungen vertreten, verdeutlicht das Ausmaß der bestehenden Rechtsunklarheit.

Kurz nach der Entscheidung wurde zudem der Referentenentwurf für ein „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze" (TTDSG) bekannt. Das geplante Gesetz soll in erster Linie der Umsetzung der „EU-Richtlinie über den europäischen Kodex für die elektronische Kommunikation"[304] dienen – hierdurch werden gleichermaßen aber auch die Regelungen des TMG neu gefasst. Da der bisherige Entwurf ebenfalls hinter einer europarechtskonformen Umsetzung der ePrivacy-Richtlinie sowie den Anforderungen einer Anpassung an die DS-GVO zurückbleibt, hat die DSK im November einen deutlichen Appell an den Gesetzgeber veröffentlicht, die ePrivacy-Richtlinie endlich vollständig und im Einklang mit der DS-GVO umzusetzen.[305]

304 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation

305 Entschließung der DSK vom 25. November 2020: „Betreiber von Webseiten benötigen Rechtssicherheit. Bundesgesetzgeber muss europarechtliche Verpflichtungen der ‚e-Privacy-Richtlinie' endlich erfüllen"; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

15.1.2 Gemengelage in den Beschwerde- und Prüfverfahren

Nicht erst seitdem die DS-GVO im Mai 2018 wirksam wurde, erhalten wir regelmäßig Beschwerden von Webseitengästen, deren Verhalten ohne Rechtsgrundlage analysiert und zu mannigfachen Werbezwecken weiterverarbeitet wird. Während wir ursprünglich vor allem mit Fällen konfrontiert waren, in denen Webseitenbetreiber*innen gar nicht erst versucht haben, eine Zustimmung für einwilligungsbedürftige Prozesse einzuholen, steht mittlerweile häufig die Wirksamkeit einer eingeholten Einwilligung in Frage.

Eine selbstbestimmte und informierte Einwilligung setzt u.a. voraus, dass den Webseiten-gästen zuerst einmal verständlich dargelegt werden muss, welche Datenverarbeitungen durch wen und zu welchen Zwecken erfolgen sollen. Auch muss die betroffene Person eine echte Wahl haben und darf (im Vergleich zur Zustimmung) keinen Mehraufwand damit haben, die Einwilligung abzulehnen. Soll eine Einwilligung für verschiedene Verarbeitungszwecke oder für die Offenlegung an unterschiedliche Dritte eingeholt werden, müssen den Besucher*innen zudem einfache Möglichkeiten zur Verfügung gestellt werden, im Detail zu konfigurieren, welchen Datenverarbeitungen sie zustimmen und welchen nicht.

Vor dem Hintergrund der auch medial sehr präsenten Entwicklungen konnten wir dieses Jahr sowohl auf Seiten der Verantwortlichen als auch auf Seiten der Betroffenen zumindest einiges an Bewegung erkennen. Bereits die DSK-Veröffentlichung der Orientierungshilfe für Anbieter von Telemedien und das EuGH-Urteil im Verfahren „Planet49“ im letzten Quartal 2019 hatten dazu geführt, dass diverse Webseitenbetreiber*innen das Tracking-Thema evaluiert haben. Ein noch größerer Schub an Veränderungen wurde nach dem o. g. BGH-Urteil sichtbar, als auf vielen Webseiten plötzlich größere und inhaltlich ausdifferenziertere Cookie-Banner erschienen sind. Spiegelbildlich konnte wiederum eine erhöhte Sensibilisierung der Webseitenbesucher*innen verzeichnet werden, die spürbar mehr Beschwerden und Prüfanregungen zu diesem Thema bei uns eingereicht haben.

Die seither häufiger auffindbaren Einwilligungsdialoge sind sicherlich ein Fortschritt. Zunehmend werden die Zwecke der Datenverarbeitung nun zumindest grob erläutert und oft auch die eingebundenen Dienste von Drittanbietern ge-

nannt. Wenn es sich hierbei jedoch um eine unüberschaubare Anzahl sog. „Partner“ handelt, bleiben die Webseitengäste dennoch ratlos zurück – zumal noch immer kaum abgeschätzt werden kann, welche Informationen über die eigene Person durch Beobachtung und Profilbildung letztlich angesammelt werden. Und nach wie vor gibt es Einwilligungsdialoge mit überbordenden Informationen, die sich häufig nicht präzise auf die relevanten Datenverarbeitungsprozesse beziehen. Die daraus folgende Intransparenz wird teilweise begleitet von einer bewusst zermürbenden Gestaltung auf bisweilen mehreren Ebenen, bei der Webseitengäste teilweise erheblich mehr Aufwand betreiben müssen, wenn sie kein Tracking wünschen. Nicht selten haben derart nutzungsunfreundliche Gestaltungen das unerfreuliche Ergebnis, dass das Tracking letztlich hingenommen wird.

Appelle, datensparsame Formen der Werbung zu entwickeln, sind bisher meist verhallt, da es für die Verantwortlichen schließlich von Vorteil ist, die Nutzenden möglichst umfassend auszuforschen. Mithin nutzen die Verantwortlichen auch jede vermeintlich verfügbare Grauzone, um ihre (finanziellen) Interessen zu verfolgen. Und von diesen Grauzonen gibt es viele. Unsere Prüfungen zeigen u.a. auch deswegen sehr unbefriedigende Ergebnisse, weil die Webseitenbetreibenden mit der wohlgewählten Gestaltung ihrer Benutzeroberflächen versuchen, die Webseitengäste zu einer schnellen Zustimmung zu verführen. So wird die Taste, mit der eine umfassende Einwilligung erteilt wird, gerne sehr deutlich hervorgehoben. Die Möglichkeit zum Ablehnen der Einwilligung wird dagegen optisch unauffällig bis kaum sichtbar gehalten und/oder mehrdeutig beschriftet (wenn diese Möglichkeit denn überhaupt auf der ersten Ebene der Banner enthalten ist). So wird der jahrelang bei PC- und Internetnutzenden antrainierte Reflex zum Wegklicken von störenden Meldungen zum Erschleichen einer eben nicht informierten Einwilligung genutzt. Die Grenzen der rechtlichen Zulässigkeit derartiger Methoden werden letztlich Gerichte abwägen müssen.

Selbst bei offensichtlichen Mängeln erweisen sich die von uns eingeleiteten Prüfverfahren leider häufig als langwierig, da wir uns nicht nur darauf beschränken (können), die Gestaltung der Cookie-Banner zu sichten, weil dies nur die Spitze eines Eisbergs ist. Auch wenn Beschwerdeführer*innen nur eine fehlende Auswahlmöglichkeit im Banner oder den Einsatz einzelner Tracking-Programme rügen, sind es vielschichtige Verkettungen von Verarbeitungsprozessen im Hintergrund, die von uns aufzuklären sind. Diese Sachverhalte zu ermitteln und zu bewerten

ist einerseits rechtlich und technisch enorm komplex, da regelmäßig eine fast unüberschaubare Anzahl von Drittanbietern mit der Webseite und untereinander verknüpft ist. Andererseits ändern sich die Prozesse auf den Webseiten auch in tatsächlicher Hinsicht regelmäßig, indem z. B. Banner optisch verändert, die eingebundenen Techniken ergänzt oder entfernt und Informationen umgeschrieben werden. Dies muss jeweils im Detail dokumentiert und analysiert, außerdem müssen die Verantwortlichen hierzu angehört werden.

Mit der DS-GVO und einigen wegweisenden Urteilen wird auch den Betreiber*innen von Webangeboten immer klarer, dass es nicht mehr möglich ist, auf Zeit zu spielen. Die Aufsichtsbehörden können nun mit mehr Rechtssicherheit gegen Verantwortliche vorgehen, die weiterhin das Verhalten der Webseitenbesucher*innen im Internet verfolgen, ohne zuvor eine informierte Einwilligung einzuholen. Wir stellen uns dieser sehr arbeitsintensiven Aufgabe auch, um für mehr Gleichbehandlung im Netz zu sorgen. Aufgrund rechtlicher und technischer Hürden ist dies jedoch ein langer Prozess.

15.2 Facebook Fanpages

Veranlasst durch mehrere gerichtliche Entscheidungen des EuGH und des Bundesverwaltungsgerichts (BVerwG) im Kontext von Facebook-Diensten und zu Fragen gemeinsamer Verantwortlichkeit[306] hatten wir Ende 2018 eine Reihe von Prüfverfahren eingeleitet.[307] Im Laufe dieser Verfahren hat Facebook eine wesentlich überarbeitete Fassung seiner Vereinbarung zur gemeinsamen Verantwortlichkeit mit den Fanpage-Betreiber*innen bereitgestellt.[308] Da diese nicht geeignet war, alle bisherigen Kritikpunkte und offenen Fragen auszuräumen, haben wir mehrere Verantwortliche abermals um Stellungnahme gebeten. Die Reaktionen fielen gemischt aus.

306 EuGH, Urteil vom 5. Juni 2018 – C-210/16; BVerwG, Urteil vom 11. September 2019 – 6 C 15 18 (Wirtschaftsakademie Schleswig-Holstein); EuGH, Urteil vom 29. Juli 2019 – C-40/17 (Fashion ID)

307 JB 2018, 1.7

308 Siehe https://de-de.facebook.com/legal/terms/page_controller_addendum

Facebook stellt den Betreiber*innen von Fanpages sog. Seiten-Insights bereit. Hierbei handelt es sich um statistische Informationen darüber, ob und wie Besucher*innen der Fanpages mit der Seite und den Inhalten interagiert haben – was also bei bestimmen Gruppen gut ankommt und was weniger. Wie der EuGH 2018 festgestellt hat, verarbeiten Facebook und die Betreiber*innen der Fanpages hierfür die personenbezogenen Daten der Besucher*innen in gemeinsamer Verantwortlichkeit. In der Konsequenz sind beide Akteur*innen nicht nur verpflichtet, in einer Vereinbarung transparent festzulegen, wer hinsichtlich dieser Daten welche Verpflichtungen nach der DS-GVO erfüllt. Es ist auch jede*r der gemeinsam Verantwortlichen selbst in der Verantwortung, die Rechtmäßigkeit der Datenverarbeitungen sicherzustellen und bei Bedarf gegenüber der zuständigen Aufsichtsbehörde nachzuweisen.

Nachdem Facebook den Fanpage-Betreiber*innen Ende 2018 erstmals eine Vereinbarung zur Verantwortlichkeitsverteilung bei den Seiten-Insights zur Verfügung gestellt hat, folgte Ende Oktober 2019 sodann eine wesentlich überarbeitete Fassung dieser Vereinbarung (die sogenannte Seiten-Insights-Ergänzung). Die neue Vereinbarung hat zwar einige der zuvor von den Aufsichtsbehörden geäußerten Kritikpunkte ausräumen können. Wie wir bereits in unserem letzten Jahresbericht angedeutet haben, bleibt die Ergänzung in entscheidenden Punkten jedoch ungenügend.[309] Letztlich werden die Fanpage-Betreiber*innen hierdurch immer noch nicht im erforderlichen Maße in die Lage versetzt, ihrer Rechenschaftspflicht hinsichtlich der Rechtmäßigkeit der Verarbeitung von Daten der Fanpage-Besucher*innen nachzukommen.

Im Februar haben wir daher erneut sechs Stellen der Landesverwaltung, sechs politische Parteien sowie sieben Berliner Unternehmen und Organisationen, u.a. aus der Handels-, Verlags- und Finanzbranche, angeschrieben. Dabei haben wir einerseits Bedenken bzw. Zweifel hinsichtlich bestimmter Bestandteile der Seiten-Insights-Ergänzung geäußert und angeregt, die fraglichen Punkte kritisch mit Facebook zu klären. Andererseits haben wir die konkrete Umsetzung von Informationspflichten auf den jeweiligen Fanpages angemahnt.

309 JB 2019, 13.6

Nachdem bereits in der ersten Anhörungsrunde mehrere der politischen Parteien unter Verweis auf unsere angebliche Unzuständigkeit keine Auskünfte erteilt hatten, war es bedauerlich, aber nicht verwunderlich, dass auch in dieser Runde nur eine von ihnen Stellung zu unseren weiteren Fragen genommen hat. Auch andere nicht öffentliche Stellen haben zwar Zweifel an unserer Zuständigkeit angemerkt, sie haben jedoch alle konstruktiv reagiert und sich inhaltlich eingelassen. Soweit es die Benutzeroberfläche auf Facebook zuließ, haben mehrere Stellen die Gelegenheit genutzt, ihre Fanpages transparenter zu gestalten, indem z. B. Informationen zur Datenverarbeitung mit weniger Aufwand verfügbar gemacht wurden. Fast alle Verantwortlichen haben zudem Kontakt zu Facebook aufgenommen. Dies hat u.a. dazu geführt, dass Facebook einen Passus in seinen Informationen zu den Seiten-Insights-Daten korrigiert hat.[310] Ursprünglich hieß es, dass „Du [...] stets das Recht [hast], eine Beschwerde bei der irischen Datenschutzkommission (siehe unter www.dataprotection.ie) oder bei deiner lokalen Aufsichtsbehörde einzureichen." Da betroffene Personen das Recht haben, sich bei jeder beliebigen Aufsichtsbehörde zu beschweren (d. h. nicht lediglich der irischen und der des eigenen Mitgliedsstaates), war diese Information anzupassen. Auf unsere übrigen Bedenken wurde demgegenüber kaum eingegangen, sodass wir die Verfahren nach wie vor nicht abschließen können.

Die Senatskanzlei, die stellvertretend für die meisten angeschriebenen öffentlichen Stellen geantwortet hat, hat sich zunächst mit Rückfragen an uns gewandt. Unser Angebot einer persönlichen Konsultation, das wir zusammen mit unseren Antworten versendet haben, wurde bisher leider nicht angenommen.

Der Fortgang unserer Prüfungsreihe hat zwar in gewissem Umfang zu einer Schärfung des Problembewusstseins bei den Verantwortlichen geführt. Es stehen jedoch nach wie vor ungeklärte Punkte im Raum, sodass die Verfahren von uns weitergeführt werden, bis der legale Betrieb der Facebook-Fanpages sichergestellt ist oder deren Betrieb eingestellt wird.

310 Siehe https://www.facebook.com/legal/terms/information_about_page_insights_data

15.3 Orientierungshilfe: Wie sicher kann und muss E-Mail heute sein?

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit war federführend an der Erarbeitung einer Orientierungshilfe beteiligt, die Maßgaben für die Nutzung von E-Mails zur Übertragung und zum Empfang von personenbezogenen Daten enthält.[311]

E-Mails sind nach wie vor ein nicht wegzudenkendes Instrument für den Austausch von Informationen zwischen Personen und Institutionen. Der Vorteil liegt in der Universalität: Nahezu jede Institution kann per E-Mail angesprochen werden und auch Privatpersonen sind in der überwiegenden Mehrheit per E-Mail erreichbar. Dabei können die Nutzenden verschiedenste Programme zum Lesen und Verfassen der Nachrichten einsetzen. Die eigentliche Arbeit geschieht im Hintergrund. Server nehmen die Nachrichten entgegen und leiten sie – möglicherweise über mehrere Zwischenstationen – an die Empfängerin oder den Empfänger weiter.

Personenbezogene Daten sind auch bei der Übertragung per E-Mail davor zu schützen, dass sie unbefugt zur Kenntnis genommen oder manipuliert werden. Dafür haben sich über die Zeit mehrere Verfahren etabliert.

Weitgehend unsichtbar für die Endnutzer*innen erfolgt die sogenannte Transportverschlüsselung. Die bereits erwähnten Server und Zwischenstationen bauen einen sicheren Kanal für die Datenübermittlung auf. Werden dafür sichere Verfahren eingesetzt[312] und wird kontrolliert, dass die Gegenseite zum Empfang berechtigt und tatsächlich diejenige ist, die sie zu sein vorgibt, dann ist die Vertraulichkeit der Übermittlung gesichert. An den Zwischenstationen allerdings liegen die Nachrichten offen.

311 Orientierungshilfe des Arbeitskreises „Technische und organisatorische Datenschutzfragen": Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, Stand: 13. März 2020; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/orientierungshilfen

312 Das Bundesamt für Sicherheit in der Informationstechnik hat hierzu einen entsprechenden Katalog veröffentlicht.

Anspruchsvoller, aber von durchgreifenderer Wirkung ist die sog. Ende-zu-Ende-Verschlüsselung. Hier findet die Ver- und Entschlüsselung unmittelbar bei den jeweiligen Verantwortlichen oder den am Austausch beteiligten Personen statt. In der Regel geschieht das in den Programmen, die die Nutzenden zum Versenden und Empfangen der Nachrichten verwenden. Entweder enthalten diese bereits die entsprechende Funktionalität oder es werden passende Erweiterungen für die Programme genutzt. Verantwortliche können jedoch auch zentral betriebene Informationstechnik einsetzen, um die Ver- und Entschlüsselung sowie die Erstellung und Prüfung von Signaturen vorzunehmen. Diese Signaturen dienen dem Schutz der Integrität[313] der Nachrichteninhalte.

Für technisch nicht versierte Privatpersonen ist allerdings die Verwendung einer der beiden verfügbaren Techniken der Ende-zu-Ende-Verschlüsselung nicht einfach. Denn zu jeder Verschlüsselung und zu jeder Signatur gehören kryptografische Schlüssel. Dabei müssen eigene Schlüssel erzeugt und verwaltet, fremde Schlüssel müssen übernommen und überprüft werden. Von Verantwortlichen, insbesondere solchen, die mit sensitiven Daten umgehen, ist zu verlangen, dass sie sich dieser Mühe unterziehen. Von Privatpersonen, die keine Verantwortlichen im Sinne der DS-GVO sind, kann das nicht erwartet werden.

Um den Verantwortlichen die Entscheidung zu erleichtern, welche Sicherheitsmaßnahmen zum Schutz von E-Mail-Nachrichten in ihrem Verantwortungsbereich zu treffen sind, hat die DSK unter unserer Federführung eine Orientierungshilfe verfasst.

Die Orientierungshilfe klärt die Sorgfaltspflichten bei der Inanspruchnahme von E-Mail-Dienstleistern und die von diesen einzuhaltenden Richtlinien. Sie legt dar, welche Voraussetzungen Verantwortliche für den sicheren Empfang von E-Mail-Nachrichten schaffen müssen, um gezielt personenbezogene Daten per E-Mail entgegennehmen zu können. Denn die Sicherheit der Übertragung hängt sowohl von der sendenden als auch von der empfangenden Person oder Stelle ab,

313 Unter der Wahrung der Integrität von Daten versteht man ihren Schutz vor unbefugter Veränderung oder Entfernung, vor unbeabsichtigtem Verlust oder Zerstörung und vor unbeabsichtigter Verfälschung; siehe Art. 5 Abs. 1 lit. f DS-GVO.

auch wenn die Verantwortung für die einzelne Übermittlung bei der sendenden Person oder Stelle liegt.

Verantwortliche, die E-Mails versenden bzw. die E-Mail-Dienstleister, die für sie handeln, müssen eine Transportverschlüsselung vornehmen. Wichtig ist dabei zu wissen, dass gängige Software regelmäßig eine unverschlüsselte Verbindung aufbaut, wenn keine verschlüsselte Verbindung zustande kommt. Das ist bei der Übermittlung personenbezogener Daten im Inhalt einer E-Mail-Nachricht nicht zulässig. Auf der anderen Seite hält die Orientierungshilfe auch fest, dass die Transportverschlüsselung bei normalem Schutzbedarf der Daten ausreicht und eine Ende-zu-Ende-Verschlüsselung nicht generell verlangt wird.

Bei hohen Risiken muss die Transportverschlüsselung besonderen Anforderungen genügen, die in der Orientierungshilfe beschrieben werden. Grundsätzlich ist dabei zusätzlich eine Ende-zu-Ende-Verschlüsselung erforderlich. Von den Umständen des Einzelfalls, insbesondere von den bestehenden Risiken, der konkreten Ausgestaltung des Übertragungswegs und ggf. getroffenen kompensierenden Maßnahmen hängt es ab, inwieweit von diesen Maßgaben abgewichen werden darf.

Unterliegen die Kommunikationsinhalte besonderen Geheimhaltungsvorschriften, so müssen diese auch bei dem Versand von E-Mail-Nachrichten eingehalten werden. Insbesondere muss die versendende Person sicherstellen, dass nur befugte Empfänger*innen die Inhalte zur Kenntnis nehmen können. Dies setzt regelmäßig eine Ende-zu-Ende-Verschlüsselung voraus.

Die Orientierungshilfe schließt mit näheren Ausführungen zu Anforderungen an die einzelnen Verfahren.

Über die Maßgaben der Orientierungshilfe hinaus raten wir Verantwortlichen, die direkt mit ihren Kund*innen kommunizieren und dabei sensitive Inhalte übermitteln, auf E-Mail als Übertragungsweg zu verzichten und alternative Wege – die Bereitstellung von Informationen über ein sicheres Webportal zum Beispiel – zu wählen.

Verantwortliche müssen auch bei Versand und Empfang von E-Mail-Nachrichten die Sicherheit der personenbezogenen Daten wahren. Die Orientierungshilfe der DSK stellt die hierbei geltenden Maßgaben zusammen.

15.4 Hinweise zum Einsatz von Google Analytics verabschiedet

In Ergänzung zu der 2019 verabschiedeten Orientierungshilfe für Anbieter*innen von Telemedien hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) im Mai Hinweise zum Einsatz von Google Analytics auf Webseiten privater Anbieter veröffentlicht.[314] Hierdurch wurden frühere Hinweise des Hamburgischen Beauftragten für Datenschutz weiterentwickelt. Dies war erforderlich, da sich sowohl das Produkt als auch der rechtliche Rahmen in der Zwischenzeit verändert haben. Insoweit ist nun eine Klarstellung erfolgt.

Google Analytics ist ein weit verbreitetes Werkzeug für Webseitenbetreiber*innen. Mithilfe dieses Werkzeugs lassen sich umfassende statistische Auswertungen der Webseitennutzung vornehmen. Hierfür wird zunächst das Nutzungsverhalten einzelner Nutzer*innen aufgezeichnet. Aus den Einzelaufzeichnungen werden dann statistische Daten errechnet, die den Webseitenbetreiber*innen zur Verfügung gestellt werden.

Neben diesen statistischen Auswertungen für die Webseitenbetreiberin oder den Webseitenbetreiber behält sich Google in seinen Nutzungsbedingungen jedoch auch vor, durch das Werkzeug gesammelte Informationen über das Nutzungsverhalten einzelner Personen auch für eigene Zwecke zu verarbeiten.[315] Google ist damit nicht ausschließlich im Auftrag der einsetzenden Webseitenbetreiber*innen tätig. Unter Berücksichtigung der aktuellen Rechtsprechung des EuGH sind Webseitenbetreiber*innen, die Google Analytics einsetzen, dadurch gemeinsam

314 Siehe https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

315 https://marketingplatform.google.com/about/analytics/terms/de/; abgerufen am 4. Dezember 2020, Ziff. 6.

mit Google für die damit verbundene Datenverarbeitung verantwortlich. Über die Einzelheiten der gemeinsamen Verantwortung ist eine gesonderte Vereinbarung zu schließen.[316]

Die Verarbeitung personenbeziehbarer Daten über die statistischen Auswertungen für Webseitenbetreiber*innen hinaus macht es erforderlich, dass Nutzer*innen einwilligen, bevor Informationen über ihr Nutzungsverhalten mittels Google Analytics erhoben und verarbeitet werden. Diese Einwilligung muss jede Webseitenbetreiberin und jeder Webseitenbetreiber, die oder der Google Analytics nutzt, von jeder Besucherin und jedem Besucher der Webseite einholen. Darauf hatten wir gemeinsam mit anderen deutschen Aufsichtsbehörden bereits am 14. November 2019 in einer Pressemitteilung hingewiesen.[317] Das nunmehr verabschiedete Papier enthält zudem einige Hinweise zur Gestaltung einer wirksamen diesbezüglichen Einwilligung.

Solange Google sich vorbehält, personenbezogene Daten aus dem Einsatz von Google Analytics zu eigenen Zwecken zu verarbeiten, müssen Webseitenbetreiber*innen hierfür eine Einwilligung von den Nutzer*innen einholen.

15.5 Veröffentlichung von Postadressen und Telefonnummern im Internet

Aus der Praxis

Ein Unternehmen veröffentlichte im Internet Postadressen und Telefonnummern von Privatpersonen aus verschiedenen Ländern auf mehreren länderspezifischen Webseiten. Für einige dieser Angebote war als Sitz des Unternehmens eine Postadresse in Berlin angegeben. Unsere Dienststelle erreichten daraufhin zahlreiche Beschwerden betroffener Personen aus verschiedenen Ländern Europas.

Die Beschwerdeführer*innen rügten, dass ihre personenbezogenen Daten dort ohne ihre Einwilligung veröffentlicht worden waren und dass sie im Übrigen auch

316 Art. 26 DS-GVO

317 Siehe https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen

nicht (oder jedenfalls nicht mehr) in sonstigen Telekommunikationsverzeichnissen ihrer Heimatländer eingetragen waren.

Unsere Ermittlungen ergaben, dass das Unternehmen an der im Impressum angegebenen Adresse keine Niederlassung unterhielt. Dort wurde lediglich durch einen Büroservice Post für das Unternehmen entgegengenommen und an dessen tatsächlichen Sitz in Toronto (Kanada) weitergeleitet.

Wir haben daraufhin die in Kanada örtlich zuständige Aufsichtsbehörde für den Datenschutz – Office of the Privacy Commissioner of Canada (OPC) – eingeschaltet. Das OPC führte zu diesem Zeitpunkt bereits eine Untersuchung der Praktiken des Unternehmens nach dem dortigen Datenschutzrecht aufgrund von Beschwerden betroffener Personen durch, die sich direkt an sie gewandt hatten.

Nach deutschem und europäischem Telekommunikationsrecht können die betroffenen Personen selbst darüber bestimmen, ob und in welchem Umfang ihre Adressdaten und/oder Telefonnummern in Teilnehmer*innenverzeichnissen veröffentlicht werden. Eine Veröffentlichung dieser Daten durch Dritte ohne Einwilligung der betroffenen Personen kommt nach den Bestimmungen der DS-GVO allenfalls und auch nur in dem Umfang in Betracht, in dem diese Daten bereits anderswo rechtmäßig öffentlich zugänglich sind.

Die kanadische Datenschutzbehörde hat uns angeboten, unabhängig von den dort laufenden Untersuchungen eine Löschung einzelner Datensätze betroffener Personen bei dem Unternehmen zu erwirken, wenn diese nicht (oder nicht mehr) in Telefonverzeichnissen anderer Anbieter verzeichnet sind. Wir haben die betroffenen Personen um ihre Einwilligung in die Übermittlung ihrer Daten an die kanadische Datenschutzbehörde gebeten und die Daten derjenigen Beschwerdeführer*innen dorthin übermittelt, die diese Einwilligung erteilt haben. Die Daten dieser betroffenen Personen wurden daraufhin aus dem Angebot des Unternehmens entfernt.

Nach Abschluss der dortigen Untersuchung hat uns das OPC darüber informiert, dass es das Unternehmen angewiesen habe, auch die Daten anderer betroffener Personen, die ebenfalls nicht in anderen Telefonverzeichnissen veröffentlicht waren, aus seinen Angeboten zu löschen und, wo dies nicht möglich war, den Daten-

bestand für das gesamte Land zu entfernen. Das Unternehmen hat daraufhin einige seiner länderspezifischen Webseiten aus dem Internet entfernt. Dazu zählten auch die Angebote für die Herkunftsländer derjenigen betroffenen Personen, die Beschwerden bei uns eingereicht hatten.

Eine Veröffentlichung von Adressdaten und/oder Telefonnummern in Teilnehmer*innenverzeichnissen darf grundsätzlich nur mit Einwilligung der Betroffenen erfolgen. Eine Ausnahme kann in Betracht kommen, wenn diese Daten bereits anderweitig rechtmäßig öffentlich zugänglich sind. Die Durchsetzung der Rechte betroffener Personen – wie hier deren Recht auf Löschung gemäß Art. 17 DS-GVO – gegenüber Verantwortlichen mit Sitz außerhalb der Europäischen Union wird wesentlich erleichtert, wenn in dem jeweiligen Sitzland ein vergleichbarer Rechtsrahmen existiert sowie eine Aufsichtsbehörde, die diesen unmittelbar vor Ort durchsetzen kann.

15.6 Befreiung vom Rundfunkbeitrag auch mit geschwärzten Bescheiden

Aus der Praxis

Empfängerinnen und Empfänger von Sozialleistungen können unter bestimmten Voraussetzungen von der Zahlung des Rundfunkbeitrags befreit werden. Sie müssen dazu beim „ARD ZDF Deutschlandradio Beitragsservice" („Zentraler Beitragsservice" – ZBS) den Bezug der Sozialleistung nachweisen. Eine betroffene Person hatte dazu eine teilweise geschwärzte Kopie des Bescheids des Sozialleistungsträgers dorthin geschickt. Der ZBS bestand jedoch für die Bewilligung der Befreiung auf der Zusendung einer ungeschwärzten Kopie des Bescheids.

Wir haben den insoweit zuständigen Rundfunk Berlin–Brandenburg (rbb) zu dem Sachverhalt um Stellungnahme gebeten. Daraufhin veranlasste die behördliche Datenschutzbeauftragte des rbb eine Neubewertung des Antrags der betroffenen Person durch den ZBS. Nach nochmaliger Prüfung hat dieser dem Antrag schließlich auf der Grundlage der ursprünglich vom Beschwerdeführer übersandten Kopie entsprochen, da die für die Befreiung maßgeblichen Angaben auch auf dieser geschwärzten Kopie des Bescheids enthalten waren.

Darüber hinaus hat der ZBS in seinem Internet-Angebot Hinweise veröffentlicht, aus denen hervorgeht, welche Angaben sich aus den Nachweisen für die Befreiung vom Rundfunkbeitrag wie z. B. Bescheinigungen von Behörden oder Bewilligungsbescheiden ergeben müssen. Dies sind der Name der Leistungsempfängerin oder des Leistungsempfängers, Angaben dazu, welche Leistung gewährt wird, und der Leistungszeitraum.[318]

Auch bei der Übersendung von Nachweisen über den Bezug von Sozialleistungen für die Befreiung vom Rundfunkbeitrag ist der Umfang der erhobenen Daten auf diejenigen Daten zu beschränken, die für die Entscheidung über die Befreiung erforderlich sind. Darüber hinausgehende Daten können von den betroffenen Personen geschwärzt werden.

15.7 Löschung personenbezogener Daten in Einzeldokumenten beim Rundfunk Berlin–Brandenburg

Unaufgefordert übersandte eine betroffene Person dem Rundfunk Berlin-Brandenburg (rbb) zusammen mit einem Auskunftsantrag eine Kopie ihres Personalausweises mit dem Hinweis, der rbb möge diese Kopie nach erfolgter Identitätsprüfung unverzüglich löschen. Im Rahmen der Auskunftserteilung an die betroffene Person stellte sich allerdings heraus, dass die Ausweiskopie zusammen mit dem Antrag auf Auskunft beim Zentralen Beitragsservice (ZBS) dauerhaft gespeichert worden war. Einen Antrag auf deren Löschung lehnte der rbb gegenüber der betroffenen Person ab.

In seiner Stellungnahme lehnte der rbb zunächst auch unserer Behörde gegenüber eine Löschung der Kopie des Personalausweises ab, weil dem Aufbewahrungsfristen entgegenstünden und zudem eine Löschung einzelner Seiten aus dem Vorgangsverwaltungssystem technisch nicht möglich sei, ohne das gesamte Eingangsdokument (den Auskunftsantrag) und das Ausgangsdokument (das Aus-

318 Siehe https://www.rundfunkbeitrag.de/buergerinnen_und_buerger/informationen/empfaenger_von_sozialleistungen/index_ger.html

kunftsschreiben) mit zu löschen. Im Übrigen sei dies mit unverhältnismäßigem Aufwand verbunden.

Bereits die dauerhafte Speicherung der Personalausweiskopie über die Identitätsprüfung hinaus war jedoch rechtswidrig. Schon deswegen wäre der rbb von sich aus und erst recht auf den Antrag der betroffenen Person hin zur Löschung der Personalausweiskopie verpflichtet gewesen.[319] Ein Anspruch auf Löschung ergab sich im vorliegenden Fall auch daraus, dass eine weitere Speicherung der Personalausweiskopie nach Beendigung der Identitätsprüfung nicht mehr erforderlich war.[320] Die von der betroffenen Person eingesandte Personalausweiskopie unterliegt keinen gesetzlichen Aufbewahrungsfristen.

Auch der Einwand des rbb, eine Löschung einzelner Teile eines einmal eingescannten Dokuments sei technisch nicht möglich, entbindet ihn nicht von der gesetzlichen Verpflichtung zur Löschung: Der rbb ist vielmehr verpflichtet, die technischen und organisatorischen Voraussetzungen dafür zu schaffen, seinen gesetzlichen Verpflichtungen zur Löschung personenbezogener Daten nachkommen zu können.[321]

Unsere datenschutzrechtliche Bewertung haben wir dem rbb mitgeteilt. Dieser hat daraufhin ein Verfahren entwickelt, mit dem auch einzelne Seiten einmal gescannter Unterlagen aus dem dortigen Datenbestand gelöscht werden können. Die Löschung der Personalausweiskopie wurde – wie ursprünglich beantragt – umgesetzt und der betroffenen Person bestätigt.

Anträge auf Auskunft über personenbezogene Daten nach Art. 15 DS-GVO sollten grundsätzlich ohne Vorlage einer Kopie des Personalausweises gestellt werden, da Ausweiskopien regelmäßig nicht erforderlich sind. Eine Verpflichtung zur Löschung von Daten kann auch für einzelne Teile gespeicherter Unterlagen bestehen. Verantwortliche sind verpflichtet, die technischen Voraussetzungen dafür zu schaffen, dass sie ihren gesetzlichen Verpflichtungen zur Löschung dieser Daten nachkommen können. Dies gilt nicht nur für die hier in

319 Siehe Art. 17 Abs. 1 lit. d DS-GVO
320 Siehe Art. 17 Abs. 1 lit. a DS-GVO
321 Siehe Art. 24 Abs. 1 DS-GVO

Rede stehende Löschung im Einzelfall, sondern auch für eine regelmäßige automatische Löschung nach Ablauf von Aufbewahrungsfristen. Mängel der eingesetzten Software können keine „Datenfriedhöfe“ rechtfertigen.

16 Politische Parteien und Gesellschaft

16.1 Auskunft über Bewertungsbögen für Stipendienbewerber*innen

Aus der Praxis

Der Umfang der Auskunft über personenbezogene Daten, die eine verantwortliche Stelle auf Anfrage erteilen muss, ist regelmäßig Gegenstand von Beschwerden und Entscheidungen. Im konkreten Fall hatte sich der Beschwerdeführer bei einem Begabtenförderungswerk um ein aus öffentlichen Geldern finanziertes Stipendium beworben. Im Laufe des Auswahlverfahrens wurde ein Bewertungsbogen erstellt, in dem verschiedene Kompetenzen des Beschwerdeführers bewertetet wurden. Dieser Bogen stellte die Grundlage der Entscheidung über die Aufnahme des Beschwerdeführers in die Studienförderung dar. Nach Abschluss des Auswahlverfahrens bat der Bewerber den Träger des Förderungswerks um Auskunft über die dort über ihn gespeicherten Daten, insbesondere auch um eine Kopie des Bewertungsbogens. Der Träger verweigerte die Offenlegung des Bewertungsbogens und berief sich auf das Urheberrecht der Mitglieder der Auswahlkommission und den Schutz von Geschäftsgeheimnissen.

Das Recht auf Auskunft umfasst grundsätzlich alle personenbezogenen Daten, die die verantwortliche Stelle zu der jeweils betroffenen Person gespeichert hat.[322] Personenbezogene Daten sind dabei nicht nur objektive Angaben wie Name, Adresse, Alter etc., sondern alle Informationen zu einer Person. Diese umfassen auch subjektive und/oder objektive Einschätzungen. Auch Zeugnisse, Beurteilungen oder Gutachten über Personen enthalten personenbezogene Daten, über die eine verantwortliche Stelle Auskunft erteilen muss.

Das Recht auf Erhalt einer Kopie solcher Dokumente ist nur eingeschränkt, soweit dadurch Informationen offengelegt würden, die ihrerseits gesetzlich besonders vor Offenlegung geschützt sind, z. B. Geschäftsgeheimnisse oder Informationen

322 Art. 15 Abs. 1 DS-GVO

über dritte Personen. In diesem Fall muss das Auskunftsinteresse der betroffenen Person mit dem jeweiligen Geheimhaltungsinteresse abgewogen werden. Aber selbst wenn das Geheimhaltungsinteresse im konkreten Fall überwiegt, darf die verantwortliche Stelle die Herausgabe der Kopie nicht pauschal verweigern, sondern muss die betreffenden Passagen ggf. schwärzen.

Die verantwortliche Stelle hat hier geltend gemacht, das dem Bewertungsbogen zugrundeliegende Formular beinhalte geschützte Geschäftsgeheimnisse. Geschäftsgeheimnisse sind zwar nach dem Geschäftsgeheimnisgesetz(GeschGehG) grundsätzlich vor Offenlegung geschützt. Dies setzt jedoch u.a. voraus, dass es sich dabei um Informationen handelt, die weder allgemein bekannt noch ohne Weiteres zugänglich sind und zusätzlich von wirtschaftlichem Wert. Dies konnten wir bei dem verwendeten Formular jedoch nicht feststellen.

Darüber hinaus hat die verantwortliche Stelle geltend gemacht, dass durch die Auskunft das Urheberrecht der Personen, die den Bewertungsbogen erstellt haben, verletzt würde. Hier ergab die Abwägung der Rechte jedoch, dass das Urheberrecht, so es denn überhaupt bestehen sollte, allenfalls minimal beeinträchtigt wäre. Denn der Bewertungsbogen sollte nur an die betroffene Person herausgegeben und nicht etwa veröffentlicht oder gar wirtschaftlich verwertet werden. In diesem Fall überwiegt das Auskunftsinteresse der betroffenen Person ein möglicherweise bestehendes Urheberrecht der Mitglieder der Auswahlkommission.

Das Förderwerk hat inzwischen die gewünschte Auskunft erteilt.

Bewertungen und Beurteilungen von Bewerber*innen, die zum Zwecke von Auswahlverfahren erstellt werden, stellen personenbezogene Daten dar. Über sie ist auf Anfrage der Betroffenen Auskunft zu erteilen. Diese Auskunft kann nur eingeschränkt werden, wenn dadurch Informationen offengelegt werden, die ihrerseits gesetzlich vor Offenlegung geschützt sind.

16.2 Begabtenförderung nur mit sensitiven Angaben?

In einem Fall hatten wir darüber zu entscheiden, welche Angaben der Träger eines Stipendienprogramms von Bewerber*innen verpflichtend verlangen darf. Der Träger verwendete ein Online-Formular, über das sich Bewerber*innen registrieren mussten. Dabei mussten sie u.a. zwingend Angaben zu ihrer Religion und zu ihrer Herkunft machen. Die Religionszugehörigkeit war für die Auswahl der Stipendiat*innen nach Angaben des Trägers jedoch kein Aufnahmekriterium.

Sowohl Informationen über die ethnische Herkunft als auch über religiöse Überzeugungen sind neben einigen anderen Datenkategorien in der DS-GVO besonders geschützt.[323] Im Zusammenhang mit ihrer Verarbeitung können erhebliche Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen (z. B. Diskriminierung) auftreten. Deshalb dürfen sie nur unter strengen Voraussetzungen verarbeitet werden.[324]

Diese Voraussetzungen liegen z. B. vor, wenn die betroffene Person in die Verarbeitung dieser Informationen eingewilligt, d. h. ihr freiwillig zugestimmt hat.[325] Freiwillig ist eine solche Zustimmung nur, wenn die betroffene Person u.a. ausreichend darüber informiert ist, wie diese Daten weiterverarbeitet werden. Außerdem muss sie die Möglichkeit haben, die Verarbeitung abzulehnen, ohne dadurch Nachteile zu erleiden. Beim Ausfüllen des Online-Formulars muss die Bewerberin oder der Bewerber selbst entscheiden können, ob sie oder er Angaben zu diesen sensitiven Themen machen möchte oder nicht. Diese Möglichkeit war im vorliegenden Fall nicht gegeben. Es gab daher keine wirksame Einwilligung im Sinne der DS-GVO.

Auch wenn die betroffene Person nicht einwilligt, erlaubt die DS-GVO in einigen Fällen die Verarbeitung sensitiver Daten. In unserem Fall spielte dabei nur folgender Erlaubnistatbestand eine Rolle: Sensitive Daten dürfen von einer politisch,

323 Siehe Art. 9 DS-GVO
324 Siehe Art. 9 Abs. 1 bis 3 DS-GVO
325 Art. 9 Abs. 2 lit. a i. V. m. Art. 4 Nr. 11, Art. 7 DS-GVO

weltanschaulich, religiös oder gewerkschaftlich ausgerichteten Stiftung, Vereinigung oder sonstigen gemeinnützigen Organisation im Rahmen rechtmäßiger interner Tätigkeiten, wie etwa der Mitgliederverwaltung einschließlich der Aufnahme neuer Mitglieder, verarbeitet werden.[326] Der Träger hat argumentiert, dass er auf der Basis eines weltanschaulich-religiös geprägten Weltbildes arbeite und deshalb im hierfür erforderlichen Maße auch Informationen zur Religion seiner Mitglieder verarbeiten dürfe.

In Bezug auf Daten zur ethnischen Herkunft griff diese Begründung von vornherein nicht, denn in ethnischer Hinsicht hatte der Träger keine bestimmte Ausrichtung. Die Verpflichtung zu dieser Angabe war damit unzulässig.

Auch im Hinblick auf die Religionszugehörigkeit war die Erhebung zum Zeitpunkt der ersten Registrierung im vorliegenden Fall nicht erforderlich. Denn der Träger hatte deutlich gemacht, dass eine bestimmte (formale) Religionszugehörigkeit nicht Voraussetzung für die Aufnahme in das Stipendienprogramm ist. Vielmehr wird nach Angaben des Trägers im späteren Bewerbungsgespräch erörtert, ob die Bewerberin oder der Bewerber dem vom Träger vertretenen Menschenbild nahesteht. Hierfür ist es ausreichend, wenn die Bewerber*innen im persönlichen Gespräch nach ihren Ansichten gefragt werden. Insbesondere die Verarbeitung dieser sensitiven Informationen von allen Bewerber*innen, die nicht zum persönlichen Gespräch eingeladen werden, ist daher nicht erforderlich und widerspricht dem Grundsatz der Datenminimierung.

Im Ergebnis war die Erhebung von verpflichtenden Angaben sowohl zur Religion als auch zur ethnischen Herkunft in der Online-Maske rechtswidrig. Wir haben den Träger verwarnt. Dieser hat daraufhin angekündigt, dass er sein Online-Formular entsprechend anpassen wird.

Bei der Gestaltung von Online-Formularen (etwa für Bewerbungsprozesse) müssen die Verantwortlichen darauf achten, dass sie nur die Angaben verpflichtend abfragen, die für den jeweiligen Zweck und zum jeweiligen Zeitpunkt

326 Art. 9 Abs. 2 lit. d DS-GVO

des Verfahrens erforderlich sind. Dies gilt umso mehr, je sensitiver die Angaben sind. Darüber hinaus können die Betroffenen freiwillige Angaben machen. Solche Felder müssen jedoch entsprechend kenntlich gemacht werden.

17 Europa

17.1 Berliner Datenschutz-Anpassungsgesetz EU verabschiedet – Defizite im Bereich der Datenschutzaufsicht bestehen weiter

Über zwei Jahre nach Ablauf der Umsetzungsfrist ist nun endlich das Gesetz zur Anpassung datenschutzrechtlicher Bestimmungen in Berliner Gesetzen an die Datenschutz-Grundverordnung (Berliner Datenschutz-Anpassungsgesetz EU) vom Abgeordnetenhaus verabschiedet worden.[327] Wie bereits in unserem Jahresbericht 2019 berichtet, handelt sich dabei um ein Mammutprojekt, durch das ca. 80 Berliner Gesetze an die europäische Datenschutz-Grundverordnung (DS-GVO) angepasst wurden.[328]

Wir haben das Gesetzgebungsvorhaben intensiv begleitet. Ausgerechnet bei dem wichtigsten datenschutzrechtlichen Regelwerk, dem Berliner Datenschutzgesetz (BlnDSG), bestehen jedoch nach wie vor erhebliche Mängel. Das gilt insbesondere im Bereich der Datenschutzaufsicht und -kontrolle.

Kontrolldefizite bestehen dabei weiterhin u.a. im wichtigen Bereich der Betroffenenrechte. Das Recht auf Auskunft über die zur eigenen Person gespeicherten Daten ist ein grundlegendes Prinzip der DS-GVO. Sollte die Auskunft im Einzelfall verweigert werden dürfen, sollen Bürgerinnen und Bürger grundsätzlich verlangen können, dass entsprechende Auskünfte zumindest gegenüber der zuständigen Datenschutzbehörde erteilt werden. Durch diese ersatzweise Information an die Aufsichtsbehörde und die daraus folgende Kontrolle soll sichergestellt werden, dass die Verarbeitung der betreffenden Daten datenschutzgerecht erfolgt. Selbst diese ersatzweise Auskunft kann allerdings nach der nunmehr weiterhin geltenden gesetzlichen Berliner Regelung von der betroffenen Behörde verweigert werden, wenn sie der Auffassung ist, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Eine solche Einschränkung der Betroffenen-

327 Siehe GVBl. 2020, S. 807 ff.
328 JB 2019, 14.1

rechte ist nicht nachvollziehbar, da es sich bei der Datenschutzbehörde um eine unabhängige, oberste Landesbehörde handelt, deren Beschäftigte zur strikten Geheimhaltung der ihnen im Dienst bekannt gewordenen Informationen verpflichtet sind. Nicht nur wird durch diese Regelung eine wichtige Kontrollfunktion der Berliner Datenschutzaufsicht ausgehebelt. Diese Regelung kann zu Fällen führen, in denen Bürger*innen ihr wichtigstes Betroffenenrecht, nämlich das Recht auf Auskunft, gänzlich abgesprochen wird. Diese Einschränkung eines Grundrechts ist rechtsstaatlich höchst bedenklich und insbesondere vor dem Hintergrund der Stärkung der Betroffenenrechte durch die DS-GVO kaum begründbar.

Ein bekanntes Kontrolldefizit im Geschäftsbereich des Abgeordnetenhauses wurde mit dem neuen BlnDSG sogar noch verschärft. Denn obwohl die Datenschutzregelungen für das Berliner Parlament nach wie vor ungeklärt sind, weitet das nun verabschiedete Gesetz die Möglichkeiten weiter aus, auch sensitive personenbezogene Daten an das Abgeordnetenhaus zu übermitteln. Nach der jüngsten Rechtsprechung des Europäischen Gerichtshofs über die Reichweite der Geltung der DS-GVO für die Arbeit des Petitionsausschusses des Hessischen Landtags[329] wird in Deutschland über die unmittelbare Geltung der DS-GVO für die Parlamente diskutiert. Selbst wenn man jedoch davon ausgeht, dass das Parlament nicht unmittelbar den Regelungen der DS-GVO unterliegt, bedürfen derartige personenbezogene Daten wirksamer und verlässlicher Schutzmaßnahmen und Kontrollmechanismen auf der Grundlage nachvollziehbarer Regelungen. Dies wurde zuletzt in Zusammenhang mit dem von der AfD-Fraktion initiierten Projekt „Neutrale Schule" deutlich, das zeigte, dass Organe der Gesetzgebung durchaus sensitive personenbezogene Daten verarbeiten. Betroffene Bürger*innen stehen solchen Initiativen in Berlin bisher ohne Kontrollmöglichkeiten gegenüber. Diesem Zustand muss dringend abgeholfen werden. Auch im Parlament muss ein der DS-GVO entsprechendes Datenschutzniveau sichergestellt werden.

Im Fachausschuss wurde zugesagt, dass im Rahmen einer Evaluierung speziell dieses Gesetzes noch in dieser Wahlperiode über von uns kritisierte Punkte noch einmal gesprochen werden solle.

329 Siehe EuGH, Urteil vom 9. Juli 2020 – C-272/19

Im Bereich der Polizei und Justiz fehlen der Datenschutzaufsicht ebenfalls nach wie vorher wirksame Durchsetzungsbefugnisse. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) kann gegenüber Polizei- und Justizbehörden weiterhin keine verpflichtenden Anordnungen treffen, sondern – wie vor Inkrafttreten der neuen europäischen Regelungen – festgestellte Verstöße nur unverbindlich beanstanden, was dem klaren Wortlaut dieser europarechtlichen Regelungen widerspricht. Dieses Defizit ist sehr gravierend, weil Polizei und Justizbehörden häufig besonders sensitive Daten über Bürger*innen verarbeiten, etwa Daten von Zeug*innen in strafrechtlichen Ermittlungsverfahren.

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

Die in einem Hauruck-Verfahren vollzogene Anpassung der Berliner Gesetze an die DS-GVO hat noch einige und teilweise sehr empfindliche Lücken gelassen. Erfreulicherweise haben die Abgeordneten des für Datenschutz zuständigen Fachausschusses angekündigt, das Berliner Datenschutzgesetz unabhängig von dem Anpassungsgesetz noch in dieser Legislaturperiode zu evaluieren. Wir hoffen, dass die Ankündigung wahr gemacht und die bestehenden Mängel beseitigt werden.

17.2 Aus der Servicestelle Europaangelegenheiten – Fallzahlen, Trends, Schwerpunkte

Die DS-GVO sieht eine enge Kooperation zwischen den europäischen Datenschutzaufsichtsbehörden vor. Dabei geht es vor allem um Fälle, die eine grenzüberschreitende Verarbeitung personenbezogener Daten beinhalten. Die BlnBDI bearbeitet Fälle als federführende Behörde, wenn das datenverarbeitende Unternehmen seinen Hauptsitz in Berlin hat, und übermittelt bei ihr eingegangene Fälle an andere federführende Aufsichtsbehörden, sofern der Hauptsitz des Unternehmens sich in einem anderen Mitgliedsstaat befindet. Dabei fungiert die interne Servicestelle Europaangelegenheiten als Scharnier zwischen den europäischen Datenschutzaufsichtsbehörden und den Fachreferent*innen bei der BlnBDI.

Sowohl alle bei uns eingehenden Beschwerden als auch alle Fälle, die wir von Amts wegen aufgreifen, sowie auch die von Unternehmen gemeldeten Datenpannen werden von uns zunächst daraufhin geprüft, ob die beanstandete Verarbeitung personenbezogener Daten grenzüberschreitend stattfindet. Dies ist vor allem dann der Fall, wenn die oder der Verantwortliche in mehr als einem Mitgliedsstaat der EU niedergelassen ist und die Verarbeitung in mehreren dieser Niederlassungen erfolgt. Jedoch kann auch bereits dann eine grenzüberschreitende Verarbeitung vorliegen, wenn die Verarbeitung zwar nur in einem Mitgliedsstaat der EU stattfindet, sie aber erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedsstaat hat oder haben kann.

Waren im vergangenen Jahr insbesondere Verfahren zur Bestimmung der federführenden Aufsichtsbehörde ein Schwerpunkt der Arbeit der Servicestelle Europaangelegenheiten, konnten wir im Jahr 2020 auf dieser Grundlage vermehrt Beschwerden an die nun als zuständig befundenen europäischen Aufsichtsbehörden übermitteln oder als federführende Behörde selbst bearbeiten. So haben wir zu einer Vielzahl der zwischen den europäischen Aufsichtsbehörden abstimmungsbedürftigen Fällen Stellung bezogen. Dies geschah zum einen dadurch, dass wir in Beschlussentwürfen die eigenen Ermittlungsergebnisse zur Abstimmung gestellt haben und diese durch endgültige Beschlüsse abschließen konnten. Zum anderen haben wir gegen die Beschlussentwürfe und damit gegen die Ermitt-

lungsergebnisse anderer Aufsichtsbehörden bei Bedarf Einspruch eingelegt und auf diese Weise inhaltliche Aspekte in das Verfahren eingebracht, die teilweise in den überarbeiteten Beschlussentwürfen und in den endgültigen Beschlüssen berücksichtigt wurden.

17.2.1 Bestimmung der federführenden Aufsichtsbehörde

Wird eine grenzüberschreitende Verarbeitung vermutet, dann wird der Fall den anderen europäischen Datenschutzaufsichtsbehörden über das digitale Binnenmarkt-Informationssystem (IMI) vorgelegt. Im Rahmen des Kooperationsverfahrens wird eine federführende Aufsichtsbehörde bestimmt, die die Ermittlungen in dem jeweiligen Fall führt. Weitere Datenschutzaufsichtsbehörden können sich als sog. betroffene Behörden melden, wenn sie bspw. davon ausgehen, dass die Verarbeitung erhebliche Auswirkungen auf betroffene Personen in ihrem Land hat.

Im IMI wurden in diesem Jahr rund 741 Verfahren zur Bestimmung der federführenden und der betroffenen Aufsichtsbehörden gemeldet. Sämtliche Verfahren wurden in der Servicestelle Europaangelegenheiten auf eine mögliche Betroffenheit bzw. Federführung der BlnBDI geprüft. In 388 Verfahren, also etwas mehr als der Hälfte der Verfahren, wurde eine Betroffenheit unserer Behörde festgestellt, sodass wir uns inhaltlich mit den jeweiligen Sachverhalten befassen mussten. Eine solche Betroffenheit ist schnell gegeben: Richtet etwa ein Online-Shop sein Angebot auch an die deutsche Kundschaft, dann müssen wir davon ausgehen, dass auch Bürger*innen in Berlin von dem Sachverhalt betroffen sein können, sodass wir uns in den Fall einschalten.

In diesem Jahr eröffnete die BlnBDI 29 neue Fälle, in denen sie als federführende Aufsichtsbehörde tätig ist. Davon sind uns zehn Fälle von anderen europäischen Aufsichtsbehörden übermittelt worden.

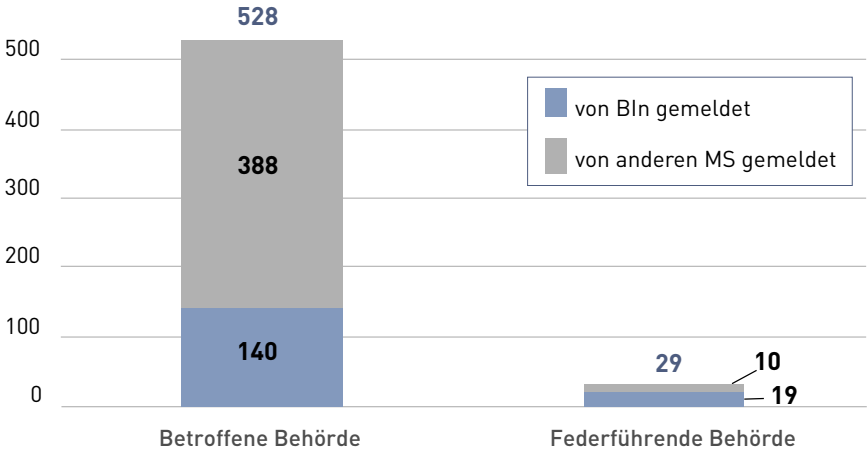

Abbildung 1: Von der BlnBDI im Berichtszeitraum geprüfte Fälle, die im IMI eingestellt wurden.

Nicht in allen Fällen verläuft die Bestimmung der federführenden Aufsichtsbehörde reibungslos. So haben wir nach der Verlagerung der Hauptniederlassung eines Verantwortlichen in einen weiteren EU-Mitgliedsstaat zusammen mit der insoweit zuständigen anderen europäischen Aufsichtsbehörde eine Vor-Ort-Prüfung in beiden Mitgliedsstaaten durchgeführt. In diesem Fall wird derzeit noch ermittelt, ob die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung tatsächlich in einer europäischen Niederlassung oder in einem Drittland getroffen werden. Sollten diese Entscheidungen nicht in einer Hauptniederlassung im Europäischen Wirtschaftsraum (EWR) getroffen und umgesetzt werden, wäre das Privileg des One-Stop-Shops nicht anwendbar. Folglich gäbe es keine federführende Aufsichtsbehörde, die als einzige Ansprechpartnerin der oder des Verantwortlichen zuständig wäre.[330] Stattdessen wäre dann eine Zuständigkeit für das Unternehmen bei jeder europäischen Aufsichtsbehörde mit entsprechenden Fällen gegeben.

330 Siehe Art. 56 Abs. 6 DS-GVO

17.2.2 Übermittlung von Fällen und Beschlussentwürfen

Wie bereits erwähnt, ist die Zahl an Verfahren zur Bestimmung der federführenden und betroffenen Aufsichtsbehörden leicht rückläufig, da die Zuständigkeit für viele große Unternehmen mittlerweile feststeht. Stattdessen können in den Fällen, in denen wir nicht federführende Behörde sind, viele Beschwerden direkt ins Englische übersetzt und dann zügig an die federführende Aufsichtsbehörde zur weiteren Bearbeitung übermittelt werden. Das hat für die Beschwerdeführer*innen auch den positiven Effekt, dass sich die Bearbeitungszeit ihrer Eingaben verkürzt. Insgesamt hat die Servicestelle Europaangelegenheiten 140 Fälle an andere Aufsichtsbehörden übermittelt. Auch in diesen Fällen bleiben wir jedoch Ansprechpartnerin für die Beschwerdeführer*innen und informieren diese regelmäßig über den Stand der Bearbeitung.

Wenn eine federführende Aufsichtsbehörde ihre Untersuchungen abgeschlossen hat, legt sie den betroffenen Aufsichtsbehörden einen Beschlussentwurf zur Abstimmung im IMI vor. Da im zweiten Jahr nach Wirksamwerden der DS-GVO immer mehr Fälle durch verfahrensbeendende Maßnahmen abgeschlossen werden konnten, ist die Zahl der Beschlussentwürfe im Berichtszeitraum deutlich gestiegen. Dies ist insbesondere vor dem Hintergrund der Corona-Pandemie beachtlich, da diese in vielen Mitgliedsstaaten zu teils signifikanten Einschränkungen der Behördentätigkeiten geführt hat.

Die Servicestelle Europangelegenheiten prüft alle Beschlussentwürfe zu Fällen, bei denen die BlnBDI sich als betroffene Aufsichtsbehörde gemeldet hat. Das Kooperationsverfahren der DS-GVO sieht vor, dass betroffene Aufsichtsbehörden gegen Beschlussentwürfe einen Einspruch einlegen können, wenn sie inhaltlich mit ihnen nicht einverstanden sind. Die BlnBDI hat bereits in mehreren Fällen Gebrauch von dieser Möglichkeit gemacht und Einsprüche gegen Beschlussentwürfe anderer Aufsichtsbehörden eingelegt. Infolge eines solchen Einspruchs muss die federführende Behörde den Beschlussentwurf bspw. im Hinblick auf eine fehlerhafte Auslegung des Sachverhalts, eine fehlende Maßnahme nach der Feststellung eines Datenschutzverstoßes oder eine fehlerhafte verfahrensrechtliche Einstellung des Verfahrens überarbeiten.

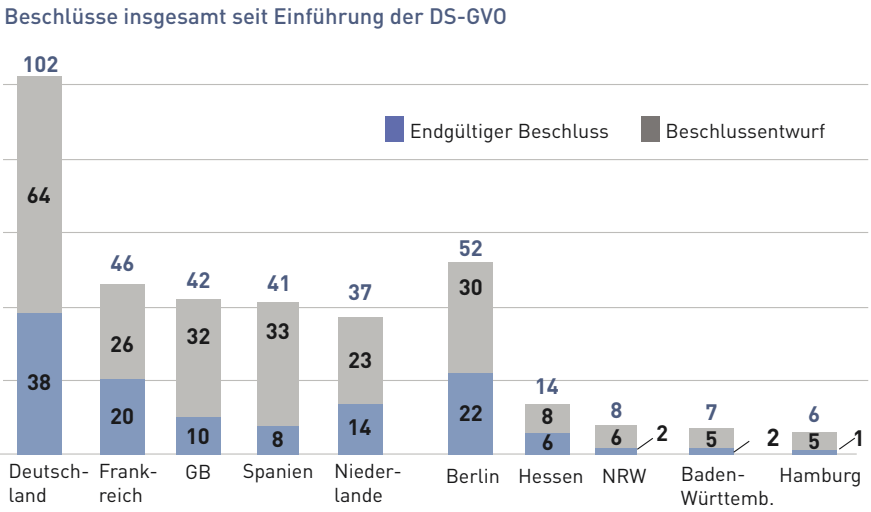

Abbildung 2: Gesamtzahl aller Beschlussentwürfe und endgültigen Beschlüsse der fünf Aufsichtsbehörden in EWR-Mitgliedsstaaten bzw. Bundesländern mit den meisten Beschlüssen seit Einführung der DS-GVO

In den uns betreffenden Fällen sind wir häufig mit den jeweiligen europäischen Partnerbehörden in den direkten Austausch getreten, um zu einer von beiden Behörden getragenen Beschlussfassung zu gelangen. In diesem Zusammenhang treffen zuweilen unterschiedliche Rechtsauffassungen aufeinander, die häufig in den unterschiedlichen Rechtstraditionen begründet sind und dann im Sinne einer Kompromisslösung nach Möglichkeit austariert werden – so geht die Angleichung der unterschiedlichen Rechtssysteme im Bereich des Datenschutzes im beruflichen Alltag vor sich. Anhand der Einsprüche gegen Beschlussentwürfe, im Zuge der Überarbeitung dieser Beschlussentwürfe und durch die Auslegung und Anwendung der DS-GVO im konkreten Fall zeigt sich die gemeinsame Arbeit aller europäischer Aufsichtsbehörden als ein konstruktives Ringen um die Vereinheitlichung des Datenschutzniveaus in der EU.

Stimmen alle betroffenen Aufsichtsbehörden einem überarbeiteten Beschlussentwurf zu, so kann die federführende Aufsichtsbehörde einen endgültigen Beschlussentwurf veröffentlichen, dessen Ergebnis auch den Beschwerdeführenden und den Verantwortlichen mitgeteilt wird.

Insgesamt hat sich die Arbeit der Servicestelle Europaangelegenheiten von Zuständigkeitsfragen stärker auf die inhaltliche Abstimmung bei der Bearbeitung von Beschwerden und der Festlegung von Maßnahmen im Hinblick auf die festgestellten Datenschutzverstöße verlagert. Wir haben in mehreren Fällen Einspruch eingelegt, in denen die federführende Aufsichtsbehörde trotz festgestelltem Datenschutzverstoß keine Abhilfemaßnahme gegen den Verantwortlichen ergreifen wollte. Denn nach den Regeln der DS-GVO müssen im Falle festgestellter Datenschutzverstöße wirksame Maßnahmen ergriffen werden. Ein Nichthandeln sieht die DS-GVO nicht vor. Dies ist für Aufsichtsbehörden teilweise schwer zu akzeptieren, deren nationales Datenschutz- bzw. Verfahrensrecht verstärkt auf verhandlungsorientierte Lösungswege setzt(e).

Soweit wir als federführende Behörde agierten, haben wir Beschlussentwürfe veröffentlicht, gegen die die jeweils betroffenen anderen europäischen Aufsichtsbehörden Einspruch einlegen konnten. Insgesamt veröffentlichte unsere Behörde in diesem Jahr 24 Beschlussentwürfe und 20 endgültige Beschlüsse.

17.3 Datenschutz durch Technikgestaltung – Neue Leitlinien des Europäischen Datenschutzausschusses

Die DS-GVO hat durch die Regelungen des sog. „privacy by design“ und „privacy by default“ die Forderung nach Datenschutz durch Technikgestaltung und das Prinzip datenschutzfreundlicher Voreinstellungen im Gesetz verankert. Wir haben an Leitlinien des Europäischen Datenschutz-Ausschusses (EDSA) mitgewirkt, mit denen die gesetzlichen Anforderungen erläutert werden.

Die DS-GVO schreibt vor, dass durch Technikgestaltung sichergestellt werden soll, dass die Datenschutz-Grundsätze eingehalten werden. Diese Grundsätze erstrecken sich auf die Rechtmäßigkeit und Transparenz der Verarbeitung, ihre Bindung an den Zweck, für den die Daten erhoben wurden, die Minimierung des Umfangs verarbeiteter Daten und die zeitliche Begrenzung ihrer Speicherung sowie die Ge-

währleistung von Richtigkeit, Vertraulichkeit und Integrität[331] der Daten. Die Einhaltung der Grundsätze muss nachgewiesen werden können.

Die technischen und organisatorischen Maßnahmen, die die Verantwortlichen treffen, sollen angemessen und effektiv sein. Die Verantwortlichen sollen und können bei der Auswahl der Maßnahmen eine Reihe von Faktoren in Betracht ziehen. Darunter sind der Stand der Technik, also die wirkungsvollsten auf dem Markt verfügbaren Technologien, die Risiken für die betroffenen Personen, die mit der Verarbeitung einhergehen, aber auch die Implementierungskosten und ganz allgemein Art, Umfang, Umstände und Zwecke der Verarbeitung. Bei alldem ist Effektivität jedoch das Schlüsselkriterium, da nur durch effektive Maßnahmen die Rechte und Freiheiten der betroffenen Personen geschützt werden.

Bereits 2019 hatte der EDSA Leitlinien zur Erläuterung der gesetzlichen Anforderungen an Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen formuliert und die Öffentlichkeit zur Kommentierung des Papiers aufgerufen. Daraufhin wurden mehr als fünfzig Kommentare von Wirtschaft und Zivilgesellschaft eingereicht. In diesem Jahr wurden die Leitlinien auf der Basis der Kommentare substantiell überarbeitet. Wir haben uns daran beteiligt.[332]

Die Leitlinien erläutern jeden der oben aufgeführten Datenschutz-Grundsätze und führen jeweils Schlüsselelemente seiner Umsetzung durch Technikgestaltung auf. Beispiele erhellen die Anwendung dieser Elemente in konkretem Kontext.

Mit Voreinstellungen werden Anwendungen, Programme und Geräte konfiguriert. Die Leitlinien stellen klar, dass diese so gewählt werden sollen, dass nur die erforderlichen personenbezogenen Daten verarbeitet werden. Diese dürfen nur im geringstmöglichen Ausmaß verarbeitet werden, nur so kurz wie möglich gespeichert bleiben und zu jedem Zeitpunkt für so wenig Personen wie möglich zugänglich sein.

331 Unter der Wahrung der Integrität von Daten versteht man ihren Schutz vor unbefugter Veränderung oder Entfernung, vor unbeabsichtigtem Verlust oder Zerstörung und vor unbeabsichtigter Verfälschung; siehe Art. 5 Abs. 1 lit. f DS-GVO.

332 Siehe https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (englische Fassung)

Die Leitlinien betonen, dass Datenschutz durch Technikgestaltung eine kontinuierliche Aufgabe der Verantwortlichen darstellt, die bereits mit der Planung der Datenverarbeitung beginnt. Technologische Fortschritte können sowohl zu zusätzlichen Risiken führen, als auch neue Möglichkeiten eröffnen, bekannte Risiken erfolgreicher zu mindern. Sie sind daher bei der Fortschreibung der Maßnahmen zu berücksichtigen.

Die Anforderungen richten sich an Verantwortliche. Diese sind zugleich dafür verantwortlich, dass auch die Verarbeitungsschritte, die durch Auftragsverarbeiter*innen und Unterauftragnehmer*innen durchgeführt werden, den Maßgaben entsprechen.

Mit den Leitlinien zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gibt der EDSA den Verantwortlichen wichtige Hinweise zur Wahrung der Rechte der betroffenen Personen. Auch Auftragsverarbeitende und Hersteller*innen sind aufgerufen, sich an der Leitlinie zu orientieren, da Verantwortliche nur Dienstleistungen und Produkte in Anspruch nehmen dürfen, die rechtskonform betrieben werden.

17.4 Weitere wichtige Leitlinien des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss (EDSA) setzt sich aus den Datenschutzaufsichtsbehörden der einzelnen EU-Mitgliedsstaaten zusammen. Auch die BlnBDI hat die Aufgabe, Beiträge zur Tätigkeit des EDSA zu leisten und arbeitet dabei eng mit den anderen deutschen Datenschutzaufsichtsbehörden zusammen.[333] Ziel der Arbeit des EDSA ist es, die einheitliche Anwendung der DS-GVO in der EU sicherzustellen. Dazu kann der Ausschuss unter anderem Leitlinien erlassen, die die abstrakten Vorschriften der DS-GVO konkretisieren. Damit soll für Unternehmen und Betroffene, aber auch für die Aufsichtsbehörden selbst die einheitliche Anwendung der DS-GVO erleichtert werden. Der EDSA hat in diesem Jahr

333 § 11 Abs. 1 Satz 1 Ziff. 7 und 11 BlnDSG

eine Rekordzahl von 12 Leitlinien erarbeitet, die im Folgenden kurz vorgestellt werden.[334]

Die Leitlinien befassen sich z. T. mit aktuellen gesellschaftlichen Herausforderungen, die auch einer datenschutzrechtlichen Lösung bedürfen; in diesem Jahr vornehmlich mit datenschutzrechtlichen Fragestellungen der Corona-Pandemie. Dabei ging es vor allem um die Nutzung von Positionsdaten und Anwendungen zur Kontaktnachverfolgung, z. B. im Zusammenhang mit Corona-Warn-Apps,[335] aber auch um die Verarbeitung von Gesundheitsdaten in der Forschung im Zusammenhang mit der Pandemie.[336]

Daneben lag ein Fokus auf aktuellen Phänomenen der Digitalisierung, wie z. B. der Verarbeitung personenbezogener Daten in vernetzten Autos,[337] der Nachverfolgung von Aktivitäten in sozialen Netzwerken[338] und dem Recht auf Vergessen im Zusammenhang mit Internetsuchmaschinen[339]. Außerdem ergab sich aus der sog. Schrems-II-Entscheidung des Europäischen Gerichtshofs die Notwendigkeit, in einer Empfehlung zu konkretisieren, unter welchen Voraussetzungen Datenübertragungen in Drittstaaten auf Standardvertragsklauseln gestützt werden können.[340]

Auch zu einigen "Klassikern" des Datenschutzrechts wurden Leitlinien verfasst, so z. B. zur Videoüberwachung[341] und zum Begriff der Einwilligung[342]. Der Bedarf

334 Bei etwa der Hälfte werden noch die Ergebnisse der Öffentlichkeitsbeteiligung ausgewertet, bevor sie endgültig verabschiedet werden.

335 Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19

336 Leitlinien 3/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch

337 Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

338 Guidelines 08/2020 on the targeting of social media users

339 Leitlinien 5/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gemäß der DSGVO, Teil 1: Version 2.0

340 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

341 Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte; siehe 13.1.

342 Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1

zur Verabschiedung einiger dieser Leitlinien ergab sich teilweise daraus, dass bestimmte Rechtsbegriffe in der DS-GVO anders formuliert sind oder ausgelegt werden als im früheren Datenschutzrecht. Dies betrifft insbesondere die Leitlinien zum Konzept von Verantwortlichen und Auftragsverarbeitenden, die sehr praxisrelevante Aussagen zu dem immer wichtiger gewordenen Rechtsinstitut der gemeinsamen Verantwortung enthalten. Gleiches gilt auch für die Leitlinien zum Datenschutz durch Technikgestaltung.[343]

Darüber hinaus hat sich der Ausschuss noch mit weiteren datenschutzrechtlichen Spezialthemen, wie z. B. dem Drittlandtransfer personenbezogener Daten durch öffentliche Stellen[344] oder dem Verhältnis zwischen der DS-GVO und der 2. Zahlungsdiensterichtlinie[345] befasst.

Von großer praktischer Bedeutung sind schließlich die Leitlinien zum Begriff des maßgeblichen und begründeten Einspruchs.[346] Diese Leitlinien, an denen die BlnBDI als Berichterstatterin beteiligt war, sind für die Zusammenarbeit der europäischen Aufsichtsbehörden von entscheidender Bedeutung, da sie die Grundvoraussetzungen für das Streitbeilegungsverfahren vor dem EDSA regeln. Der EDSA war in diesem Jahr mit dem ersten Streitbeilegungsverfahren in einem Einzelfall befasst,[347] wofür diese Leitlinien eine wichtige Grundlage bildeten.

Alle Leitlinien können auf der Internetseite des EDSA abgerufen werden.[348] Soweit eine deutsche Übersetzung vorliegt, veröffentlichen wir diese auch auf unserer Internetseite.[349]

343 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default; siehe hierzu im Einzelnen 17.3

344 Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies

345 Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR

346 Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679

347 Siehe 17.5

348 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_de

349 https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitlinien

17.5 Erstes Streitbeilegungsverfahren vor dem Europäischen Datenschutzausschuss – Eine verpasste Chance!

Mehr als zwei Jahre nach Wirksamwerden der DS-GVO hat der EDSA seinen ersten verbindlichen Beschluss in einem sog. Kohärenzverfahren erlassen. Ein solches Streitbeilegungsverfahren vor dem Ausschuss wird dann eingeleitet, wenn sich zwei oder mehrere Aufsichtsbehörden in der EU nicht einig sind, wie mit einem bestimmten Fall umzugehen ist. In diesem Fall ging es um eine Datenpanne in der mobilen App des Unternehmens Twitter, die zur Folge hatte, dass nicht zur Veröffentlichung bestimmte personenbezogene Daten zeitweise im Internet frei zugänglich waren. Da dieses Unternehmen seinen Hauptsitz in Irland hat, hatte die irische Aufsichtsbehörde die Aufgabe, den anderen betroffenen Aufsichtsbehörden einen ersten Beschlussentwurf vorzulegen.

Mit dem von der irischen Aufsichtsbehörde vorgelegten Beschlussentwurf war eine Vielzahl europäischer Aufsichtsbehörden nicht einverstanden und legte diverse Einsprüche ein. Da es sich um das erste Streitbeilegungsverfahren handelte, mussten zunächst Leitlinien geschaffen werden, wie im Einzelnen mit derartigen Einsprüchen umzugehen ist.[350] Wir haben uns an der Erstellung der Leitlinien beteiligt und konnten z. B. durchsetzen, dass auch Einsprüche in Bezug auf die Höhe eines Bußgelds möglich sind. Die bundesweite Koordinierung des deutschen Einspruchs oblag der hamburgischen Aufsichtsbehörde, der wir in dem Verfahren zugearbeitet haben. Inhaltlich ging es sowohl um die rechtliche Begründung des Beschlussentwurfs als auch um die Höhe der vorgeschlagenen Geldbuße.

Leider hat es der EDSA aus formalen Gründen weitgehend abgelehnt, sich mit den inhaltlichen Argumenten zur rechtlichen Begründung auseinanderzusetzen. Darunter waren sehr wichtige Fragen, wie z. B. zur Integrität und Vertraulichkeit,[351] zur Verantwortung des Verantwortlichen[352] und zur Datensicherheit[353]. Dies ist auf

350 Guidelines 9/2020 on relevant and reasoned objection under Regulation 2016/679
351 Siehe Art. 5 Abs. 1 lit. f DS-GVO
352 Siehe Art. 24 DS-GVO
353 Siehe Art. 32 DS-GVO

der einen Seite verständlich. Schließlich ist das Streitbeilegungsverfahren strengen Fristen unterworfen und der Ausschuss wollte in seinem ersten Kohärenzverfahren vor allem seine Handlungsfähigkeit beweisen. Auf der anderen Seite kann der Ausschuss mit einem solchen Vorgehen seiner wichtigsten Aufgabe nicht gerecht werden, die einheitliche Anwendung der DS-GVO sicherzustellen. Dazu hätte hier ein wesentlicher Beitrag geleistet werden können, indem über sämtliche aufgeworfenen Rechtsfragen entschieden worden wäre. Daher haben die deutschen Aufsichtsbehörden bei der Abstimmung gegen den Beschluss des EDSA gestimmt. Dieser wurde allerdings mehrheitlich angenommen.

Einziger Lichtblick ist ein Aspekt, den die BlnBDI inhaltlich betreut hat. Bei dem gemeinsamen Einspruch der deutschen Aufsichtsbehörden haben wir insbesondere die Höhe des vorgeschlagenen Bußgelds kritisiert, welches sich nach der Beschlussvorlage ursprünglich im Bereich zwischen 0,005 % und 0,01 % des Jahresumsatzes des betroffenen Unternehmens bewegen sollte. Nach der DS-GVO muss ein Bußgeld jedoch in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein.[354] Ein Bußgeld in einem so niedrigen Bereich ist jedoch für das betreffende Unternehmen kaum spürbar, sodass wir über die hamburgische Aufsichtsbehörde gegen die Höhe Einspruch eingelegt haben. Dieser Teil des Einspruchs hatte Erfolg, sodass die irische Aufsichtsbehörde das Bußgeld neu berechnen muss.

Es bleibt zu hoffen, dass der Ausschuss bei zukünftigen Streitbeilegungsverfahren die Gelegenheit nutzt, zu inhaltlichen Fragen Stellung zu nehmen. Ansonsten kann er seiner Aufgabe, für eine europaweit einheitliche Anwendung der DS-GVO zu sorgen, kaum gerecht werden.

354 Art. 83 Abs. 1 DS-GVO

17.6 Auswirkungen des Brexit auf europäische Kooperationsverfahren

Mit Ende der Übergangsphase zum 31. Dezember 2020 trat Großbritannien aus der Europäischen Union aus. Der Brexit hat erhebliche Auswirkungen auf die Bearbeitung von Beschwerden in der Zusammenarbeit zwischen den europäischen Aufsichtsbehörden (Kooperationsverfahren).

Grundsätzlich werden Beschwerden, denen eine grenzüberschreitende Datenverarbeitung[355] zugrunde liegt, zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden abgestimmt. Das ist dann der Fall, wenn ein Unternehmen mehr als eine Niederlassung in der EU hat oder die Datenverarbeitung (aufgrund der europaweiten Tätigkeit) erhebliche Auswirkungen auf Betroffene in mehreren Mitgliedsstaaten hat. Die federführende Behörde ist die jenes Landes, in dem das Unternehmen seine Haupt- bzw. einzige Niederlassung hat; sie dient als einheitliche Ansprechpartnerin des Unternehmens.[356]

Ab dem 1. Januar 2021 werden Beschwerden, die sich gegen Unternehmen mit der Hauptniederlassung in Großbritannien richten, nicht mehr im sog. One-Stop-Shop-Verfahren zwischen den europäischen Aufsichtsbehörden abgestimmt, sofern diese Unternehmen keine neue Hauptniederlassung innerhalb der EU benannt haben. Das bedeutet, dass ab diesem Zeitpunkt keine Verfahren im IMI, das als Kommunikationsplattform der europäischen Aufsichtsbehörden dient,[357] unter Beteiligung von Großbritannien geführt und abgestimmt werden. Jede Aufsichtsbehörde ist nun selbst für die bei ihr eingereichten Beschwerden zuständig und ermittelt direkt gegenüber dem jeweiligen Unternehmen in Großbritannien. Das Privileg, mit der jeweils federführenden Aufsichtsbehörde eine einheitliche Ansprechpartnerin in Fragen des Datenschutzes zu haben, entfällt für diese Unternehmen ab diesem Zeitpunkt.

Für die Bearbeitung von Beschwerden, die bereits vor dem Brexit bei der BlnBDI eingegangen sind, ist die BlnBDI mit der Aufsichtsbehörde in Großbritannien in

355 Siehe Art. 4 Nr. 23 DS-GVO

356 Für weitere Details zum Kooperationsverfahren siehe auch 17.2

357 Siehe 17.2

Kontakt getreten, um bereits vor dem Stichtag wichtige Informationen zu einer möglichen Verlagerung der Hauptniederlassungen von Unternehmen in die EU zu erlangen. In Absprache mit der Aufsichtsbehörde in Großbritannien haben wir auch die fraglichen Unternehmen in Großbritannien selbst kontaktiert, um zu erfahren, ob diese ihre Hauptniederlassungen in einen anderen Mitgliedsstaat verlagert oder eine Vertretung[358] innerhalb der EU benannt haben. Wir hoffen, dass wir dadurch das drohende Chaos, welches der Brexit auch in diesem Bereich verursacht, zumindest abgemildert haben.

Die BlnBDI war in einer europäischen Arbeitsgruppe zum Themenkomplex des Brexits aktiv, um viele Einzelfragen zu Fällen, in die die Aufsichtsbehörde in Großbritannien bisher eingebunden war, zu klären. Dies gilt einerseits in Fällen, in denen diese als federführende Behörde tätig war und die Bearbeitung der Beschwerden bis zum 31. Dezember 2020 nicht abschließen konnte. Andererseits betrifft dies auch Beschwerden, die von britischen Betroffenen eingereicht und von einer Aufsichtsbehörde in einem anderen Mitgliedsstaat bearbeitet werden. Die im Rahmen des Brexits zu erwartenden Verlagerungen der Hauptniederlassungen von Unternehmen und die damit verbundene Änderung der Zuständigkeit von Aufsichtsbehörden kann dazu führen, dass sich die Bearbeitung von Beschwerden gegen Unternehmen mit Hauptsitz in Großbritannien verzögert.

358 Siehe Art. 27 DS-GVO

18 Informationspflicht bei Datenpannen

18.1 Überblick und Einzelfälle

Nach dem drastischen Anstieg der Meldungen von Datenpannen im Jahr 2019 auf 1.017 Fälle blieb die Anzahl der Meldungen im Berichtszeitraum mit 925 Fällen[359] auf hohem Niveau.

Daraus lässt sich zweierlei ableiten: einerseits die zunehmende Sensibilisierung der Verantwortlichen im Hinblick auf den rechtmäßigen Umgang mit Datenpannen, andererseits aber auch die Tatsache, dass sich insgesamt zu viele Datenpannen ereignen, wobei von einer hohen Dunkelziffer auszugehen ist.

Auffällig waren diesmal die zahlreichen Meldungen von Datenpannen im medizinischen Bereich. Hier ging es z. B. um Fehlversendungen von Diagnoseberichten, Laborbefunden oder Röntgenaufnahmen durch ärztliches Personal, etwa weil eine falsche Faxnummer verwendet wurde. Da es sich bei Gesundheitsdaten um besonders schützenswerte Daten handelt,[360] haben die Verantwortlichen zumeist bereits in der Meldung[361] an uns mitgeteilt, dass die jeweils Betroffenen vorsorglich und unabhängig von einer Rechtspflicht[362] über den Vorfall informiert sowie Maßnahmen zur künftigen Vermeidung solcher Fehler getroffen worden seien. Zu diesen Maßnahmen gehörte z. B. die Einführung des Vier-Augen-Prinzips beim Versendungsvorgang.

Einen Großteil der Meldungen erhielten wir von einem überregional tätigen medizinischen Abrechnungsdienst. Hier ging es überwiegend um die unbefugte Kennt-

359 821 Meldungen im nichtöffentlichen Bereich, 104 Meldungen im öffentlichen Bereich

360 Siehe Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO)

361 Nach Art. 33 Abs. 1 DS-GVO ist die Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden ab Kenntnis des Vorfalls zu informieren.

362 Nach Art. 34 Abs. 1 DS-GVO muss der Verantwortliche die betroffene Person über den Vorfall informieren, wenn mit ihm ein hohes Risiko für ihre Rechte verbunden ist.

nisnahme von Rechnungen für privatärztliche Leistungen. Ursächlich für diese Datenpannen war aber nicht das Fehlverhalten des Abrechnungsdienstes. Vielmehr lag der Fehler bei den jeweiligen Leistungserbringer*innen, die die Adressen der behandelten Personen nicht verifiziert hatten, sodass die Rechnungen die richtigen Adressaten von vornherein nicht erreichen konnten.

Der korrekte Umgang mit einem solchen Fall der postalischen Unzustellbarkeit hätte allerdings zur Rücksendung an den absendenden medizinischen Dienst führen müssen. Stattdessen wurden die Rechnungen vom zustellenden Unternehmen bei falschen Empfänger*innen abgeben oder in deren Briefkasten eingeworfen. Diese haben den Abrechnungsdienst dann über die Falschzustellung informiert, häufig nachdem sie den Briefinhalt auf eigene Betroffenheit geprüft und damit sensitive Daten der behandelten Person zur Kenntnis genommen hatten. Der Abrechnungsdienst seinerseits hat die Vorfälle bei uns gemeldet und zugleich mitgeteilt, dass er selbst die jeweils betroffenen Personen informiert habe oder informieren werde, sobald ihm deren korrekte Adressen vorliegen. Diese Herangehensweise ist vorbildlich, denn ein möglicher und u. U. langwieriger Streit darum, ob die oder der Leistungserbringende und/oder das Zustellunternehmen die rechtliche Verantwortung für die Datenpanne trägt und dementsprechend die von der Panne Betroffenen hierüber informieren muss, wird zugunsten einer möglichst schnellen Benachrichtigung der Betroffenen vermieden. Dass ein Zustellunternehmen Personal beschäftigt, das sich offenbar nicht an die vertragliche Hauptpflicht hält, nämlich Postsendungen nur bei korrekter Adressierung auszuliefern, steht auf einem anderen Blatt.

Ebenfalls relativ häufig waren Meldungen einer bundesweit tätigen Gewerkschaft, weil jeweils verschiedene Landesbezirke oder Fachbereiche bei der elektronischen Versendung von Gewerkschaftsnachrichten an ihre Mitglieder offene E-Mail-Verteiler genutzt hatten. Solche Datenpannen, bei denen „nur“ die u. U. personifizierte E-Mail-Adresse gegenüber allen anderen E-Mail-Empfänger*innen offengelegt wurde, scheinen auf den ersten Blick rechtlich wenig bedeutsam zu sein, zumal der Fehler auf Anhieb für alle Betroffenen offenkundig ist. Dennoch ist hier zu berücksichtigen, dass aus der Zugehörigkeit einer Person zu diesem E-Mail-Verteiler direkt auf ihre Gewerkschaftszugehörigkeit geschlossen werden kann – ein nach dem Gesetz besonders schützenswertes personenbezogenes Da-

tum.[363] Deshalb ist es wichtig, dass sich die oder der Verantwortliche des Fehlers bewusst ist und adäquat handelt. Dies geschah in allen uns gemeldeten Fällen dadurch, dass – dieses Mal allerdings mit „verborgenen" E-Mail-Adressen – eine weitere E-Mail mit einer Entschuldigung für die Datenpanne an denselben Verteiler geschickt wurde, verbunden mit der Zusage, künftig bei der Versendung von E-Mails verstärkt darauf zu achten, dass der E-Mail-Verteiler nicht für alle Empfänger*innen sichtbar ist.

Zunehmend haben uns auch Banken Datenpannen gemeldet, für die sie verantwortlich waren. Hier ging es vornehmlich um Falschübersendungen von Kreditunterlagen oder die unbefugte Offenbarung von Bankkontoinformationen wie z. B. der ungekürzten IBAN oder von Kontosalden. Anfängliche Unstimmigkeiten mit einzelnen Bankinstituten, ob hierdurch ein hohes Risiko für die Betroffenen einhergeht mit der Folge, dass die Bank die Betroffenen zwingend über den Vorfall benachrichtigen muss,[364] haben sich alsbald aufgelöst: In nahezu allen gemeldeten Fällen haben sich die Banken für maximale Transparenz entschieden und die jeweiligen Betroffenen vorsorglich über die Datenpanne informiert. Auch dies ist aus unserer Sicht lobenswert.

Insgesamt gingen die Verantwortlichen mit Datenpannen sachgerecht um. Wo Menschen arbeiten, passieren Fehler. Für uns ist wichtig, dass und wie ein Fehler insbesondere gegenüber den Betroffenen „eingefangen" wird. Dazu gehört zum einen das Eingeständnis der oder des Verantwortlichen, dass sich eine Datenpanne ereignet hat, und zum anderen das Ergreifen von Maßnahmen, um solche Fehler in der Zukunft möglichst zu vermeiden.

18.2 Datenpanne Kammergericht

Im vorigen Jahr berichteten wir über den Schadsoftware-Befall am Kammergericht, dessen Beseitigung zu einem monatelangen Ausfall der Informationstechnik des Gerichts führte.[365] Der Angriff und die nachfolgende Analyse offenbarten

363 Siehe Art. 9 Abs. 1 DS-GVO
364 Siehe Art. 34 Abs. 1 DS-GVO
365 JB 2019, 2.4

Sicherheitsschwächen der bisherigen Infrastruktur, die durch einen Neuaufbau der Informationstechnik mit Unterstützung des ITDZ[366] beseitigt wurden.

Der Befall der Computernetze des Kammergerichts mit der Schadsoftware Emotet hatte zur Folge, dass von heute auf morgen die gesamte Informationstechnik abgeschaltet werden musste und damit die digitale Arbeit des Gerichts größtenteils für Monate lahmgelegt wurde. Nach und nach wurden die einzelnen Arbeitsplätze wieder in Betrieb genommen, zunächst ohne jegliche Netzverbindung. Für notwendige Verbindungen nach außen wurden als Datenschleuse sog. Transfer-PCs eingerichtet. Bezüglich der sicheren Ausgestaltung dieser Schnittstelle hatten wir Hinweise gegeben.

Zugleich wurde durch externe Spezialisten eine forensische Analyse des Angriffs durchgeführt und die bisherige IT-Infrastruktur bewertet. Das Ergebnis offenbarte gravierende Schwächen beim Schutz der durch das Gericht verarbeiteten sensitiven Daten. Da die lokal auf den Computern installierten Virenscanner die Infektion nicht bemerkt hatten und die Datennetze des Gerichts nicht ausreichend voneinander abgeschottet waren, konnte die Schadsoftware Emotet sich auf einer Reihe von Arbeitsplätzen und Servern verteilen.

Die Betreiber*innen der Schadsoftware erlangten so Zugang zu der Informationstechnik des Gerichts. Dieser Zugang wurde u.a. dazu genutzt, Spuren in Form von Protokolldaten zu löschen, sodass sich auch mit der forensischen Analyse nicht mehr sicher feststellen ließ, ob und welche Daten möglicherweise in die Hände der Angreifer*innen gelangt sind. Auch der Weg der Infektion ließ sich nicht sicher rekonstruieren. Die erste Infektion durch eine derartige Schadsoftware erfolgt allerdings oft durch eine manipulierte Datei, die einzelnen Personen per E-Mail zugesandt wird.

Das gesamte Ausmaß der Kompromittierung der Systeme sowie die Frage, ob Daten abgeflossen sind, konnte die forensische Analyse nicht aufklären. Leider wurde auch darauf verzichtet, zumindest Teile der gelöschten Dateien aus der Da-

366 Das Informationstechnik-Dienstleistungszentrum (ITDZ) ist ein kommunales Unternehmen, das für die Digitalisierung der Berliner Verwaltung die notwendige Informationstechnik und eine sichere Vernetzung bereitstellt.

tensicherung wiederherzustellen und so ein vollständigeres Bild über den Vorfall zu erlangen.

Da das Kammergericht nicht über ein System verfügte, mit dem es zuverlässig die Schadsoftware-Freiheit der alten Systeme und der mit ihnen gespeicherten Daten feststellen konnte, entschied es sich, sein gesamtes Netzwerk neu aufzubauen. In diesem Zusammenhang wurden die meisten vom Kammergericht benötigten Dienste zum ITDZ verlegt. Die ursprünglich im alten System abgelegten Unterlagen blieben isoliert und standen über einen längeren Zeitraum lediglich als Archiv zur Einsichtnahme zur Verfügung.

Der Neuaufbau der Informationstechnik des Kammergerichts eröffnete die Möglichkeit, auch die Struktur der Netze und Anwendungen besser aufzustellen, als es bislang der Fall war. So verfügt das aufgebaute neue System über eine strikte Trennung zwischen den intern für die unterschiedlichen Fachverfahren genutzten Komponenten und den externen Komponenten für Internetnutzung und E-Mail-Kommunikation. Erstere werden nun in der vom ITDZ administrierten SBC-Umgebung[367], bei der sich sämtliche Programme und Daten auf geschützten Servern befinden und die Arbeitsplätze nur noch als Terminals, d. h. nur zur Tastatur-Eingabe und Bildschirm-Ausgabe, verwendet werden.

Durch die Abschottung der mit dem Internet verbundenen Komponenten und eine Aufteilung des Netzes in separate, voneinander getrennte Bereiche ist es nun wesentlich unwahrscheinlicher, dass eine erneute Infektion mit einer Schadsoftware ähnlich weitreichende Folgen hätte.

Ein weiterer wesentlicher Schritt bestand in der Ausstattung der Richterinnen und Richter mit mobilen Dienstgeräten, die ihnen eine Arbeit auch in ihrer häuslichen Umgebung erlauben.

Zuvor fand diese Heimarbeit – auf gesetzlicher Grundlage – mit Privatgeräten statt und Daten wurden zwischen diesen Privatgeräten und der dienstlichen Informationstechnik unkontrolliert ausgetauscht, vornehmlich über USB-Sticks oder durch den Versand per E-Mail.

367 SBC – Server Based Computer

Stufenweise wurden eine ausreichende Anzahl mobiler Dienst-Laptops bereitgestellt bzw. auf Wunsch auch stationäre Heimarbeitsplätze eingerichtet. Seit Herbst besteht auch die Möglichkeit, über eine VPN-Lösung mobil auf die interne Informationstechnik und damit auf wesentliche Justiz-Fachverfahren und zentral gespeicherte Verfahrensakten des Gerichts zuzugreifen. Die Dokumentenerstellung und -verwaltung erfolgt nun über das Justiz-Fachverfahren forumSTAR. Der zuvor übliche Datenaustausch über USB-Sticks wurde auch technisch unterbunden, indem die USB-Schnittstellen der (mobilen) Dienstgeräte deaktiviert wurden und die Nutzung von Massenspeichern nur noch an Transfer-PCs erlaubt ist. Zudem stehen den Mitarbeitenden nun an den (mobilen) Arbeitsplätzen wieder dienstliche E-Mail-Accounts zur Verfügung.

Die Sicherheit der eingesetzten Systeme ist Voraussetzung datenschutzkonformer Behördentätigkeit. Daher ist es zwingend notwendig, die Architektur der eingesetzten Informationstechnik auch im Hinblick auf den Schutz gegen Schadsoftware auszugestalten. Privates und Dienstliches ist strikt zu trennen. Das Kammergericht hat den Vorfall zum Anlass genommen, die eingesetzten IT-Systeme grundsätzlich zu modernisieren und in hohem Maße abzusichern.

19 Informationsfreiheit

19.1 Entwicklungen in Deutschland

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) fand in diesem Jahr aus besonderem Anlass unter dem Vorsitz des Hessischen Beauftragten für Datenschutz und Informationsfreiheit statt, weil kürzlich nunmehr auch in Hessen der allgemeine Informationszugang gesetzlich normiert worden ist.[368] Mitglieder der IFK sind alle Informationsfreiheitsbeauftragten in Deutschland; sie sind bei den jeweiligen Datenschutzaufsichtsbehörden angesiedelt. Die Bundesländer Bayern, Niedersachsen und Sachsen sind mangels eigener Gesetze noch immer nicht in der IFK vertreten.

19.2 Entwicklungen in Berlin

19.2.1 Änderung des Berliner Informationsfreiheitsgesetzes

Aus der Praxis

Vor dem Hintergrund der Neufassung des Berliner Datenschutzgesetzes (BlnDSG), mit der im Jahr 2018 eine Anpassung an die Datenschutz-Grundverordnung (DS-GVO) erfolgte, hatten wir im selben Jahr bei der hierfür federführenden Senatsverwaltung für Inneres und Sport auch eine Änderung des Berliner Informationsfreiheitsgesetzes (IFG) im Hinblick auf die Aufgaben und Befugnisse der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) in diesem Bereich angeregt.

Eine Anpassung des Gesetzes war schon deswegen erforderlich, weil Verweise aus dem IFG auf das BlnDSG nach dessen Änderung nicht mehr stimmten. Zur Begründung hatten wir ergänzend darauf hingewiesen, dass es schon aufgrund der eigenständigen Bedeutung der Informationsfreiheit sinnvoll sei, das IFG komplett eigenständig zu gestalten. Diese Eigenständigkeit hat sich durch die Euro-

368 Siehe JB 2018, 13.1

päisierung des Datenschutzrechts noch einmal verstärkt. Wir haben deshalb dafür geworben, die Regelungen zu Aufgaben und Befugnissen der BlnBDI aus dem BlnDSG herauszulösen und unmittelbar in das IFG aufzunehmen, das bislang nur einen entsprechenden Verweis auf das BlnDSG vorsah. Für unser Anliegen sprach auch, dass die Informationsfreiheitsbeauftragten – anders als die Datenschutzbeauftragten – primär als Schlichtungsstelle sowie beratend gegenüber Antragsteller*innen und informationspflichtigen Stellen tätig werden, sodass die neuen Aufgaben und Befugnisse der Datenschutzbeauftragten nach der DS-GVO nicht ohne Weiteres auf die Informationsfreiheitsbeauftragten übertragen werden könnten. Der bloße Verweis auf die entsprechenden Regelungen des BlnDSG, wie er bislang im IFG zu finden war,[369] erwies sich deshalb als nicht mehr sachgerecht.

Unser Anliegen wurde allerdings nicht schon mit Wirksamwerden der DS-GVO im Jahr 2018, sondern erst mehr als zwei Jahre später, gegen Ende des Berichtszeitraums, teilweise aufgegriffen: Im Zuge der Novellierung der landesrechtlichen Bestimmungen zur Anpassung an die Erfordernisse der DS-GVO[370] wurde auch das IFG geändert.[371]

Allein in Bezug auf die Errichtung unserer Behörde, die Ernennung und Beendigung des Amtsverhältnisses sowie die Rechtsstellung der oder des Beauftragten selbst wird nun noch auf die Bestimmungen des BlnDSG verwiesen.[372] Dagegen ist nun ausdrücklich neben der datenschutzrechtlichen Befugnis zur Verarbeitung personenbezogener Daten auch der Umfang der Kontrollmöglichkeiten unserer Behörde im IFG selbst normiert.[373] Dazu gehören Beratungen und die Abgabe von Empfehlungen ebenso wie die Pflicht öffentlicher Stellen, uns vor dem Erlass von Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften anzuhören, wenn sie die Informationsfreiheit betreffen.[374]

369 § 18 Abs. 2 IFG a. F.

370 Siehe 17.1

371 Art. 5 des Gesetzes zur Anpassung datenschutzrechtlicher Bestimmungen in Berliner Gesetzen an die Verordnung (EU) 2016/679 (Berliner Datenschutz-Anpassungsgesetz EU – BlnDSAnpG-EU) vom 12. Oktober 2020, GVBl. 2020, S. 807 (808 f.)

372 § 18 Abs. 1 IFG

373 § 18 Abs. 5 und 6 IFG

374 § 18 Abs. 2 IFG

Leider wurden weitere die Arbeit unserer Behörde betreffende Regelungen, die für den Bereich des Datenschutzes im BlnDSG ausdrücklich festgelegt sind, nicht in das IFG übernommen. Es handelt sich dabei vor allem um das Recht, jederzeit Zugang zu Diensträumen und Informationsverarbeitungsanlagen zu erhalten, sowie um eine Festlegung zum Umfang der Stellungnahmen von Verwaltungen, bei denen Mängel im Bereich der Informationsfreiheit festgestellt wurden.[375] Es wäre sinnvoll gewesen, auch hier vorzusehen, dass derartige Stellungnahmen auch die Maßnahmen enthalten sollten, die aufgrund einer Beanstandung unserer Behörde getroffen wurden. Auch diesbezüglich hätte sich – nicht zuletzt, um die Bedeutung der Informationsfreiheit hervorzuheben – ein Gleichklang beider Gesetze angeboten. Wir werden dieses Ansinnen im Rahmen der beabsichtigten Entwicklung eines Transparenzgesetzes, das das IFG ersetzen soll, weiterverfolgen.[376]

Die Änderung des IFG im Hinblick auf die explizite Regelung der Aufgaben und Befugnisse unserer Behörde im Gesetz selbst war überfällig.

19.2.2 Endlich am Start – Entwurf für ein Berliner Transparenzgesetz

Zur Erfüllung der Koalitionsvereinbarung, in der u.a. die Weiterentwicklung des IFG hin zu einem Transparenzgesetz festgeschrieben worden war,[377] hat der Senat im Sommer zunächst Eckpunkte für ein solches Gesetz beschlossen. Wir hatten zuvor die Gelegenheit zur Stellungnahme erhalten. Unsere zum Teil massive Kritik wurde jedoch im späteren Referentenentwurf eines „Gesetzes zur Weiterentwicklung des Informationszugangs für die Allgemeinheit" (Entwurf eines Berliner Transparenzgesetzes – BlnTG-E) der hierfür federführenden Senatsverwaltung für Inneres und Sport leider nicht berücksichtigt. Wir haben auch hierzu Stellung genommen und unsere Kritik erneut geäußert und zum Teil vertieft.

So haben wir als einen zentralen Mangel des BlnTG-E hervorgehoben, dass über die bisher bereits im geltenden IFG bestehenden Bereichsausnahmen eine Viel-

375 Siehe § 13 Abs. 4 sowie Abs. 2 BlnDSG
376 Siehe 19.2.2
377 JB 2018, 13.2.1

zahl weiterer Ausnahmen für diverse Behörden vorgesehen ist. Dies würde eine deutliche Verschlechterung gegenüber der bisherigen Rechtslage bedeuten und insofern keine Weiter-, sondern eine Rückentwicklung des IFG. Dies wird nicht aufgewogen durch den neuen proaktiven Informationszugang, der – als Kernbestandteil eines modernen Transparenzgesetzes – öffentliche Stellen antragsunabhängig zur Bereitstellung von Informationen auf einer elektronischen Plattform, d. h. in einem Transparenzportal, verpflichtet. Die Liste der Ausnahmen vom Anwendungsbereich[378] ist derart lang, dass wir darum gebeten haben, zumindest diejenigen zu streichen, die über die bisherige Rechtslage hinausgehen. Die geplanten Ausnahmen einschließlich der von uns empfohlenen Streichungen stellen sich demnach – analog zum geltenden IFG – wie folgt dar:

„Keine Informationspflicht nach diesem Gesetz besteht

1. für Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden, soweit sie als Organe der Rechtspflege oder aufgrund besonderer Rechtsvorschriften in richterlicher Unabhängigkeit tätig geworden sind, für die für Justiz zuständige Senatsverwaltung, soweit sie als Fachaufsichtsbehörde über die Staatsanwaltschaft ~~oder in Gnadenangelegenheiten~~ tätig wird sowie für im Rahmen von Disziplinarverfahren entstandene Vorgänge ~~und Vergabekammern~~;
2. für den Rechnungshof, soweit er in richterlicher Unabhängigkeit tätig geworden ist; dies gilt nicht für seine Jahresberichte;
3. für Vorgänge ~~der Steuerverwaltung sowie~~ der Innenrevisionen;
4. für den Verfassungsschutz;
5. für das Abgeordnetenhaus von Berlin in Bezug auf parlamentarische Angelegenheiten;
6. öffentlich-rechtliche Rundfunkanstalten in Bezug auf journalistisch-redaktionelle Informationen;
7. ~~für allgemeinbildende Schulen, Schulbehörden und Schulaufsichtsbehörden in Bezug auf Informationen, die die Erstellung einer Rangliste ermöglichen und somit geeignet sind, die Verwirklichung der Bildungs- und Erziehungsziele zu gefährden.~~;

378 Siehe § 3 Abs. 1 BlnTG-E

8. für ~~Universitätskliniken, Wissenschafts- und~~ Forschungseinrichtungen, ~~Hochschulen, Schulen sowie für Bildungs- und Prüfungseinrichtungen,~~ es sei denn, es sind Informationen über den Namen von Drittmittelgebern, die Höhe der Drittmittel und die Laufzeit der mit Drittmitteln finanzierten abgeschlossenen Forschungsvorhaben betroffen;
9. für Grundlagenforschung oder anwendungsbezogene Forschung; § 7 Absatz 1 Nummer 9 bleibt unberührt;
10. ~~für Selbstverwaltungskörperschaften der freien Berufe in Bezug auf Informationen, die einer beruflichen Geheimhaltungspflicht unterliegen.“~~

Es kann nicht Aufgabe eines Transparenzgesetzes sein, die Pflicht zur Offenlegung von Informationen weiter einzuschränken, als es zuvor der Fall war. Jede (weitere) Bereichsausnahme schmälert den Wert eines modernen Transparenzgesetzes in der Öffentlichkeit erheblich.

So ist z. B. nicht nachvollziehbar, warum die für Justiz zuständige Senatsverwaltung in **Gnadenangelegenheiten (Nr. 1)** von einer gesetzlich normierten Transparenz gänzlich befreit sein soll, gibt es doch zahlreiche allgemeine Informationen (wie Zahlen zu Gnadenerlassen), die für die Öffentlichkeit interessant sein können. Dasselbe gilt für die **Vergabekammern (Nr. 1 a. E.)** in Bezug auf ihre Entscheidungen – Einzelinformationen der Unternehmen dürften durch die vorgesehene Regelung zum Schutz von Geschäftsgeheimnissen ausreichend geschützt sein.[379]

Auch **Vorgänge der Steuerverwaltung (Nr. 3)** sollten nicht von vornherein ausgeklammert werden, denn auch sie sind grundsätzlich von öffentlichem Interesse, z. B. im Hinblick auf Steuerberechnungsmodelle in den Finanzämtern.

Obwohl es der bisherigen Rechtslage entspricht,[380] ist nicht nachvollziehbar, aus welchem Grund der **Verfassungsschutz (Nr. 4)** auch in Zukunft überhaupt keiner Transparenzpflicht unterliegen soll. Dies steht im Widerspruch zu den Vorschriften, die ausdrücklich eine Pflicht des Verfassungsschutzes zur Unterrichtung der Öffentlichkeit vorsehen und damit eine Kontrollmöglichkeit durch die Bür-

379 Siehe § 16 BlnTG-E

380 Siehe § 32 Abs. 3 Verfassungsschutzgesetz Berlin (VSG Bln)

gerinnen und Bürger bzw. die Medien manifestieren.[381] Der Öffentlichkeit können zweifelsohne allgemeine Informationen über die Aufgaben und Befugnisse, Arbeitsfelder und Vorgehensweisen des Verfassungsschutzes zugänglich gemacht werden, ohne Sicherheitsaspekte zu tangieren. Darüber hinaus kann und muss der Verfassungsschutz die Öffentlichkeit bei Gefahren für die freiheitliche demokratische Grundordnung ohnehin informieren. Hierunter fällt bspw. die Veröffentlichung von Hinweisen zu aktuellen Geschehnissen im extremistischen Spektrum, die Information über die ideologischen Grundlagen des Islamismus, des Rechts-, Links- und Ausländerextremismus sowie über die wichtigsten in Berlin vertretenen extremistischen Gruppierungen. Die jetzt vorgesehene Regelung hätte zur Folge, dass noch nicht einmal die bislang öffentlichen Verfassungsschutzberichte in das Transparenzportal als veröffentlichungspflichtige Informationen einzustellen wären.[382] Im Übrigen sollten – wie in anderen Bereichen der inneren Sicherheit auch – die im Gesetz vorgesehenen Ausnahmetatbestände[383] genügen, um den Schutzbedarf eines Teils der Arbeit des Verfassungsschutzes zu gewährleisten.

Ein vollkommen falsches Signal geht vom überwiegenden Ausschluss der **Wissenschaftseinrichtungen, Hochschulen, Schulen und Bildungseinrichtungen bzw. der allgemeinbildenden Schulen, Schulbehörden und Schulaufsichtsbehörden** aus **(Nr. 7 und 8).** Gerade im Wissenschafts- und Bildungsbereich ist Transparenz im Hinblick auf Informationen der Verwaltung besonders bedeutsam. So sollten Studierende bzw. Eltern von Schulkindern (ggf. auf Antrag) erfahren dürfen, wie viele Vorlesungen bzw. Unterrichtsstunden in einem bestimmten Fach während eines Studien- bzw. Schuljahres ersatzlos ausgefallen sind. Das gilt umso mehr in Pandemie-Zeiten. Die Erstellung einer „Rangliste" für Schulen mag – ob zu Recht oder zu Unrecht – von der Schulaufsicht nicht erwünscht sein, sollte aber nicht dazu führen, dass vorhandene Informationen (z. B. im Rahmen der Schulinspektionsberichte) von vornherein nicht offengelegt werden: Dass einzelne Schulen durch Offenlegung „zu Unrecht eine negative Bewertung erfahren würden, da einzelne statistische Werte in den Fokus gerückt würden",[384] ist spekulativ und nimmt die Bewertung durch mündige Eltern und die Öffentlichkeit insgesamt vor-

381 Siehe § 5 Abs. 1 und § 26 Satz 1 VSG Bln
382 Siehe § 7 Abs. 1 Nr. 8 BlnTG-E
383 Z. B. § 13 Abs. 1 Nr. 4 BlnTG-E
384 So die Begründung zu § 3 Nr. 7 BlnTG-E

weg. Darüber hinaus ist der Nebensatz in der o. g. Nr. 7 zu unbestimmt und birgt deshalb ein erhebliches Streit- bzw. Klagepotenzial.

Die **Universitätskliniken (Nr. 8)** verfügen ebenfalls über allgemeine Informationen in Bezug auf die Krankenhausverwaltung, die nicht von vornherein geheim zu halten sind. Als prominentes Beispiel sei hier die Zahl der für Covid-19-Erkrankte freigehaltenen Betten genannt.

Ein Ausnahmetatbestand für die **Selbstverwaltungskörperschaften der freien Berufe (Nr. 10)** ist wegen des Absatzes 2 der geplanten Norm nicht erforderlich. Danach besteht die Informationspflicht nicht, soweit andere Rechtsvorschriften entgegenstehen.

Zusätzlich zu diesen ausufernden Bereichsausnahmen haben wir die geplanten zusätzlichen Einschränkungen der Veröffentlichungspflicht[385] moniert. Die diesbezügliche Liste einschließlich der von uns empfohlenen Streichungen stellt sich wie folgt dar:

„Von der Veröffentlichungspflicht ausgenommen sind:

1. Verträge mit einem Gegenstandswert von weniger als 100.000 Euro, wenn zwischen den Vertragspartnern im Laufe der vergangenen zwölf Monate Verträge mit einem Gegenstandswert von weniger als insgesamt 100.000 Euro abgeschlossen worden sind;
2. Subventions- und Zuwendungsvergaben mit einem Wert von weniger als 100 Euro bei juristischen Personen beziehungsweise weniger als 1.000 Euro bei sonstigen teilrechtsfähigen Organisationen und natürlichen Personen in einem Zeitraum von zwölf Monaten an eine Empfängerin oder einen Empfänger;
3. die Erteilung einer Baugenehmigung oder eines Bauvorbescheides an eine Antragstellerin oder einen Antragsteller, sofern es sich um reine Wohnbebauung mit maximal fünf Wohneinheiten handelt.

385 Siehe § 9 BlnTG-E

4. ~~Gutachten und Dienstleistungen für Einzelfälle, zum Beispiel arbeitsmedizinische Untersuchungen oder Laboruntersuchungen von Produkten oder Bodenproben,~~
5. Gutachten und Dienstleistungen, bei denen eine Veröffentlichung aus datenschutzrechtlichen Gründen unzulässig wäre,
6. ~~Gutachten und Dienstleistungen, die nur Einzelaspekte eines insgesamt noch nicht abgeschlossenen Themas erörtern,~~
7. Gutachten und Dienstleistungen, die der internen Meinungsbildung des Senats im Vorfeld noch zu treffender Entscheidungen dienen,
8. ~~Gutachten und Dienstleistungen im Zusammenhang mit rechtlichen Auseinandersetzungen, wenn deren Veröffentlichung die Interessen des Landes Berlin beeinträchtigen würde und~~
9. ~~Gutachten und Dienstleistungen, die vertrauliche Geschäftsdaten enthalten oder deren Veröffentlichung gegen die Verschwiegenheitspflicht nach § 395 des Aktiengesetzes verstoßen würde.~~

Die aus unserer Sicht zu streichenden Ausnahmen von der Veröffentlichungspflicht entsprechen offenbar den Ausführungen einer seit 2013 bestehenden, uns nicht bekannten Verwaltungsvorschrift der Senatsverwaltung für Finanzen, also einer untergesetzlichen Regelung, die – mindestens fragwürdige, wenn nicht rechtswidrige – Abweichungen von der bisherigen Gesetzeslage, dem IFG, vorsieht.

Die Erforderlichkeit dieser Ausnahmen ist in der Gesetzesbegründung nicht dargelegt; unklar ist im Übrigen bei allen genannten Ausnahmen, was der Begriff der „Dienstleistungen“ beinhaltet.

Bei **Nr. 4** ist darüber hinaus unklar, an welche Einzelfälle gedacht ist und aus welchem Grund die offenbar gesundheitsrelevanten Informationen nicht offenzulegen sind.

Nr. 9 spricht von „vertraulichen Geschäftsdaten", die nicht näher definiert sind; der an anderer Stelle des Gesetzentwurfs geregelte Schutz von Geschäftsgeheimnissen[386] reicht hierfür aus.

Weitere Änderungsempfehlungen zum BlnTG-E betrafen datenschutzrechtliche Aspekte. So sollte eine anonyme Antragstellung grundsätzlich möglich sein. Denn ein Individualantrag muss nicht in jedem Fall die Identität der antragstellenden Person erkennen lassen, sondern nur, soweit die Identität für die Beantwortung der Anfrage erforderlich ist. Sie ist aber nicht erforderlich, wenn die antragstellende Person lediglich die Auskunft erhalten soll, dass die gewünschten Informationen nicht vorhanden sind; sie ist ebenfalls nicht erforderlich in Fällen des Gebührenverzichts,[387] denn ein rechtsmittelfähiger (Gebühren-)Bescheid muss dann nicht erteilt werden. Der Name und die postalische Anschrift sind allerdings dann erforderlich, wenn ein Gebührenbescheid zugestellt werden muss.[388]

Die Offenlegung der Kerndaten von Beschäftigten[389] auf Antrag sollte neben der „Telekommunikationsnummer" die E-Mail-Adresse und den Namen der unterzeichnenden Person umfassen. Denn die E-Mail-Adresse ist im Zeitalter der elektronischen Kommunikation das wichtigste Kontaktdatum und sollte grundsätzlich nicht schutzbedürftig sein. Unterzeichnende Personen tragen die inhaltliche Verantwortung, sodass ihre Namen ebenfalls grundsätzlich nicht schutzbedürftig sind.

Wir hoffen, dass das Transparenzgesetz rechtzeitig vor dem Ende der Legislaturperiode im Herbst 2021 verabschiedet wird. Bis dahin werden wir das Gesetzgebungsverfahren weiter kritisch, aber auch konstruktiv begleiten. Dabei wird auch darauf zu achten sein, dass die jüngsten Änderungen des IFG zusammen mit unseren weiteren Empfehlungen[390] in das neue Transparenzgesetz übernommen werden.

386 Siehe § 16 BlnTG-E
387 Siehe § 20 Abs. 1 Satz 2 BlnTG-E
388 Anders § 15 Abs. 2 BlnTG-E
389 Bislang zulässig nach § 6 Abs. 2 Satz 1 Nr. 2 IFG
390 Siehe 19.2.1

19.2.3 Ein Transparenzbarometer für Berlin

Die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung übersandte uns den Referentenentwurf für ein Gesetz zur Transparenzmachung von Ergebnissen amtlicher Kontrollen in der Lebensmittelüberwachung (Entwurf eines Lebensmittelüberwachungstransparenzgesetzes – LMÜTranspG-E) sowie den Entwurf für die das Gesetz ausführende Verordnung, die auch die Beurteilungskriterien enthält. Mit diesem Vorhaben soll eine entsprechende Koalitionsvereinbarung von 2016 umgesetzt werden. Hier ist festgelegt, dass Berlin sich für ein Mehr an Transparenz im Bereich der Lebensmittelhygiene einsetzen und erforderlichenfalls auch eigene landesrechtliche Regelungen schaffen wird.

Wir haben uns bereits in der Vergangenheit mit einem Vorläufer-Modell, dem Smiley-Projekt im Bezirk Pankow, befasst und es aus Sicht der Informationsfreiheit und des Datenschutzes begrüßt.[391] Es basierte seinerseits auf entsprechenden Modellen für Gaststätten in Dänemark, konnte aber hierzulande nicht weitergeführt werden, weil es an einer Rechtsgrundlage für die Veröffentlichung der amtlichen Kontrollergebnisse fehlte.

Diese Rechtsgrundlage für die verpflichtende Veröffentlichung der Ergebnisse der amtlichen Lebensmittelkontrolle soll nun geschaffen werden. Kernbestandteil ist das sog. Transparenzbarometer, auf dem die Kontrollergebnisse durch ein buntes Balkendiagramm grafisch dargestellt werden. Darin markiert ein auf Grün zeigender Pfeil, dass die Hygiene-Anforderungen erfüllt sind, und ein auf Gelb zeigender Pfeil, dass diese Anforderungen teilweise erfüllt sind. Steht der Pfeil auf Rot, sind die Anforderungen unzureichend erfüllt.[392] Unter dem Transparenzbarometer werden die Beurteilungsmerkmale und deren Beurteilung in Textform angeführt. Um sicherzustellen, dass die Verbraucher*innen sich vor dem Besuch z. B. einer Gaststätte oder eines Imbissstandes über den dortigen Hygienezustand informieren können, soll dieses Unternehmen verpflichtet sein, das Transparenzbarometer unverzüglich an oder in der Nähe der Eingangstür anzubringen. Zusätzlich zu dieser Informationsmöglichkeit vor Ort ist eine Veröffentlichung im Internet durch

391 JB 2008, 15.2.2; JB 2011, 13.2
392 § 5 Abs. 4 LMÜTranspG-E

die zuständige Lebensmittelaufsicht vorgesehen,[393] damit die Effizienz der Information gesteigert wird.

Im LMÜTranspG-E war zunächst auch vorgesehen, dass das Transparenzbarometer neben den Betriebsstätten mit Anschrift auch die verantwortlichen Lebensmittelunternehmer*innen namentlich ausweist.[394] Das haben wir hinterfragt, indem wir die zuständige Senatsverwaltung gebeten haben, uns zu verdeutlichen, aus welchem Grund die verpflichtende Offenlegung der Namen der für den Betrieb Verantwortlichen – zusätzlich zur verpflichtenden Offenlegung der Namen der Betriebsstätten – für erforderlich gehalten wird. Offenbar war dies nicht begründbar, denn der Gesetzentwurf wurde daraufhin entsprechend geändert. Sowohl aus Transparenz- als auch aus Datenschutzsicht ist die Nennung der Betriebsstätten mit Anschrift im Transparenzbarometer völlig ausreichend.

Wir begrüßen das geplante Transparenzmodell als einen überfälligen Schritt zur Stärkung der Verbraucherinformation, insbesondere in Bezug auf Gaststätten in Berlin.

19.3 Nachhilfe für die Senatsverwaltung für Umwelt, Verkehr und Klimaschutz

Uns erreichten zwei Beschwerden, die das bei der Senatsverwaltung für Umwelt, Verkehr und Klimaschutz angesiedelte Verkehrsmanagement betrafen.

Aus der Praxis

(1) Der Allgemeine Deutsche Fahrrad-Club Berlin e. V. (ADFC) beschwerte sich Anfang Februar bei uns darüber, dass er auf seinen Antrag auf Einsichtnahme in die Vertragsmodalitäten der Stadt mit der Alliander Stadtlicht GmbH von Mitte Dezember 2019 trotz Erinnerung keine Reaktion erhalten habe. Zur Begründung des Begehrens wurde vom ADFC vorgetragen, dass es in Berlin immer wieder zu massiven Verzögerungen und langen Realisierungszeiträumen für die Anpassung von Lichtsignalanlagen durch das Unternehmen komme. Die langen Wartezeiten führten gerade bei unfallträchtigen Kreuzungen immer wieder zu le-

393 § 8 Abs. 1 LMÜTranspG-E

394 § 8 Abs. 1 LMÜTranspG-E i. V. m. § 4 des entsprechenden Verordnung-E

bensgefährlichen Situationen für Passant*innen und Radfahrende. Deshalb ging es dem ADFC konkret darum zu erfahren, welche Leistungen und Sanktionsmechanismen im Falle einer Nichterfüllung vertraglich vereinbart wurden, wie die Evaluation der Leistungserbringung geregelt wurde und welche Kündigungsmöglichkeiten des Vertrages vereinbart worden waren.

Wir haben daraufhin Kontakt zu der zuständigen Senatsverwaltung aufgenommen und darum gebeten, sich der Sache anzunehmen und über den Antrag nunmehr unverzüglich, d. h. ohne schuldhaftes Zögern,[395] zu entscheiden[396] sowie uns eine Kopie des Bescheids zu übersenden. Nach einem Monat ohne Reaktion auch uns gegenüber mussten wir die Senatsverwaltung Ende März an die Erledigung der Angelegenheit erinnern. Daraufhin erhielten wir Mitte April eine Kopie des Bescheids der Senatsverwaltung, mit dem der Antrag auf Informationszugang abgelehnt wurde. Zur Begründung wurde vor allem angeführt, dass einer Offenlegung des Vertrags der Schutz von Betriebs- und Geschäftsgeheimnissen[397] entgegenstehe. Solche Geheimnisse seien alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich seien und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse habe. Ein Interesse an der Nichtverbreitung ist anzuerkennen, wenn die Offenlegung der Information geeignet ist, möglichen Konkurrenten exklusives technisches oder kaufmännisches Wissen zugänglich zu machen und so die Wettbewerbsposition des Unternehmens nachteilig zu beeinflussen oder ihm in sonstiger Weise wirtschaftlichen Schaden zuzufügen.

Zwar hat die Senatsverwaltung in richtiger Weise die gängige Definition der Rechtsprechung zu Betriebs- und Geschäftsgeheimnissen herangezogen;[398] allerdings hat sie den Schutzbedarf in Bezug auf den gesamten Vertrag angenommen, obwohl die Offenlegung des gesamten Vertrags nicht beantragt war. Stattdessen hätte die Senatsverwaltung prüfen müssen, ob die konkret gewünschten Teilinformationen aus dem Vertrag jeweils schützenswerte Betriebs- oder Geschäftsgeheimnisse darstellen.

395 Siehe § 121 Abs. 1 Satz 1 Bürgerliches Gesetzbuch (BGB)

396 Siehe § 14 Abs. 1 Satz 1 IFG

397 Siehe § 7 IFG

398 Ständige Rechtsprechung: siehe z. B. BVerfG, Beschluss vom 14. März 2006 – 1 BvR 2087/03, 1 BvR 2111/03; BVerwG, Urteil vom 28. Mai 2009 – 7 C 18.08

Vor diesem Hintergrund haben wir dem ADFC empfohlen, gegen den Bescheid Widerspruch einzulegen. Dieser Empfehlung ist er Anfang Mai gefolgt. Nach einer Zwischennachricht der Senatsverwaltung von Anfang August an den ADFC, den Widerspruch „nunmehr" prioritär zu behandeln, haben wir uns Anfang Oktober nach dem Sachstand erkundigt. Daraufhin wurde uns mitgeteilt, dass der Widerspruch in der zweiten Oktoberhälfte beschieden werde. Diese Zusage wurde erfüllt: Der angefochtene Bescheid wurde aufgehoben und dem ADFC die Einsichtnahme in den gesamten Generalübernehmervertrag für das Management von Planung, Bau, Betrieb und Instandhaltung der Lichtsignalanlagen-Infrastruktur zugesprochen, aus denen sich die wesentlichen Leistungen, die Sanktions- und die Evaluationsmechanismen sowie die Regelungen zur Kündigung des Generalübernehmervertrags ergeben. Weiterhin wurde das Recht auf Einsicht in zwei Anlagen zum Vertrag bestätigt, aus denen sich zusätzliche Leistungspflichten und Vertragsstrafen ergeben. Allein die enthaltenen „monetären Beträge und Prozentzahlen" wurden unter Hinweis auf schützenswerte Betriebs- und Geschäftsgeheimnisse geschwärzt.

Dies ist ein Musterbeispiel für unsere erfolgreiche Tätigkeit in der Funktion als Schiedsstelle nach dem IFG.[399]

Aus der Praxis

(2) Ein Petent hatte bei der Senatsverwaltung für Umwelt, Verkehr und Klimaschutz einen Antrag auf Einsicht in eine erteilte Ausnahmegenehmigung für die temporäre Nutzung eines Bussonderfahrstreifens für Be- und Entladetätigkeiten eines ansässigen Autohauses beantragt. Die Akteneinsicht wurde zwar bewilligt. Allerdings wurde hierfür eine Gebühr in Höhe von 25,00 Euro festgesetzt und um Vorabüberweisung des Betrags innerhalb von drei Wochen gebeten. Hiergegen hat der Petent Widerspruch eingelegt und uns um Unterstützung gebeten.

Wir haben der Senatsverwaltung mitgeteilt, dass es sich bei den angefragten Informationen um „Umweltinformationen" handelt, deren Einsichtnahme vor Ort gebührenfrei ist.[400] Denn der Begriff „Umweltinformation" ist nach der Rechtsprechung des Bundesverwaltungsgerichts weit auszulegen; ein auch nur mittelba-

399 Siehe § 18 IFG

400 Siehe § 18a Abs. 4 Satz 3 Nr. 1 IFG

rer Zusammenhang der einzelnen Daten mit der Umwelt reicht hiernach aus.[401] Dies war bei den in Rede stehenden Informationen der Fall. Denn die dem Autohaus erteilte Ausnahmegenehmigung für die temporäre Nutzung des Bussonderfahrstreifens für Be- und Entladetätigkeiten ist objektiv eine Erschwernis für den Bus- und Fahrradverkehr, was nach allgemeiner Lebenserfahrung dazu führen kann, dass Betroffene von der Nutzung dieser Verkehrsmittel Abstand nehmen und stattdessen den eigenen Pkw nutzen. Damit würde aber der mit der Bus- bzw. Radnutzung in Berlin verfolgte Zweck, Umweltemissionen zugunsten des Klimaschutzes zu minimieren, konterkariert. Vor diesem Hintergrund war hier zumindest der mittelbare Zusammenhang der angefragten Informationen mit der Umwelt zu bejahen.

Später teilte uns der Petent mit, dass er eine Mahnung zur vorab festgesetzten Gebühr (zuzüglich Mahnkosten) erhalten habe. Wir haben die Senatsverwaltung darauf hingewiesen, dass der Bescheid auch deshalb rechtswidrig sei, weil der angefochtene Bescheid ohne nähere Begründung, also pauschal, zur Vorauszahlung der Gebühr verpflichtete. Dies widerspricht der Rechtsprechung des OVG Berlin–Brandenburg,[402] nach der im Bereich des Informationszugangs eine Amtshandlung nur ausnahmsweise von der vorherigen Entrichtung der Verwaltungsgebühr abhängig gemacht werden darf. Voraussetzung dafür seien Anhaltspunkte, dass ohne die Vorauszahlung das Haushaltsinteresse gefährdet wäre. Dies kann etwa der Fall sein, wenn die antragstellende Person zahlungsunfähig oder -unwillig ist.

Da es hierfür keine Anhaltspunkte gab, ist die Senatsverwaltung unserer Auffassung gefolgt und hat dem Widerspruch insoweit stattgegeben. Im Übrigen wurde er zurückgewiesen: Ein auch nur mittelbarer Zusammenhang der in der Sondergenehmigungsakte enthaltenen Informationen mit der Umwelt sei nicht erkennbar. So sei nicht messbar und in der Akte keine Information darüber enthalten, wie viel höher die Umweltbelastung wäre, wenn BVG-Kund*innen oder Radfahrende wegen der erforderlichen Umfahrung aufgrund von Be- und Entladetätigkeiten nicht mehr den Bus oder das Fahrrad, sondern den eigenen Pkw nutzen würden.

401 BVerwG, Urteil vom 23. Februar 2017 – 7 C 31.15

402 OVG Berlin–Brandenburg, Beschluss vom 26. Mai 2014 – OVG 12 B 22.12

Wir haben dem Petenten empfohlen, die Angelegenheit gerichtlich klären zu lassen, weil es bei dem laut Rechtsprechung ausreichenden mittelbaren Zusammenhang der Informationen mit der Umwelt nicht darauf ankommt, ob tatsächlich Emissionswerte vorliegen bzw. diese in die Akte, in die Einsicht begehrt wird, aufgenommen wurden. Es reicht aus, dass die begehrten Informationen nach allgemeiner Lebenserfahrung mittelbare Auswirkungen auf die Umwelt haben könnten.

Die Senatsverwaltung hat einen erheblichen Begründungsaufwand betrieben, damit sie die Akteneinsicht vor Ort nicht gebührenfrei zulassen muss, sondern nur gegen Zahlung von 25,00 Euro. Damit soll offenbar vergleichbaren Anträgen vorgebeugt werden, die angesichts zunehmend chaotischer Verkehrsverhältnisse in Berlin nicht unwahrscheinlich sind.

20 Aus der Dienststelle

20.1 Entwicklungen

Das vergangene Berichtsjahr war für die Dienststelle der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) in mehrfacher Hinsicht ein besonderes Jahr.

Wie in vielen anderen Bereichen der öffentlichen Verwaltung war und ist der Umgang mit der Corona-Pandemie auch für die Dienststelle der BlnBDI eine besondere Herausforderung. Einerseits musste der Dienstbetrieb pandemieverträglich gestaltet werden, andererseits durften die dafür notwendigen und umfassenden strukturellen Maßnahmen zur Veränderung der Arbeitsorganisation den gesetzlichen Auftrag der BlnBDI nicht missachten und die Qualität der Arbeit nicht über Maßen beeinträchtigen.

Durch die Beschaffung und den Einsatz mobiler Endgeräte konnte für die Mehrheit der Dienstkräfte die Möglichkeit des, wenn auch eingeschränkten, Arbeitens im sog. Homeoffice geschaffen werden. Die Anwesenheit der Mitarbeiter*innen in den Räumen der Dienststelle wurde dadurch, soweit technisch möglich und im Rahmen der Tätigkeitsbeschreibungen der Dienstkräfte vertretbar, erheblich reduziert. Präsenztermine mit Dritten in der Dienststelle, Vor-Ort-Termine und Prüfungen außerhalb der Dienststelle wurden nur durchgeführt, soweit dies zwingend erforderlich war.

Das Arbeiten im Homeoffice, die antizyklische Anwesenheit der Dienstkräfte in den Diensträumen und der Verzicht auf (größere) Gruppenbesprechungen mit persönlicher Anwesenheit haben die bisherige Arbeitsorganisation und die internen Kommunikationsabläufe maßgeblich verändert. Durch den Einsatz von technischen Hilfsmitteln und Formaten (z. B. Video- und Telefonkonferenzen) konnte dies nur z. T. ausgeglichen werden. Die Auswirkungen auf das soziale und kollegiale Miteinander der Mitarbeiter*innen sind mit Sicherheit nicht zu unterschätzen.

Wie berichtet,[403] hat der Haushaltsgesetzgeber mit dem Doppelhaushalt 2020/2021 auf die neuen Anforderungen und die erheblich gestiegene Arbeitsbelastung der gesamten Dienststelle nach dem Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) reagiert und der BlnBDI für die Jahre 2020/2021 insgesamt 21 neue Stellen (13 Stellen für 2020 und 8 Stellen für 2021) bewilligt. Der Berliner Gesetzgeber hat damit ein starkes Zeichen für die Bedeutung des Datenschutzes in Berlin im Allgemeinen und die Stärkung von Betroffenenrechten im Besonderen gesetzt. Erwartungsgemäß hat die erfreuliche Verbesserung der Personalausstattung in der aufsichtsbehördlichen Praxis der Dienststelle jedoch nicht unmittelbar zu einer Änderung der angespannten Lage geführt. Die für das Jahr 2020 bewilligten Stellen mussten ausgeschrieben, besetzt und die neuen Mitarbeiter*innen eingearbeitet werden. Hier sind wir aber auf einem sehr guten Weg.

Vor allem konnte mit dem bewilligten Personalzuwachs unsere Informatikabteilung (Abteilung III) endlich angepasst werden an die nachhaltig veränderten Herausforderungen und Aufgaben, die nicht nur durch die DS-GVO, sondern auch durch die umfassende Digitalisierung des wirtschaftlichen und öffentlichen Lebens entstanden sind. Um die Kompetenzen zu bündeln, die Effizienz zu steigern und das Zusammenwirken mit den juristischen Abteilungen zu fördern, wurde die bisherige Referatsstruktur in der Abteilung III aufgelöst und neu strukturiert in Form von themenbezogenen Kompetenzteams für Prüfungen, Labortätigkeiten, Beratung, Datenschutz-Folgenabschätzung/Akkreditierung/Zertifizierung, Beschwerden und Datenpannen. Die Aufgaben in den Kompetenzteams werden jeweils von einem Teamleiter koordiniert, der auch nach außen als Ansprechpartner fungiert.

Auch die Zusammenarbeit mit nationalen und internationalen Gremien und Einrichtungen,[404] die parlamentarische Begleitung von datenschutzrelevanten Vorhaben sowohl auf Berliner als auch auf Bundesebene sowie die Kooperation mit politischen, gesellschaftlichen und wirtschaftlichen Akteur*innen und Multiplikator*innen zur Förderung des Datenschutzes und der Informationsfreiheit ist für

403 JB 2019, 18.1

404 Z. B. die nationale, die europäische und die internationale Datenschutzkonferenz, die nationale und die internationale Konferenz der Informationsfreiheitsbeauftragten, die Berlin Group, der Europäische Datenschutzausschuss und dessen Arbeitskreise, die sog. Subgroups

die BlnBDI von erheblicher fachlicher Bedeutung. Um die aufgrund der DS-GVO extrem gewachsene Zahl an Abstimmungsverfahren in diesen Bereichen zu bündeln und zuverlässig abteilungsübergreifend zu koordinieren, wurde dieser Aufgabenbereich zusammengefasst und einem neu geschaffenen „Referat Gremien-, Presse- und Öffentlichkeitsarbeit" zugewiesen, das im Organisationsgefüge direkt der Dienststellenleitung unterstellt ist. Durch dieses neue Referat soll insgesamt auch eine verstärkte Presse- und Öffentlichkeitsarbeit ermöglicht werden, um unseren gesetzlichen Informationspflichten gegenüber der Öffentlichkeit besser gerecht werden zu können.

Der erfreuliche und dringend erforderliche Personalzuwachs hat auf der anderen Seite zu enormen Raumproblemen geführt. Für die Dienststelle besteht ein erheblicher Flächenmehrbedarf, der im Dienstgebäude in der Friedrichstraße in Kreuzberg nicht realisiert werden kann. Ein Umzug der gesamten Dienststelle in größere Räumlichkeiten ist daher unabdingbar. Auf der Suche nach einem neuen Standort wurde uns von der Berliner Immobilienmanagement GmbH (BIM) im Frühjahr eine Liegenschaft in Alt-Moabit angeboten, die diese Vorgabe erfüllt. Nach einer umfangreichen Prüfung durch die BIM und die Senatsverwaltung für Finanzen, unter Zugrundelegung einer zuvor erstellten Bedarfsanalyse, erfolgte mit Beschluss des Hauptausschusses des Abgeordnetenhauses von Berlin im Dezember die Freigabe zur Anmietung des Objekts durch die BlnBDI. Aufgrund umfangreicher notwendiger Maßnahmen zur Herrichtung der Liegenschaft kann der Umzug in die neuen Räumlichkeiten jedoch leider erst im Sommer 2022 erfolgen. Um den aktuellen Bedarf an zusätzlichen Büroräumen decken zu können, mussten daher im November als Übergangslösung andere Räume angemietet werden. Die – wenn auch nur vorübergehende – Aufteilung auf zwei Standorte stellt für die gesamte Dienststelle eine zusätzliche organisatorische und logistische Herausforderung dar.

20.2 Aus der Arbeit der Servicestelle Bürgereingaben – Fallzahlen, Trends, Schwerpunkte

Die Bearbeitung von Bürger*innenbeschwerden ist nicht nur eine unserer arbeitsintensivsten, sondern auch eine unserer bedeutsamsten Aufgaben, da wir aus ihnen viele wertvolle Hinweise für unsere aufsichtsrechtliche Praxis erhalten. Erste Anlaufstelle für alle datenschutzrechtlichen Anfragen und Beschwerden von Bürger*innen ist die Servicestelle Bürgereingaben. Deren Mitarbeiter*innen nehmen Eingaben postalisch, per Fax, E-Mail oder über das elektronische Beschwerdeformular auf unserer Webseite entgegen, beantworten diese in den meisten Fällen direkt oder verteilen sie innerhalb der Dienststelle an die jeweiligen Fachreferate.

Seit Wirksamwerden der DS-GVO im Mai 2018 ist die Zahl der Bürgereingaben kontinuierlich gestiegen und verbleibt seitdem auf diesem sehr hohen Niveau: Jeden Monat gehen bei uns ca. 400 Eingaben ein. Trotz der Einschränkungen durch die Corona-Pandemie hat die Servicestelle Bürgereingaben ihre Aufgaben durchgängig erfüllt. Die Pandemie hat zu einigen inhaltlichen Schwerpunkten geführt, die immer wieder Gegenstand von Bürger*innenbeschwerden waren. Zahlreiche Beschwerden und Anfragen von Bürger*innen betrafen auch die Verlagerung vieler Lebensbereiche ins Digitale. Als Schwerpunkte kristallisierten sich hierbei die Situation von Beschäftigen in Unternehmen sowie die Lage in den Schulen heraus.[405] So gab es insbesondere in der ersten Jahreshälfte gehäuft Anfragen zu Datenschutz und IT-Sicherheit von spezifischen Videokonferenzsystemen.[406]

Viel Aufmerksamkeit verbuchten auch die Regeln zur Kontaktnachverfolgung. Im Rahmen der Infektionsschutzregelungen hat das Land Berlin das Friseurhandwerk, Gastronomiebetriebe sowie viele andere Stellen dazu verpflichtet, Informationen zur Kontaktnachverfolgung von Gästen oder Kundschaft zu erheben. Uns erreichten viele Anfragen zur generellen datenschutzrechtlichen Zulässigkeit der

405 Siehe 1.4
406 Siehe 1.3

Kontaktnachverfolgung und konkrete Beschwerden von Betroffenen über offen einsehbare Kontaktlisten in Gastronomiebetrieben und Geschäften.[407]

Ein Themenschwerpunkt außerhalb des Pandemiegeschehens lag im Bereich „Tracking", also der Nachverfolgung von Internetnutzer*innen, u.a. mittels sog. Cookies. Der Europäische Gerichtshof (EuGH) hatte bereits 2019 geurteilt, dass Besucher*innen einer Internetseite der Verwendung von Tracking-Cookies und anderen Tracking-Technologien selbst aktiv zustimmen müssen.[408] Viele Internetseiten bieten jedoch keine akzeptable Möglichkeit, Cookies zu deaktivieren. Dementsprechend haben auch die Beschwerden zu diesem Themenkomplex deutlich zugenommen.

Wie bereits in den Vorjahren betrifft ein Großteil der Beschwerden weiterhin die Durchsetzung von Betroffenenrechten, hier vor allem die Rechte auf Auskunft und auf Löschung der eigenen Daten. So beschwerten sich Bürger*innen vor allem über Unternehmen, die auf ihre diesbezüglichen Anfragen nur unzureichend oder gar nicht reagiert haben. Weitere Schwerpunkte lagen in den Bereichen Videoüberwachung und Wohnungswirtschaft.

20.3 Datenschutz und Medienkompetenz

Die BlnBDI hat sich zum Ziel gesetzt, die Medien- und Datenschutzkompetenz insbesondere von Grundschulkindern zu fördern. Im Rahmen unserer medienpädagogischen Arbeit haben wir daher nun auch erstmalig Projekttage an Grundschulen durchgeführt. Unser Angebot stieß auf großes Interesse und der steigende Bedarf an Schulungen und begleitendem Lehrmaterial ist nochmals deutlich geworden. Um weitere Workshops und Projekte an Schulen und in Bildungseinrichtungen in der Fläche durchführen zu können, wollen wir künftig dazu übergehen, auch Multiplikator*innen zu schulen.

407 Siehe 1.1.3

408 EuGH, Entscheidung vom 1. Oktober 2019 – C-673/17 („Planet49"); siehe auch JB 2019, 13.2

Die fortschreitende Digitalisierung erfordert gerade angesichts der Corona-Pandemie noch größere Anstrengungen in Bezug auf die datenschutzrechtliche Aufklärung von Kindern und Jugendlichen, aber auch Hilfestellung für Lehrpersonal und Eltern. Dazu werden wir unser medienpädagogisches Angebot stetig erweitern und umfangreiches Informations- und Unterrichtsmaterial anbieten.

Zudem bauen wir unser digitales Angebot unter www.data-kids.de kontinuierlich aus, erweitern das Themenspektrum und binden zunehmend auch audiovisuelle Medien und interaktive Spiele ein. Ergänzende Informationsmaterialien für Kinder, Lehrkräfte und Eltern stellen wir zum kostenlosen Download zur Verfügung.

20.4 Zusammenarbeit mit dem Abgeordnetenhaus von Berlin

Der Ausschuss für Kommunikationstechnologie und Datenschutz (KTDat) tagte in diesem Jahr insgesamt achtmal und setzte sich mit zahlreichen Themen rund um Digitalisierung und Datenschutz auseinander. Die BlnBDI hat an allen Sitzungen teilgenommen und stand dem Ausschuss beratend zur Seite. Wichtige Besprechungspunkte waren u.a. die Digitalisierung der Schulen,[409] das Berliner Onlinezugangsgesetz[410] und die Einführung der elektronischen Gesundheitsakte[411]. Von großer Bedeutung waren auch die Beratungen zum Berliner Datenschutz-Anpassungsgesetz EU, mit dem das Landesrecht an die Vorgaben der DS-GVO angepasst wurde.[412] Die BlnBDI hat diesen Anpassungsprozess, soweit es ihr möglich war, begleitet und sich insbesondere für die Beseitigung von Regelungsmängeln aus dem alten Berliner Datenschutzgesetz (BlnDSG) eingesetzt. Mit der Verabschiedung des betreffenden Gesetzes wurden jedoch leider nicht alle angemahnten rechtlichen Defizite behoben. Wir hoffen sehr, dass dies im Rahmen der angekündigten Evaluierung des neuen BlnDSG nachgeholt wird.[413]

409 Siehe 1.4

410 Siehe 2.1

411 Siehe 5.3

412 Siehe 1.4

413 Siehe Pressemitteilung vom 2. Oktober 2020: „Anpassung des Berliner Datenschutzrechts – es gibt noch einiges zu tun"; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen

20.5 Zusammenarbeit mit anderen Stellen

Die **Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)** stand in diesem Jahr unter dem Vorsitz von Sachsen. Sie tagte am 12. Mai und am 25./26. November jeweils virtuell. Bei der Konferenz im November handelte es sich um eine Jubiläumssitzung, bei der die DSK sich zum 100. Mal seit ihrem Bestehen getroffen hat – leider den Umständen entsprechend ebenfalls nur digital. Daneben fanden noch drei Zwischenkonferenzen jeweils als Videokonferenzen am 29. Januar, 16. Juni und 22. September statt. Die DSK fasste während ihrer Sitzungen zahlreiche Entschließungen und Beschlüsse zu aktuellen datenschutzrechtlichen Fragen,[414] u.a. zum Einsatz von Google Analytics, zur Verwendung von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie und zum Einsatz von Windows 10 Enterprise. Die BlnBDI hat darüber hinaus am 13./14. Oktober am Arbeitskreis der DSK „DSK 2.0" teilgenommen, der sich mit der strategischen Neuausrichtung der DSK befasst und daran arbeitet, Entscheidungsprozesse innerhalb der DSK und ihre Arbeitsweise insgesamt zu optimieren.

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)** tagte unter dem Vorsitz von Hessen am 3. Juni und 1. Dezember jeweils als Videokonferenz. Entschließungen hat das Gremium diesmal nicht gefasst; es erfolgte ein allgemeiner Erfahrungsaustausch zum Informationszugang auf kommunaler Ebene. Zusätzlich haben Vertreter des Regierungspräsidiums Darmstadt als Gäste interessante Einblicke in die Verwaltungspraxis im Umweltinformationsrecht sowie im Verbraucherinformationsrecht betreffend Lebensmittel gegeben. Die IFK hat sich vorgenommen, einen Mechanismus zu entwickeln, anhand dessen informationspflichtige Stellen sich im Hinblick auf die Einhaltung und effiziente Umsetzung des Informationszugangsrechts selbst überprüfen, also ein „Self-Audit" durchführen können.

Die Global Privacy Assembly (GPA)[415] fand als dreitägige Videokonferenz vom 13. bis 15. Oktober statt. Im Vordergrund der Konferenz stand die zukünftige strate-

414 Alle Entschließungen und Beschlüsse der DSK sind auf unserer Webseite unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk abrufbar.

415 Ehemals International Conference of Data Protection and Privacy Commissioners

gische Ausrichtung der Konferenz. Einen weiteren Schwerpunkt der Veranstaltung bildeten die Herausforderungen für den Datenschutz im Rahmen der Covid-19-Pandemie. Die GPA nahm zahlreiche Berichte und Entschließungen an,[416] u.a. zum transparenten und diskriminierungsfreien Einsatz von künstlicher Intelligenz.

Pandemiebedingt tagte **die Internationale Arbeitsgruppe für Datenschutz in der Technologie (Berlin-Group – IWGDPT),** deren Vorsitz die BlnBDI innehat, in diesem Jahr nicht. Stattdessen wurde die laufende Arbeit an Arbeitspapieren zu den Themen Web Tracking, Datenübertragbarkeit, Sensor Networks und Spracherkennungssoftware in einem schriftlichen Verfahren fortgeführt. Eine Veröffentlichung ist für das Jahr 2021 vorgesehen.

20.6 Pressearbeit

Das mediale Interesse an der Arbeit unserer Behörde war, wie auch in den Vorjahren, sehr hoch. In diesem Jahr beantworteten wir über 200 Presseanfragen. Auch in der Pressestelle dominierten Themen zum Datenschutz während der Corona-Pandemie unsere Arbeit. Mit Abstand die meisten Fragen erreichten uns zur Kontaktdatenerhebung durch Restaurants und andere Betriebe.[417] Als konkrete Hilfestellung veröffentlichten wir Musterformulare für Verantwortliche, damit diese ihrer Pflicht zur Erhebung von Kontaktdaten datenschutzgerecht nachgehen konnten. Des Weiteren nahm das Thema Digitalisierung der Schulen bei unserer Pressearbeit sehr viel Raum ein.[418] Insbesondere unsere Einschätzung zum Lernraum Berlin war Gegenstand diverser Interviews und Anfragen. Enormes überregionales mediales Interesse im Zusammenhang mit der Pandemie erzeugten außerdem unsere Hinweise und Prüfergebnisse zum datenschutzkonformen Einsatz von Videokonferenzdiensten. Per Ampelsystem bewertet diese Veröffentlichung in anschaulicher Weise, ob und inwieweit Verantwortliche unter rechtlichen und

416 Alle Entschließungen und Berichte der GPA sind auf der Webseite der GPA unter https://globalprivacyassembly.org/document-archive/adopted-resolutions/ und https://globalprivacyassembly.org/document-archive/working-group-reports/ abrufbar.

417 Siehe 1.1.3

418 Siehe 1.4

technischen Gesichtspunkten gängige Videokonferenzdienste datenschutzgerecht einsetzen können.[419]

Abgesehen von Fragen zum Datenschutz während der Corona-Pandemie waren der Emotet-Befall beim Kammergericht sowie der Einsatz der Personalsoftware Zonar durch das Unternehmen Zalando wichtige Themen, zu denen uns eine Vielzahl von Presseanfragen erreichten. Unsere Pressestelle stand Journalistinnen und Journalisten zu diesen und diversen anderen Themen als Kontakt zur Verfügung, damit die teils schwierigen datenschutzrechtlichen und -technischen Fragen in der Medienberichterstattung verständlich und richtig dargestellt werden konnten.

Mit insgesamt 14 Pressemitteilungen wandte sich die BlnBDI u.a. auch mit eigenen Themen an die Öffentlichkeit. Wir thematisierten z. B. problematische Entwicklungen im Bereich der Gesetzgebung. So wiesen wir bspw. auf Regelungsmängel beim Berliner Datenschutz-Anpassungsgesetz EU oder bei den vom Senat veröffentlichten Eckpunkten zum geplanten Berliner Transparenzgesetz hin.[420] Zudem nutzten wir das Instrument Pressemitteilung, um eigene Veröffentlichungen, wie etwa einen Ratgeber für Smartphone-Sicherheit, die Ergebnisse unserer Prüfung von Videokonferenzdiensten oder unsere Hilfestellungen zur Digitalisierung der Schule publik zu machen. Außerdem informierten wir auf diesem Wege über wichtige aktuelle Entwicklungen wie z. B. das sog. „Schrems II"-Urteil des Europäischen Gerichtshofs und bezogen dabei immer eine klare Position.[421]

Folgende Pressemitteilungen haben wir in diesem Jahr veröffentlicht:

- BlnBDI begrüßt Beschluss der Europäischen Leitlinie zur Videoüberwachung (30. Januar 2020)
- BlnBDI zur Datenpanne bei der Investitionsbank Berlin (30. März 2020)
- Jahresbericht 2019 (3. April 2020)
- Lehren aus der Krise ziehen (4. Mai 2020)

419 Siehe 1.3
420 Siehe 17.1 und 19.2
421 Siehe 1.2

- Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen (25. Mai 2020)
- Ratgeber zu Smartphone-Sicherheit für Jugendliche veröffentlicht (9. Juni 2020)
- Kontaktdatenerhebung durch Gewerbetreibende – Musterformulare der BlnBDI (24. Juni 2020)
- Kurzprüfung von Videokonferenzdiensten – BlnBDI veröffentlicht Ergebnisse (3. Juli 2020)
- Nach „Schrems II": Europa braucht digitale Eigenständigkeit (17. Juli 2020)
- Berliner Polizei verweigert Aufklärung von fragwürdigen Abfragen in Polizeidatenbanken (13. August 2020)
- Datenschutz in der Kita – BlnBDI veröffentlicht neue Broschüre (17. August 2020)
- BlnBDI zu den Eckpunkten für ein Transparenzgesetz (3. September 2020)
- Berliner Datenschutz-Anpassungsgesetz – Regelungsmängel bestehen fort (2. Oktober 2020)
- Datenschutz ist kein Hindernis für digitalen Unterricht (4. Dezember 2020)

Alle Pressemitteilungen sind auf unserer Webseite unter https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen abrufbar. Mit einer E-Mail an die Adresse presse@datenschutz-berlin.de ist eine Aufnahme in unseren Presseverteiler möglich.

20.7 Öffentlichkeitsarbeit

20.7.1 Veranstaltungen und Vorträge

Die diesjährige zentrale Veranstaltung anlässlich des 14. Europäischen Datenschutztages fand auf Einladung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) am 28. Januar in Berlin, in der Vertretung der Europäischen Kommission in Deutschland statt. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, DSK-Vorsitzender des Vorjahres, hat diese Veranstaltung organisiert. Das Thema

lautete „Künstliche Intelligenz – zwischen Bändigung und Förderung". Zur Bedeutung von KI-Lösungen und Algorithmen in Wirtschaft und Technik und den damit verbundenen Herausforderungen referierten Vertreter*innen aus Politik, Wissenschaft, Justiz und Praxis.

Viele weitere geplante Veranstaltungen wurden aufgrund der Corona-Pandemie und des über Monate dauernden Lockdowns entweder abgesagt oder fanden im kleineren Rahmen statt. Manches wurde in digitalisierter Form durchgeführt. Unter den veränderten Bedingungen war es uns nicht mehr in allen Fällen möglich, an Veranstaltungen teilzunehmen.

Auch die Vortragstätigkeit war unter den neuen Bedingungen erst einmal deutlich eingeschränkt. Nach einer Vorbereitungsphase fand die gewohnt rege Kommunikation der nationalen und internationalen Fachgremien, Arbeitsgruppen und Arbeitskreise allerdings weiter statt. Auch die Teilnahme an Fachgesprächen, Kongressen und Workshops wurde wieder verstärkt möglich. Die Veranstaltungen haben größtenteils im Rahmen von Videokonferenzen stattgefunden.

Einige Beispiele seien hier genannt:

- Vortrag „Ist der Betriebsrat ein eigener Verantwortlicher?" für den GDD-Winterworkshop (vom GDD e. V., Gesellschaft für Datenschutz und Datensicherheit e. V) am 27. Januar 2020 in Garmisch-Partenkirchen; Online-Vortrag „Datenschutz & Personalrat/Betriebsrat" beim Workshop für den BvD e. V. (Bundesverband der Datenschutzbeauftragten e. V.) am 5. Mai 2020. Im Rahmen dieser Vorträge wurde die Frage erörtert, ob eine Beschäftigtenvertretung für ihre eigene Datenverarbeitung verantwortlich ist oder das jeweilige Unternehmen. Wir gehen davon aus, dass das Unternehmen verantwortlich ist;

- Gespräch mit Leiterinnen und Leitern des Rechtsstaatsprogramms der Konrad-Adenauer-Stiftung zum Thema „Der digitale Staat. Einsatz von KI – Fluch oder Segen? Gezielte Nutzung digitaler Mittel zur Einschränkung von Freiheitsrechten" am 11. Februar in Berlin;

- Vortrag zu "Enforcement of the GDPR in Berlin/Germany in Practice" am 25. Mai 2020 im Rahmen der Online-Konferenz „GDPR Day 2020". Bei dem „GDPR

Day 2020“ handelte es sich um eine unabhängig organisierte Konferenz im Zusammenhang mit der Umsetzung der DS-GVO in den GUS-Ländern (Russland, Belarus, Ukraine), die Spezialisten aus diesen Ländern zusammengebracht hat;

- Vortrag im Rahmen des „Interactive Roundtable“ bei der Bitkom Privacy Conference 2020 am 29. September 2020 zu „Hinweisen für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten“, die unsere Behörde als Ergebnis einer Kurzprüfung der Videokonferenzsysteme veröffentlicht hat. Dazu haben wir grundlegende Anforderungen und Empfehlungen sowie eine Checkliste für die Durchführung von datenschutzgerechten virtuellen Konferenzen formuliert. Darüber hinaus gab es Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenz-Diensten.[422]

- Vortrag zum Thema “Big brother, privacy and public health – Effective enforcement of data protection regulation in times of COVID-19” am 12. November 2020 im Rahmen des (digitalen) deutsch-brasilianischen Demokratieforums der Deutschen Botschaft Brasilia. Brasilien ist derzeit mit der Ausgestaltung der Datenschutzaufsicht befasst und war in diesem Zusammenhang an unseren Erfahrungen interessiert.

20.7.2 Veröffentlichungen

Ein wichtiger Teil der Öffentlichkeitsarbeit unserer Behörde sind die Publikationen. Die Infothek auf unserer Webseite enthält vielfältige Informationsmaterialien, die digital abgerufen und zum Teil als gedruckte Ausgabe kostenfrei bestellt werden können. Das Angebot wird beständig ausgebaut und aktualisiert, so auch in diesem Jahr.

Neben dem Tätigkeitsbericht des vergangenen Berichtszeitraums haben wir drei Ratgeber für den Datenschutz umfangreich überarbeitet, ergänzt und im neuen Design drucken lassen:

422 Siehe auch 1.3

- Der in der Vergangenheit stark nachgefragte **Ratgeber „Wie sicher ist dein Smartphone?“** wurde erstmalig im Jahr 2008 veröffentlicht und ist nun in der 3., aktualisierten und ergänzten Auflage erschienen. Für die Neuauflage war es uns besonders wichtig, junge Menschen nicht nur für die bekannten Gefahren wie Smartphone-Viren, Spionage und Datenklau zu sensibilisieren, sondern ihnen auch konkrete Tipps zu geben, mit welchen Vorkehrungen sie sich bestmöglich schützen können.

- Der **Ratgeber „Auskunfteien“** aus dem Jahr 2001 wurde in der Vergangenheit bereits mehrmals grundlegend überarbeitet. In der seit dem Frühjahr vorliegenden Ausgabe ist der Text an die neue Rechtslage (DS-GVO) angepasst und neu aufgelegt worden. In dem Ratgeber wird in kurzen übersichtlichen Kapiteln u.a. über die Tätigkeit der Auskunfteien informiert, es werden die Anforderungen an die Datenverarbeitung durch Auskunfteien formuliert und das Auskunftsrecht sowie weitere Betroffenenrechte detailliert beschrieben.

- Auch der **Ratgeber „Umgang mit Passwörtern“** aus dem Jahr 2000 erschien dieses Jahr in einer weiteren aktualisierten und neu strukturierten Ausgabe. Bei der zunehmenden Nutzung von Online-Diensten ist es besonders wichtig, die Nutzenden auf eine stärkere Absicherung der Daten hinzuweisen. Was ist ein Passwortmanager? Wie erfolgt die Authentifizierung einer Person? Welche Möglichkeiten gibt es für eine Mehrfaktor-Authentifizierung? Welche Anforderungen an ein sicheres Passwort sollten beachtet werden? – In der Broschüre werden diese und andere Fragen beantwortet und Hilfestellungen angeboten.

Außerdem ist die 2018 herausgegebene **Broschüre „Datenschutz bei Bild-, Ton- und Videoaufnahmen. Was ist in der Kindertageseinrichtung zu beachten?“** rechtzeitig vor Beginn des neuen Kitajahres nach der Sommerpause in der 2. Auflage erschienen. Mit der neu überarbeiteten Broschüre informieren die Senatsverwaltung für Bildung, Jugend und Familie und die Berliner Beauftragte für Datenschutz und Informationsfreiheit umfassend über die aktuellen rechtlichen Vorgaben. Die vor allem an Träger, Kita-Leitungen und pädagogische Fachkräfte gerichtete Broschüre wurde bereits allen 2.700 Berliner Kitas zur Verfügung gestellt.[423]

423 Siehe auch 4.2

In unserem Internetangebot finden Betroffene sowie interessierte Bürgerinnen und Bürger auch Tipps zum **„Selbstdatenschutz"**. Hier zeigen wir ihnen, wie man Datenspuren im Internet vermeiden kann, was sichere Passwörter ausmacht oder wie man sicher drahtlose Netzwerke (WLANs) nutzt. Zudem bieten wir Hilfen zur Geltendmachung der eigenen Datenschutzrechte, z. B. **Musterschreiben** zum Versand an datenverarbeitende Stellen. Mit diesen Schreiben können sich Betroffene an Berliner Behörden und andere Stellen wenden, um Auskunft über die zur eigenen Person gespeicherten Daten zu bekommen, sie gegebenenfalls berichtigen oder unzulässig gespeicherte Daten löschen zu lassen. Derzeit bieten wir Musterschreiben für die Bereiche Ordnungsaufgaben, Innere Sicherheit, Adressenhandel und Werbung, SCHUFA und Telekommunikation an.[424]

Neben den eigenen Publikationen stellen wir auf unserer Webseite auch Informationen zur intensiven Zusammenarbeit mit den Kolleginnen und Kollegen aus anderen Bundesländern und deren Ergebnisse zur Verfügung:

- **Die Beschlüsse der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK):** Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder treffen sich regelmäßig zweimal im Jahr unter dem jährlich wechselnden Vorsitz einer oder eines Datenschutzbeauftragten zu ihren Datenschutzkonferenzen. Die Ergebnisse dieser Treffen werden der Öffentlichkeit als Konferenzbeschlüsse oder -entschließungen bekannt gegeben. Diese Dokumente der DSK seit 2005 wie auch die gemeinsam herausgegebenen Papiere für die Praxis des Datenschutzes in verschiedenen Sachgebieten (Kurzpapiere, Orientierungshilfen und Anwendungshinweise) stehen allen Interessierten in unserer Infothek zur Verfügung.

- In gleicher Weise veröffentlichen wir die **Leitlinien des Europäischen Datenschutzausschusses (EDSA)**. Der EDSA ist eine unabhängige europäische Einrichtung, die mit Wirksamwerden der DS-GVO eingerichtet wurde, um Zweifelsfragen in der Auslegung der DS-GVO zu klären und so die einheitliche Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union sicherzustellen. Er setzt sich zusammen aus Repräsentant*innen der nationa-

424 Siehe https://www.datenschutz-berlin.de/buergerinnen-und-buerger/selbstdatenschutz/datencheck

len Datenschutzaufsichtsbehörden und dem Europäischen Datenschutzbeauftragten. Der EDSA gibt regelmäßig Leitlinien zu zentralen Themen der DS-GVO heraus. Alle Dokumente werden sukzessive ins Deutsche übersetzt. Soweit sie bereits in die deutsche Sprache übersetzt wurden, können diese auf unserer Seite heruntergeladen werden.

20.7.3 Ausblick

Durch den Stellenzuwachs für den Doppelhaushalt 2020/2021 konnte die dringend notwendige Neustrukturierung des Bereichs Öffentlichkeitsarbeit in unserer Behörde vollzogen werden. Seit September gibt es das neu geschaffene Referat „Gremien-, Presse- und Öffentlichkeitsarbeit", welches direkt bei der Dienststellenleitung angesiedelt ist.[425] Die einzelnen Arbeitsbereiche können nun besser aufeinander abgestimmt werden. Insbesondere haben wir jetzt eine definierte Zuständigkeit für die Betreuung der diversen Gremien und die Koordinierung der zahllosen Abstimmungsverfahren, die seit Wirksamwerden der DS-GVO in extremer Weise zugenommen haben.

Um eine möglichst breite Öffentlichkeit für die Themen Datenschutz und Informationsfreiheit sensibilisieren zu können, werden wir neben der stetigen Erweiterung unserer Publikationen insbesondere unsere digitalen Angebote weiter ausbauen. Zudem soll sowohl der Austausch mit Politik und Medien als auch mit Bürgerinnen und Bürgern intensiviert und gefördert werden.

In den kommenden Jahren werden wir auch die Netzwerkarbeit auf allen Ebenen verstärken und Kooperationen bspw. mit zivilgesellschaftlichen Akteur*innen, wissenschaftlichen Institutionen, Schulen und Bildungsträger*innen ausbauen sowie neue Veranstaltungsformate umsetzen.

425 Siehe auch 20.1

21 Statistik für den Jahresbericht

Sowohl bei den eingereichten Beschwerden als auch bei den gemeldeten Datenpannen bleibt die Anzahl der bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) eingegangenen Fälle auf einem sehr hohen Niveau. Damit setzt sich der Trend der vergangenen zwei Jahre fort. Dies wird besonders im Vergleich zur Anzahl der Fälle vor Geltung der Datenschutz-Grundverordnung (DS-GVO) deutlich.

Die Darstellung des folgenden Kapitels orientiert sich an den einheitlichen Kriterien, die die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beschlossen hat. Zudem kommt die BlnBDI damit ihren Berichtspflichten aus der DS-GVO und dem Bundesdatenschutzgesetz (BDSG) nach. Hierbei ist jedoch zu beachten, dass aufgrund der Corona-Pandemie und den dadurch erschwerten Arbeitsbedingungen noch nicht alle Vorgänge abschließend statistisch erfasst sind. Die hier angegebenen Zahlen stehen demnach unter Vorbehalt.

21.1 Beschwerden

Die BlnBDI erreichten im Jahr 2020 4.868 Eingaben von Betroffenen, von welchen 2.430 als förmliche Beschwerden im Sinne der DS-GVO zu behandeln waren.[426] Für den Großteil der Beschwerden eröffnete die BlnBDI Verfahren in eigener Zuständigkeit. Insgesamt waren das in diesem Jahr 1.909 Verfahren. Davon richteten sich mehr als 80 % gegen private Stellen (1.656), der Rest gegen Behörden (253). In 521 Fällen lagen die Beschwerden nicht im Zuständigkeitsbereich der BlnBDI, bspw. weil die Verantwortlichen ihren deutschen Hauptsitz in einem anderen Bundesland hatten. Diese Beschwerden gab die BlnBDI an die zuständigen Kolleg*innen in den anderen Bundesländern oder an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ab.

426 Siehe Art. 77 DS-GVO

Damit bleibt die Zahl der bei der BlnBDI eingereichten Beschwerden seit Geltung der DS-GVO auf vergleichbar hohem Niveau. Die nachfolgende Grafik gibt einen Überblick über die Anzahl der bei der BlnBDI eingereichten Beschwerden von Betroffenen gegenüber öffentlichen und nicht öffentlichen Stellen sowie über Abgaben an andere deutsche Aufsichtsbehörden seit 2017.

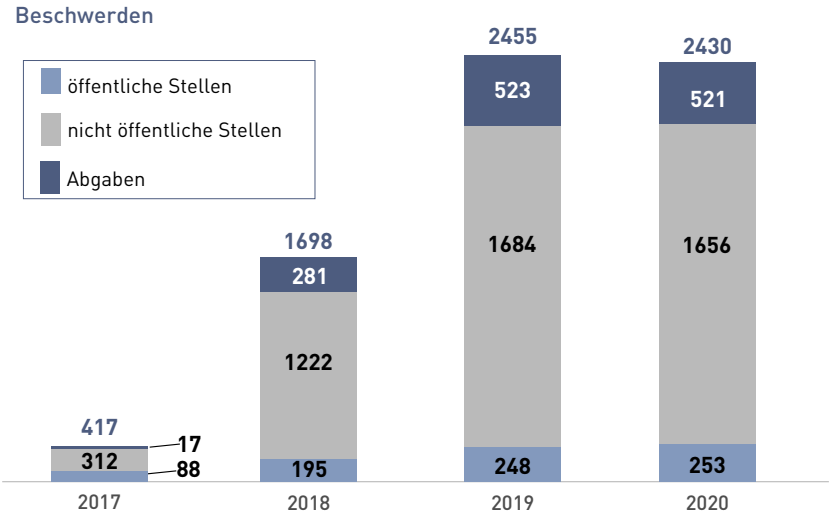

Abbildung 3: Beschwerden 2017–2020

21.2 Beratungen

Mit dem Begriff Beratungen werden alle schriftlichen datenschutzrechtlichen Auskünfte gegenüber Verantwortlichen, betroffenen Personen und der öffentlichen Verwaltung beschrieben. Der Schwerpunkt lag hierbei in der Beratung betroffener Personen, also Bürger*innen, mit 2.438 Fällen. Daneben beriet die BlnBDI zahlreiche Verantwortliche. Hinzu kommt eine Vielzahl telefonischer Auskünfte, die nicht statistisch erfasst werden.

Aufgrund der Corona-Pandemie konnten leider weniger statistisch erfasste Beratungen von Verantwortlichen stattfinden.

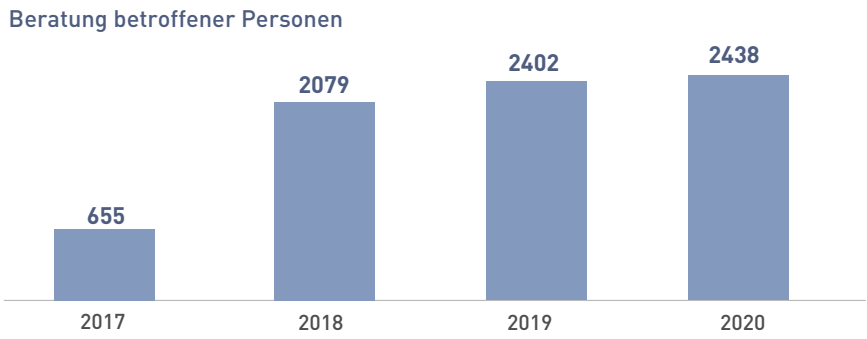

Abbildung 4: Beratungen betroffener Personen

21.3 Datenpannen

Auch im Jahr 2020 haben Verantwortliche bei der BlnBDI wieder sehr viele Datenpannen gemeldet. Wie bereits in früheren Jahresberichten erläutert, liegt das an den in der DS-GVO deutlich verschärften Melde- und Informationspflichten.[427] Im Berichtszeitraum gab es insgesamt 925 Meldungen von Verantwortlichen. Davon entfielen 821 auf den nicht öffentlichen Bereich, d. h. vor allem auf private Unternehmen. Öffentliche Stellen meldeten uns 104 Datenpannen.

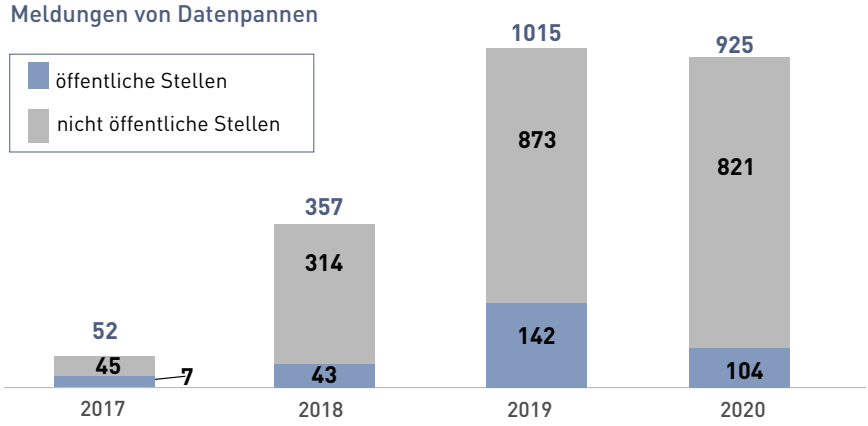

Abbildung 5: Meldungen von Datenpannen

427 JB 2018, 1.3; JB 2019, 15.1

21.4 Abhilfemaßnahmen

Stellt die BlnBDI einen Verstoß gegen die DS-GVO durch Verantwortliche fest, kann sie verschiedene Abhilfemaßnahmen ergreifen.[428] Im Jahr 2020 hat die BlnBDI zwei Warnungen und 308 Verwarnungen ausgesprochen. Von der Möglichkeit, Zertifizierungen zu widerrufen oder eine Anordnung zu erlassen, wurde im Berichtszeitraum kein Gebrauch gemacht. In 47 Fällen hat die BlnBDI Geldbußen verhängt. Zum Ende des Berichtszeitraums waren die entsprechenden Verfahren jedoch noch nicht alle rechtskräftig abgeschlossen.

Zusätzlich zu den hier genannten Fällen wurde im Berichtszeitraum eine größere Anzahl weiterer Verfahren eröffnet, in denen noch kein Bescheid ergangen ist.

Abhilfemaßnahmen 2020	
Warnungen	2
Verwarnungen	308
Anweisungen und Anordnungen	0
Widerruf von Zertifizierungen	0

Tabelle 1: Abhilfemaßnahmen

21.5 Förmliche Begleitung bei Rechtssetzungsvorhaben

Die BlnBDI hat nach dem Berliner Datenschutzgesetz unter anderem die Aufgabe, das Abgeordnetenhaus, den Senat und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen datenschutzrechtlich zu beraten. Dazu gehören sowohl schriftliche Stellungnahmen als auch Besprechungen mit Fraktionen und Abgeordneten sowie förmliche Anhörungen im Abgeordnetenhaus und in dessen Ausschüssen.

428 Siehe Art. 58 Abs. 2 DS-GVO

Im Berichtszeitraum haben wir bei 33 Gesetzgebungsvorhaben beraten, wie z. B. bei Änderungen des Polizeigesetzes[429] und des Landeskrankenhausgesetzes[430] oder bei der Schaffung gesetzlicher Grundlagen für eine*n Bürger*innen- und Polizeibeauftragte*n[431]. Diese Gesetzgebungsprojekte waren teilweise sehr umfangreich und umfassten mitunter Änderungen zahlreicher Einzelgesetze, wie z. B. das Berliner Datenschutz-Anpassungsgesetz EU, mit dem allein ca. 80 Gesetze an die DS-GVO angepasst wurden.[432]

Hinzu kamen 12 Beratungen bei Rechtsetzungsvorhaben, die die Schaffung und Änderung von Rechtsverordnungen und Verwaltungsvorschriften zum Gegenstand hatten. Auch bei Projekten der Bundesgesetzgebung nahmen wir wiederholt gemeinsam mit den anderen Datenschutzbehörden des Bundes und der Länder Stellung, wenn diese so wichtige Vorhaben wie z. B. die Evaluierung des Bundesdatenschutzgesetzes betrafen.

21.6 Europäische Verfahren

Die DS-GVO sieht vor, dass die europäischen Datenschutzaufsichtsbehörden bei grenzüberschreitenden Fällen zusammenarbeiten.[433] Im Rahmen des Kooperationsverfahrens wird dazu eine federführende Aufsichtsbehörde bestimmt, die die Ermittlungen in dem jeweiligen Fall führt.[434] Weitere Datenschutzaufsichtsbehörden können sich als betroffene Behörden melden, wenn der Verantwortliche eine Niederlassung in ihrem Land hat oder die Verarbeitung erhebliche Auswirkungen auf betroffene Personen in dem jeweiligen Land hat. Dabei kooperieren die jeweiligen Aufsichtsbehörden eng miteinander.[435]

429 Siehe 3.2
430 Siehe 5.1
431 Siehe 3.3
432 Siehe 17.1
433 Siehe JB 2018, 1.1
434 Siehe Art. 56 Abs. 1 DS-GVO
435 Siehe Art. 60 Abs. 1 bis 3 Satz 1 und Art. 61, 62 DS-GVO

Nach Abschluss der Ermittlungen legt die federführende Aufsichtsbehörde den betroffenen Aufsichtsbehörden einen Beschlussentwurf zur Stellungnahme vor.[436] Insgesamt veröffentlichte unsere Behörde in diesem Jahr 24 Beschlussentwürfe und 20 endgültige Beschlüsse. Zur Abstimmung und Kooperation nutzen die europäischen Datenschutzaufsichtsbehörden das elektronische Binnenmarkt-Informationssystem (IMI).

Die nachfolgende Tabelle gibt einen Überblick über die Beteiligung der BlnBDI an den wichtigsten dieser europäischen Verfahren.[437]

Europäische Verfahren	
Art. 56-Verfahren (betroffen)	388
Art. 56-Verfahren (federführend)	29
Art. 60ff.-Verfahren	44

Tabelle 2: Europäische Verfahren

436 Siehe Art. 60 Abs. 3 Satz 2 DS-GVO

437 Für weitere Informationen und Zahlen zu europäischen Kooperationsverfahren siehe 17.2

Anhang

Rede der Berliner Beauftragten für Datenschutz und Informationsfreiheit, Maja Smoltczyk, zu der Stellungnahme des Senats zum Jahresbericht 2018 vor dem Abgeordnetenhaus von Berlin am 1. Oktober 2020

Sehr geehrter Herr Präsident,
meine sehr verehrten Damen und Herren,

wir sprechen heute über meinen Jahresbericht für das Jahr 2018 – ein bisschen später als sonst, aber insofern passend, als Sie nachher auch noch über das Datenschutz-Anpassungsgesetz EU zu entscheiden haben, das heute ebenfalls auf der Tagesordnung steht – und beide Tagesordnungspunkte verbindet, dass sie von demselben Ereignis im Jahr 2018 bestimmt sind.

Denn 2018 war das Jahr, in dem die Datenschutz-Grundverordnung wirksam wurde und enorme Herausforderungen für jeden von uns mit sich gebracht hat. Doch trotz aller Herausforderungen kann man nicht oft genug darauf hinweisen, dass es sich bei diesem europäischen Gesetzesprojekt um einen Meilenstein handelt in einer Zeit der immer schneller werdenden globalen Digitalisierung, in der grundlegende europäische Bürger*innenrechte nur dann bewahrt werden können, wenn man sich auf europäischer Ebene zusammenschließt. Es ist ein Projekt, auf das wir als Europäer*innen stolz sein können – und für das wir im Übrigen international bewundert werden.

Meine Behörde hatte sich gut auf diese Zäsur vorbereitet, wurde aber von der Zunahme der Eingaben und Meldungen von Datenpannen geradezu überrollt. Mit Wirksamwerden der Datenschutz-Grundverordnung im Mai 2018 kam es zu einer Verdrei- bis -vierfachung des Beschwerdeaufkommens, die sich bis heute auf dem dreifachen Niveau eingependelt hat. Auch die Anzahl der gemeldeten Datenpannen und die Menge an Beratungsanfragen vervielfachten sich und sind auf hohem Niveau verharrt.

Gleichzeitig stiegen auch die fachlichen Anforderungen an meine Mitarbeiterinnen und Mitarbeiter extrem an, da unsere Arbeit sich nunmehr zu einem großen Teil im europäischen Raum abspielt in enger Zusammenarbeit mit den übrigen EU-Aufsichtsbehörden. Und dies alles bei zunächst im Jahr 2018 nur unwesentlich aufgestocktem Personal.

Aber wir konnten feststellen, dass meine Behörde inhaltlich sehr gut vorbereitet war. Um für diesen Tag gewappnet zu sein, hatten wir vorab die Struktur unserer Behörde und unsere Arbeitsweisen grundlegend überdacht und neu gestaltet sowie gemeinsam mit den anderen deutschen und den europäischen Aufsichtsbehörden völlig neue Verfahren der Zusammenarbeit entwickelt. Und wir haben alles in unserer Kraft Stehende getan, um Unternehmen und Behörden zu beraten und bei der Umstellung auf die Verordnung zu begleiten.

Dennoch stellte die Umsetzung der Datenschutz-Grundverordnung einen riesigen Kraftakt für mein Haus dar. Es war nicht nur die Menge an Anfragen, die bewältigt werden musste, hinzu kam, dass die Fälle im Jahr 2018 teils nach „altem“ und teils nach „neuem“ Recht zu bewerten waren. Mit den neuen Sanktionsregeln haben wir zudem Befugnisse bekommen, mit denen wir Verstöße gegen den Datenschutz nun zumindest im privatwirtschaftlichen Raum wirkungsvoll ahnden können. Auch die Nutzung dieser neuen Sanktionsinstrumente stellt sehr hohe Anforderungen an meine Behörde.

Ich habe das große Glück, hochmotivierte Expert*innen an meiner Seite zu haben, die ihre Arbeit mit viel Engagement verrichten. Für diesen Einsatz möchte ich mich bei meinen Mitarbeiterinnen und Mitarbeitern sehr herzlich bedanken! – Danken möchte ich an dieser Stelle aber auch Ihnen, die Sie mit dem letzten Doppelhaushalt für eine personelle Verstärkung meines Hauses ab 2020 gesorgt haben, die es uns ermöglicht, den gestiegenen Anforderungen immer besser gerecht zu werden.

Inhaltlich hat uns im Jahr 2018 wieder ein bunter Strauß von Themen beschäftigt: Die Themen reichten vom unzulässigen Austausch von Sozialdaten, der fehlenden Löschung von Daten im Klinischen Krebsregister und in Berliner Krankenhäusern, über Video- und Audioaufzeichnungen im Unterricht, der Speicherung von Daten bei Lieferdiensten bis hin zum Scoring von Richter*innen und zur elektro-

nischen Gesundheitsakte. Viel Raum haben die Datenschutzrechte von Kindern eingenommen.

Gerade im Bereich der Kitas war aufgrund des neuen europäischen Rechts die Unsicherheit zum datenschutzgerechten Umgang mit personenbezogenen Daten groß.

Und einige der Themen beschäftigen uns bis heute:

Eines davon war das Urteil des Europäischen Gerichtshofs zu den Facebook Fanpages, mit der das Gericht festgestellt hat, dass auch die Fanpage-Betreibenden gemeinsam mit Facebook eine datenschutzrechtliche Verantwortung für die auf ihren Seiten verarbeiteten Daten ihrer Besucher*innen tragen. Dies betrifft viele Verantwortliche in dieser Stadt unmittelbar.

Ein anderes Thema waren die Speicherpraxis der Berliner Polizei und die missbräuchlichen Zugriffe auf die Polizeidatenbank POLIKS.

Ein Thema, das mir seit Beginn meiner Amtszeit sehr am Herzen liegt, ist die Stärkung der Datenschutzkompetenz von Kindern und Jugendlichen. Mit unserer Kinderwebseite www.data-kids.de haben wir im Frühjahr 2018 ein Angebot gestartet, das auf großen Zuspruch von Kindern, Lehrkräften und Eltern trifft und für das wir sogar für den deutschen Kindersoftwarepreis TOMMI nominiert wurden.

Im Bereich der Informationsfreiheit hat mich vor allem ein Thema umgetrieben, das uns sicher noch viele Jahre begleiten wird: Die Digitalisierung der öffentlichen Verwaltung. Immer öfter werden automatisierte Entscheidungen mithilfe von Algorithmen und Künstlicher Intelligenz getroffen – und das weitgehend intransparent. Eine Verwaltungsentscheidung muss jedoch immer überprüfbar und daher nachvollziehbar, kontrollierbar und verständlich sein. Die Konferenz der Informationsfreiheitsbeauftragten von Bund und Ländern hat hierzu ein wegweisendes Positionspapier beschlossen, das in gekürzter Fassung später auch von der Internationalen Konferenz der Informationsfreiheitsbeauftragten verabschiedet wurde.

Erlauben Sie mir abschließend noch einen kurzen Ausblick auf das Datenschutz-Anpassungsgesetz EU, das heute ebenfalls auf der Tagesordnung steht.

Ich beschränke mich hier ausdrücklich auf die Punkte, die Bezug zu meinem Jahresbericht haben. – Es ist gut, dass endlich – zwei Jahre nach Wirksamwerden der Datenschutz-Grundverordnung – die Anpassung des Berliner Landesrechts an das europäische Recht vorgenommen wird. Leider aber gibt es wichtige Bereiche, die mit diesem Gesetz noch nicht gelöst werden.

In meinem Bericht 2018 habe ich darauf hingewiesen, dass es nach wie vor keine Datenschutzordnung für das Abgeordnetenhaus von Berlin gibt. Obwohl auch hier im Haus mit personenbezogenen Daten gearbeitet wird, gab und gibt es dafür keinerlei Kontrollmöglichkeiten und keine Regelungen für betroffene Personen, ihre Datenschutzrechte geltend zu machen. Dieses Problem verschärft sich mit Inkrafttreten des Datenschutz-Anpassungsgesetzes, weil dem Berliner Parlament künftig noch viel umfassendere Befugnisse eingeräumt werden sollen, auch mit besonders schützenswerten Daten umzugehen. Hier muss dringend nachgearbeitet werden!

Darüber hinaus gibt es im Berliner Datenschutzgesetz relevanten Nachbesserungsbedarf im Bereich der Datenschutzaufsicht sowie der effektiven Sicherung von Betroffenenrechten. Mehrere Regelungen entsprechen nicht den Anforderungen der Datenschutz-Grundverordnung und sollten überdacht werden.

Ich hoffe hier sehr auf die Ankündigung der Koalitionsfraktionen, dieses Gesetz vor Ablauf der Wahlperiode noch einmal separat zu evaluieren und anzupassen.

Meine Damen und Herren, es bleibt viel zu tun. Erst kürzlich hat der Europäische Gerichtshof in seiner „Schrems-II"-Entscheidung festgestellt, dass die bisherigen Rechtsgrundlagen für Datenübermittlungen in Drittstaaten und insbesondere in die USA nur noch sehr eingeschränkt nutzbar sind. Das stellt Wirtschaft, Verwaltung und uns, die wir das durchsetzen müssen, vor riesige Herausforderungen. Wir stellen uns dieser Aufgabe und werben gleichzeitig dafür, dies auch als große Chance für mehr digitale Eigenständigkeit in Europa zu sehen. Hieran müssen wir gemeinsam arbeiten.

Vielen Dank für Ihre Aufmerksamkeit!

Glossar

2-Faktor-Authentifizierung	Nachweis der Identität einer Person über zwei der drei folgenden Merkmale: 1. Besitz eines Gerätes, über das ausschließlich diese Person verfügt, 2. Kenntnis eines Geheimnisses (z. B. ein Passwort), das nur ihr bekannt ist, 3. biometrische Charakteristika der Person wie ihren Fingerabdruck.
Abo-Falle	Bezeichnet umgangssprachlich eine unseriöse Geschäftspraxis im Internet, bei der Verbraucher*innen unbeabsichtigt ein kostenpflichtiges Abonnement eingehen. Ein solches Angebot ist im Regelfall so aufgebaut, dass Verbraucher*innen in der irrigen Annahme gelassen werden, dass die dort bereitgestellten Dienste kostenfrei seien, aber tatsächlich Kosten anfallen. Bevor Verbraucher*innen die Dienste nutzen, müssen sie ihre persönlichen Daten angeben. Wenig später meldet sich der Anbieter bei ihnen und verlangt z. T. hohe Geldbeträge für das angeblich abgeschlossene Abonnement.
Customer-Relationship-Management-(CRM-)System	Als CRM-System bezeichnet man eine Software zur Verwaltung der Kundenbeziehungen.
Anonym/Pseudonym	Anonyme Daten können nicht mehr einer Person zugeordnet werden. Bei pseudonymen Daten ist dies einer bestimmten dritten Partei möglich unter vorab festgelegten Bedingungen.
App	Anwendungsprogramm für Mobiltelefone.

Art. 29-Gruppe	Gruppe nach Art. 29 Europäische Datenschutzrichtlinie, die sich aus Vertreterinnen und Vertretern aller europäischen Datenschutzbehörden zusammensetzt. Sie hat beratende Funktion; vornehmlich gegenüber der Europäischen Kommission, aber auch gegenüber anderen Datenverarbeiter*innen innerhalb der Europäischen Union.
Chief Information Security Officer (CISO)	Verantwortliche*r für die Ausarbeitung von Sicherheitsrichtlinien, für die Ausrichtung, Planung und Koordination von Maßnahmen zur Gewährleistung der Sicherheit der von einer Organisation verarbeiteten Informationen sowie für die Bewertung der Umsetzung dieser Maßnahmen und der verbleibenden Risiken.
Cookie	Ein Cookie ist eine Textdatei, die dazu dient, mit einer Webseite verbundene Informationen auf dem Computer der Nutzerinnen bzw. Nutzer lokal abzuspeichern und dem Webseitenserver auf Anfrage zurück zu übermitteln. Dadurch können ggf. die Nutzerinnen und Nutzer wiedererkannt und besuchte Webseiten sowie Zeitpunkte des Besuchs zugeordnet werden.
Cookie-Banner	Banner sind Grafik- oder Animationsdateien, die in die Webseite eingebunden sind und entweder am Rand erscheinen oder sich über die Webseite legen. In der Regel enthalten diese Werbung. Cookie-Banner enthalten in der Regel Hinweise zum Einsatz von Cookies und sind zumeist mit einem einfachen „Ok"-Knopf versehen.
Dashcam	Als Dashcam wird eine Videokamera bezeichnet, die am Armaturenbrett (engl. dash board) oder an der Windschutzscheibe eines Fahrzeugs befestigt ist.
DKIM-Signatur	DKIM steht für Domain Keys Identified Mail. Dabei handelt es sich um eine Methode der E-Mail-Authentifizierung. DKIM fügt E-Mails eine digitale Signatur hinzu, die der Absender-Domain zugeordnet ist und bei allen ausgehenden E-Mails genutzt wird. Dies ist eine Technik, die Fälschungen der E-Mail-Absender*innen oder des Inhalts von E-Mails erkennbar macht. Ver- oder gefälschte

E-Mails können so automatisch abgewiesen oder gesondert behandelt, unverfälschte E-Mails akzeptiert und als echt behandelt werden.

Double-Opt-In-Verfahren

Double-Opt-In-Verfahren bezeichnet einen Prozess, bei dem Nutzende nach der Eintragung ihrer Kontaktdaten in einen Verteiler diese in einem separaten zweiten Schritt nochmals bestätigen müssen. Meist wird hierzu eine E-Mail-Nachricht mit der Bitte um Bestätigung an die jeweils angegebenen Kontaktdaten gesendet. Daneben kann eine Bestätigung aber auch per SMS oder telefonisch erfolgen.

DS-GVO

Europäische Datenschutz-Grundverordnung – Die Datenschutz-Grundverordnung (DS-GVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewärleistet werden. Die Verordnung ersetzt die aus dem Jahr 1995 stammende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Sie ist bereits am 24. Mai 2016 in Kraft getreten, wurde aber aufgrund einer zweijährigen Übergangsfrist erst am 25. Mai 2018 wirksam. Seitdem ist sie in allen Mitgliedsstaaten der Europäischen Union unmittelbar anwendbar.

DSK

Die Datenschutzkonferenz (DSK) besteht aus den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.

EDSA	Der Europäische Datenschutzausschuss (EDSA) ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beiträgt und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördert. Der EDSA besteht aus Vertretern der nationalen Datenschutzaufsichtsbehörden und dem Europäischen Datenschutzbeauftragten (EDSB).
EG / Erwägungsgrund	Erwägungsgründe sind Erklärungen des europäischen Gesetzgebers zum eigentlichen Gesetzestext, die diesem regelmäßig bei europäischen Rechtsvorschriften beigefügt werden.
eID	„Elektronische Identität"; dabei handelt es sich um einen elektronischen Identitätsnachweis (mit Chip), mit dessen Hilfe elektronische Vorgänge ausgeführt werden können.
Ende-zu-Ende-Verschlüsselung	Der Inhalt einer Datenübertragung wird so verschlüsselt, dass nur die oder der vom Sender festgelegte Empfänger*in die Daten entschlüsseln, d. h. wieder lesbar machen kann. Zwischenstationen wie z. B. E-Mail-Anbieter*innen sehen hingegen nur verschlüsselte Daten.

Fanpage	Facebook Fanpage: Eine Facebook Fanpage ist die Präsenz von Marken, Unternehmen, Organisationen und Personen des öffentlichen Lebens bei dem sozialen Netzwerk Facebook, die dazu dient, das Unternehmen oder die Marke etc. im Netzwerk mithilfe der vom Netzwerk zur Verfügung gestellten Kommunikationsmittel zu vermarkten, z. B. indem die Seite von Facebook-Nutzer*innen weiterempfohlen bzw. im „Freundeskreis" der Nutzer*innen geteilt wird. Die Fanpage ist zudem ein öffentliches Profil und kann von Personen außerhalb des Netzwerks abgerufen werden; sie wird bei den einschlägigen Suchmaschinen indexiert, d. h. in der Ergebnisliste aufgeführt. Im Gegensatz zur Profilseite, die von Privatpersonen genutzt wird, geht es nicht um das „Befreunden", sondern darum, mithilfe der Seite z. B. direkt mit Kund*innen im Netzwerk zu kommunizieren bzw. „Fans" zu sammeln.
Firmware	Die Firmware eines Geräts ist Software, die in elektronische Geräte eingebettet ist, um deren grundlegende Funktion zu gewährleisten. Sie ist durch Anwender*innen nicht oder nur mit speziellen Mitteln bzw. Funktionen austauschbar. Firmware ist funktional fest mit der Hardware verbunden; das eine ist ohne das andere nicht nutzbar.
Geodaten	Digitale geologische Daten, die z. B. in Navigationssystemen verarbeitet werden.
GovData	Datenprotal für Deutschland, das einen zentralen und einheitlichen inhaltlichen Zugang zu Verwaltungsdaten aus Bund, Ländern und Kommunen bietet, die diese in ihren jeweiligen Open Data-Portalen zugänglich gemacht haben.
GPS / GPS-Sender	Global Positioning System; dt.: Globales Positionsbestimmungssystem.

Hashfunktion	Bei einer kryptografischen Hashfunktion handelt es sich um eine mathematische Berechnungsvorschrift, die aus beliebigen Ausgangsdaten wie bspw. einem Dokument oder auch nur einem Wort bzw. einer Telefonnummer einen eindeutigen Prüfwert mit fester Länge berechnet. Diese Berechnung ist nicht umkehrbar – aus den Prüfwerten können die Ausgangsdaten nicht zurückberechnet werden. Bei wiederholter Berechnung mit gleichen Ausgangsdaten ergibt sich jedoch immer der gleiche Prüfwert.
Hashwert	Der Hashwert ist das Ergebnis (der Prüfwert) der Anwendung einer [obigen] kryptografischen Hashfunktion. Bei dieser handelt es sich um eine mathematische Berechnungsvorschrift, die aus beliebigen Ausgangsdaten wie bspw. einem Dokument oder auch nur einem Wort bzw. einer Telefonnummer einen eindeutigen Hashwert mit fester Länge berechnet.
IMI	Das Binnenmarkt-Informationssystem (IMI) ist ein mehrsprachiges Online-Tool, das den Informationsaustausch zwischen Behörden erleichtert, die an der praktischen Umsetzung des EU-Rechts beteiligt sind. Die Datenschutzaufsichtsbehörden der EU-Mitgliedsstaaten stimmen damit Fälle ab, denen eine grenzüberschreitende Verarbeitung personenbezogener Daten zugrunde liegt.
Informierte Einwilligung	„Informierte Einwilligung“ bezeichnet eine Einwilligungserklärung, bei welcher die Nutzer*innen nach vorheriger, vollständiger Information über die geplante Verarbeitung ihrer Daten, deren Art, Umfang und Zweck der Verarbeitung dieser dann eindeutig zugestimmt haben.
Integrität	Unter der Wahrung der Integrität von Daten versteht man ihren Schutz vor unbefugter Veränderung oder Entfernung, vor unbeabsichtigtem Verlust oder Zerstörung und vor unbeabsichtigter Verfälschung.
IP-Adresse	Internet Protokoll Adresse = die Adresse eines Computers im Internet.

IT-Architektur	Festlegung der Zusammensetzung informationstechnischer Systeme aus verschiedenen Komponenten und deren Zusammenwirken.
Kohärenzverfahren	Wenn im One-Stop-Shop-Verfahren kein Konsens zwischen den beteiligten Aufsichtsbehörden gefunden werden kann, trifft der Europäische Datenschutzausschuss (EDSA) im Rahmen des Kohärenzverfahrens verbindliche Beschlüsse. Darüber hinaus werden im Kohärenzverfahren mit dem Ziel der einheitlichen Anwendung der DS-GVO auch Stellungnahmen des EDSA – etwa zur Festlegung von Standard-Datenschutzklauseln – abgestimmt.
Link	Verweis oder Sprung zu einem elektronischen Dokument.
Marktortprinzip	Die DS-GVO ist anwendbar, sobald ein Unternehmen Waren und Dienstleistungen für Personen in der Europäischen Union anbietet oder das Verhalten von Bürgerinnen und Bürgern beobachtet und in diesem Zusammenhang personenbezogene Daten verarbeitet. Der Anwendungsbereich der DS-GVO erfasst damit auch außereuropäische Unternehmen, die auf dem europäischen Markt aktiv sind, selbst wenn sie keine Niederlassung in der Europäischen Union haben. Durch das Marktortprinzip sollen einheitliche Wettbewerbsbedingungen für alle Unternehmen geschaffen werden, die auf dem europäischen Markt Waren und Dienstleistungen anbieten.
Messenger-Dienst	Telekommunikationsdienst, bei dem zwei oder mehr Teilnehmende Textnachrichten (ggf. auch Audio- oder Video-Nachrichten sowie weitere Dateien) so austauschen, dass die Nachrichten möglichst unmittelbar bei den Empfänger*innen ankommen.
Metadaten	Die bei einer Datenübermittlung anfallenden Daten unterteilt man in Inhaltsdaten – bspw. der Text einer E-Mail – und alle anderen sog. Metadaten, die die Kommunikationsumstände betreffen, d. h. Zeitpunkt, Absender, Empfänger, Standorte bei mobilen Endgeräten sowie technische Adressen/Kennnummern der zur Kommunikation verwendeten Geräte.

Mikroblogging

Beim Mikroblogging werden kurze SMS-ähnliche Texte erstellt, die in einem Blog oder Kurznachrichtendienst eingestellt werden. Es geht beim Mikroblogging nicht darum, thematisch in die Tiefe zu gehen, sondern innerhalb kurzer Zeit und ohne großen Aufwand Nachrichten aller Art zu produzieren.

Neuronale Netze

Künstliche Neuronale Netze sind in der Regel an den Organisationsprinzipien und den Lernprozessen des menschlichen Gehirns orientierte Computermodelle.

One-Stop-Shop

Das One-Stop-Shop-Prinzip soll sicherstellen, dass jedes in der EU ansässige Unternehmen in der Datenschutzbehörde vor Ort eine einheitliche Ansprechpartnerin vorfindet. Diese soll die jeweiligen Datenschutzfragen mit den anderen europäischen Datenschutzbehörden abstimmen. Die Unternehmen sollen so von dem Aufwand entlastet werden, sich innerhalb der EU mit unterschiedlichen Datenschutzbehörden auseinandersetzen zu müssen. Für Unternehmen mit Niederlassungen in verschiedenen Mitgliedsstaaten ist die Aufsichtsbehörde am Sitz der Hauptverwaltung die zentrale Ansprechpartnerin.

Die DS-GVO sieht den One-Stop-Shop aber nicht nur für die Unternehmen, sondern auch für die Bürgerinnen und Bürger vor. Auch diese können sich unkompliziert bei ihrer Aufsichtsbehörde vor Ort in ihrer Landessprache auch über ausländische Unternehmen beschweren.

Open Data

Datenbestände, die den Bürgerinnen und Bürgern sowie der Wirtschaft ohne Beschränkung zur freien Weiterverwendung frei zugänglich gemacht werden.

Open Government	„Open Government“ beschreibt offenes Regierungs- und Verwaltungshandeln insbesondere durch: • Transparenz, z. B. über Verfahren und Entscheidungen sowie den Zugang zu Informationen, • Partizipation, etwa in Form von Bürgerdialogen oder Konsultationen, • Zusammenarbeit zwischen Regierung und Nichtregierungsorganisationen sowie ressort- und ebenenübergreifend, • Nutzung neuer Technologien zur Verbesserung des Regierungs- und Verwaltungshandelns.
Opt-In / Opt-out	Opt-in meint, dass eine Datenverarbeitung nur zulässig ist, wenn die betroffene Person sich ausdrücklich dafür entschieden hat, also in der Regel ihre Einwilligung gegeben hat. Bei einem Opt-out-Verfahren dagegen muss die betroffene Person ausdrücklich aktiv werden, um die Datenverarbeitung zu verhindern.
Opt-Out-Modell	„Opt-Out-Modell“ bezeichnet ein Verfahren, dass die Einwilligung annimmt, wenn dieser nicht innerhalb eines vorher festgelegten Zeitraums widersprochen wurde.
Pixel	Kleine Grafiken auf Webseiten, die meist nur 1×1 Pixel messen und beim Aufruf einer Webseite von einem Server geladen werden. Das Herunterladen wird registriert und kann für Auswertungen im Bereich des Online-Marketings genutzt werden.
Pre-Recording-Funktion	Bezeichnet die Aufzeichnung und Speicherung eines vorgewährten Zeitbereichs in einer Endlosschleife, d. h., es handelt sich um eine Aufzeichnungsfunktion, bei der bereits wenige Sekunden vor Betätigen des Aufzeichnungsknopfes eine Speicherung der Daten erfolgt.
Privacy by Default	Produkte werden mit den datenschutzfreundlichsten Voreinstellungen ausgeliefert.

Privacy by Design	Die Hersteller berücksichtigen den Datenschutz bereits bei der Herstellung und Entwicklung von Produkten.
Profiling	Unter Profiling ist jede Art der automatisierten Bewertung bestimmter persönlicher Aspekte einer natürlichen Person zu verstehen. Zu diesen Aspekten können etwa die Arbeitsleistung, die wirtschaftliche Lage, die Gesundheit, persönliche Vorlieben, die Interessen, die Zuverlässigkeit, das Verhalten, der Aufenthaltsort oder mögliche Ortswechsel einer Person gehören. Ziel des Profilings ist es, diesbezüglich eine Analyse vorzunehmen bzw. eine Vorhersage zu treffen. Profiling kommt z. B. im Werbebereich und bei der Vertragsanbahnung zum Einsatz, aber etwa auch die Polizei setzt zunehmend auf entsprechende Vorhersageverfahren.
Pseudonymisieren	Pseudonymisieren ist das Ersetzen identifizierender Angaben wie Name, Adresse, Geburtsdatum oder anderer eindeutiger Kennzeichen bzw. Merkmale durch eine andere Bezeichnung (z. B. eine laufende Nummer) derart, dass ein Rückschluss auf die Person ohne Kenntnis der Zuordnungsregel nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.
Public Consultation	dt.: Öffentliche Konsulation. Vor der Verabschiedung von Leitlinien führt der Europäische Datenschutzausschuss (EDSA) öffentliche Konsultationen durch, um die Ansichten und Anliegen aller Interessenträger*innen und Bürger*innen zu hören. In der Regel werden Leitlinien vor ihrer endgültigen Verabschiedung auf der Internetseite des EDSA veröffentlicht. Dann besteht in der Regel für sechs bis acht Wochen die Möglichkeit, die Leitlinie zu kommentieren. Hauptsächlich machen Wirtschaftsverbände und Unternehmen von dieser Möglichkeit Gebrauch. Der ESDA erhält aber auch Feedback von zivilgesellschaftlichen Gruppen und Bürger*innen. Nach Ablauf der Konsultationsphase entscheidet der EDSA, welche Änderungswünsche berücksichtigt werden.
Quellcode	Der Programmcode (technische Grundlage) einer Software.

Ringspeicher

Ein Ringspeicher speichert Daten kontinuierlich in einem gewissen Zeitraum und überschreibt diese nach Ablauf einer vorgegebenen Zeit wieder, um den Speicherplatz für neue Daten freizugeben.

Score-Wert
Rating-Stufe

Wirtschaftsauskunfteien sammeln Informationen über Menschen, insbesondere über deren wirtschaftliche Situation und deren Zahlungsverhalten. Daraus errechnen sie einen nummerischen Wert, der die Zahlungsfähigkeit (Bonität) der betreffenden Person abbilden soll, den sog. Score-Wert. Abhängig von diesem Score-Wert wird den betroffenen Personen dann eine Wahrscheinlichkeit zugeordnet, mit der sie offene Forderungen begleichen bzw. nicht begleichen, sog. Rating-Stufe. Diese Informationen können Unternehmen abrufen, bevor sie Verträge

abschließen, bei denen sie sich auf eine spätere Leistung der Vertragspartnerin oder des Vertragspartners verlassen müssen.

sensitive Daten

Besondere Arten personenbezogener Daten. Dazu gehören Angaben über die ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Social Plugins

Social Plugins oder auch Social Media Plugins verbinden Webseiten oder Apps mit sozialen Netzwerken. Betreiberinnen und Betreiber fügen einen Programmcode in den Quellcode ihrer Webseite oder App ein, der automatisch Daten zum Betreiber des sozialen Netzwerks sendet und von diesen Daten abruft. Die Betreiber des sozialen Netzwerks erfahren so, wofür sich die Besucherinnen und Besucher der Webseite interessieren, und können mittels Profiling Persönlichkeitsprofile erstellen sowie Werbung personalisieren. Ein Betreiber kann bspw. anzeigen, dass Bekannte der Webseiten-Besucherin bzw. des Webseiten-Besuchers die Webseite mit „Gefällt mir“ markiert haben. Durch Social Plugins können insbesondere durch Netzwerkeffekte erhebliche Besuchszahlen für Webseiten und in der Folge regelmäßig erhebliche Umsätze generiert werden.

Software-as-a-Service (SaaS)	Bei Software-as-a-Service (SaaS) betreibt der Anbieter die Server und die Software für den jeweiligen Dienst. Nutzende erhalten nur einen Zugriff auf die Leistungen dieses Dienstes, meist nur die Oberfläche, die oft im Web-Browser angezeigt wird. Es handelt sich dabei um einen typischen Cloud-Dienst. Im Gegensatz dazu erwerben Nutzende bzw. ihre Institutionen im klassischen Modell Software und Server und betreiben die Software selbst.
Sozialsphäre	Die Sozialsphäre ist der Bereich, in dem der Mensch sich im Austausch mit anderen Menschen befindet. Hiervon ist sowohl der private als auch der berufliche Bereich umfasst.
Tracking	Tracking ist im Verständnis der Datenschutzaufsichtsbehörden das Protokollieren und Auswerten des Verhaltens von Besucherinnen und Besuchern von Webseiten oder Apps zur in der Regel webseitenübergreifenden Nachverfolgung. Die Anwendungsgebiete reichen von einer reinen Reichweitenmessung über statistische Auswertung etwa nach Browser, Betriebssystem, Spracheinstellungen sowie Aufenthalts-Land und Tests zur Benutzungsfreundlichkeit von Webseiten bis hin zur detaillierten Beobachtung und Aufzeichnung sämtlicher Mausbewegungen und Eingaben sowie zur webseiten- und geräteübergreifenden Erstellung von Nutzungs- und Persönlichkeitsprofilen zu Werbezwecken.
Tracking / Cookie Walls	Verhinderung der Nutzung einer Webseite bei Nichtakzeptieren von Cookies.
Verhaltensregeln	engl.: Code of conduct. Es handelt sich dabei um ein Instrument der Selbstregulierung. Gemäß Art. 41 DS-GVO können Verbände und andere Vereinigungen Verhaltensregeln ausarbeiten, mit denen die Anwendung der DS-GVO präzisiert wird. Aufgabe der Aufsichtsbehörden ist es, die Ausarbeitung solcher Verhaltensregeln zu fördern und zu genehmigen.

Verkehrsdaten	Technische Informationen, die bei der Nutzung eines Telekommunikationsdienstes anfallen, etwa bei einem Telefonanruf anrufende und angerufene Telefonnummer, Beginn und Ende der Verbindung und bei Telefonaten im Mobilfunknetz auch der Standort. Auch als Verbindungsdaten bezeichnet.
Wearable	Wearable Computer oder kurz Wearables sind Computer, die so klein sind, dass sie weder einen Raum ausfüllen noch einen Schreibtisch benötigen, sondern z. B. als Armband und Brille getragen oder in Kleidung eingearbeitet werden können. Während der Anwendung sind sie am Körper der Benutzenden befestigt und oftmals direkt mit dem Internet verbunden. So kann z. B. ein Blutdruckmessgerät, welches dauerhaft oder über einen längeren Zeitraum am Arm getragen wird, durchaus als Gerät aus dem Bereich Wearable Computing bezeichnet werden.
WIFI-Basisstationen	Gerät zur drahtlosen Datenübertragung; wird meist bei drahtgebundenen Internetzugängen verwendet, um mobilen Geräten in der Nähe eine Nutzung des Internets zu ermöglichen, ohne Kabel anschließen zu müssen.
WiFi-Tracking	Eine Technik, mit der Bewegungsverläufe von Personen anhand von Standortdaten verfolgt werden können, die unter Rückgriff auf das Smartphone dieser Personen erfasst werden.

Stichwortverzeichnis

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

Infothek der Berliner Beauftragten für Datenschutz und Informationsfreiheit

Tätigkeitsberichte: Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat von Berlin jährlich einen Bericht über ihre Tätigkeit vorzulegen. Neben aktuellen technischen und rechtlichen Entwicklungen wird darin über Schwerpunktthemen und Einzelfälle aus den jeweiligen Geschäftsbereichen berichtet. Der Tätigkeitsbericht wird von uns auch als Broschüre für die Bürgerinnen und Bürger veröffentlicht.

Ratgeber und Faltblätter zum Datenschutz: In diesen Publikationen haben wir praktische Informationen zu immer wieder auftretenden Fragen im Alltag zusammengestellt. Damit wollen wir die Menschen in die Lage versetzen, ihre Datenschutzrechte bzw. ihr Recht auf Informationszugang eigenständig wahrzunehmen.

Gesetzestexte: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Berliner Datenschutzgesetz als gedruckte Ausgabe oder zum Downloaden.

Kurzpapiere, Orientierungshilfen und Anwendungshinweise: Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder befassen sich intensiv mit den neuen Rechtsgrundlagen und deren Anforderungen und stimmen eine einheitliche Sichtweise ab. Die Ergebnisse dieses Prozesses sind gemeinsame Kurzpapiere zur DS-GVO, Orientierungshilfen und Empfehlungen, die die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) veröffentlicht.

Leitlinien: Der Europäische Datenschutzausschuss (EDSA) besteht aus Vertreter*innen der europäischen Datenschutzbehörden und den Europäischen Datenschutzbeauftragten. Er veröffentlicht Leitlinien, Empfehlungen und sog. bewährte Verfahren zu zentralen Themen der DS-GVO. Soweit diese bereits in deutsche Sprache übersetzt wurden, können sie auf unserer Webseite heruntergeladen werden.

Alle Informationsmaterialien sind auf unserer Webseite abrufbar und einige auch in gedruckter Form erhältlich. Eine Übersicht finden Sie unter **www.datenschutz-berlin.de**.

Ein umfassendes medienpädagogisches Informationsangebot stellen wir auf unserer Kinderwebseite **www.data-kids.de** zur Verfügung. Dort finden Kinder, Lehrkräfte und Eltern umfangreiche Materialien, die dabei helfen, sich in der Welt des Datenschutzes besser zurechtzufinden.

Der Jahresbericht 2020 umfasst folgende Schwerpunkte:

Datenschutzfragen im Zusammenhang mit Corona; Internationaler Datenverkehr nach der „Schrems II"-Entscheidung des Europäischen Gerichtshofs; Einsatz von Videokonferenzsystemen; Digitalisierung der Schulen – BER 2.0?; Startschuss für die Zertifizierung

www.datenschutz-berlin.de

be Berlin