Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Datenschutz und Informationsfreiheit

Jahresbericht 2018

Jahresbericht

der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2018

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. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den am 23. März 2018 vorgelegten Jahresbericht 2017 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2018 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

Hinweis
Das Glossar (am Ende der Broschüre) bietet eine Liste mit Erklärungen verschiedener Fachbegriffe. Die farbliche Hervorhebung von Wörtern im Text (z. B. Marktortprinzip) weist darauf hin, dass diese im Glossar abgedruckt sind.

Abkürzungsverzeichnis

ABl. EU	Amtsblatt der Europäischen Union
ASOG	Allgemeines Sicherheits- und Ordnungsgesetz
BAO	Fachverfahren Beihilfe Online
BauGB	Baugesetzbuch
BDSG (a. F.)	Bundesdatenschutzgesetz (alte Fassung)
BEEG	Bundeselterngeld- und Elternzeitgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BlnDSG (a. F.)	Berliner Datenschutzgesetz (alte Fassung)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVG	Berliner Verkehrsbetriebe
DAkkS	Deutsche Akkreditierungsstelle
DB AG	Deutsche Bahn AG
Drs.	Drucksache
DSFA	Datenschutz-Folgenabschätzung
DSK	Deutsche Datenschutzkonferenz
DS-GVO	Europäische Datenschutz-Grundverordnung
EDSA	Europäischer Datenschutzausschuss
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuch
EGovG Bln	Berliner E-Government-Gesetz
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GG	Grundgesetz
GPS	Global Positioning System
GVBl.	Gesetz- und Verordnungsblatt für Berlin
GwG	Geldwäschegesetz
HIS	Hinweis- und Informationssystem der Versicherungswirtschaft

IBAN	Internationale Bankkontonummer (International Bank Account Number)
IFG	Berliner Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
IMI	Elektronisches Informationssystem der europäischen Behörden
INPOL	Informationssystem der Landespolizeibehörden in Deutschland
ISBJ	Integrierte Software Berliner Jugendhilfe
ISO	Internationale Organisation für Standardisierung
IT	Informationstechnik
IWGDPT	Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation (sog. Berlin-Group)
JB	Jahresbericht
JI-Richtlinie	Europäische Datenschutz-Richtlinie für Justiz und Inneres
KJHG	Kinder- und Jugendhilfegesetz
KTDat	Ausschuss für Kommunikationstechnologie und Datenschutz
KunstUrhG	Kunst-Urhebergesetz
KV	Kassenärztliche Vereinigung
KWG	Kreditwesengesetz
LABO	Landesamt für Bürger- und Ordnungsangelegenheiten
LAGeSo	Landesamt für Gesundheit und Soziales
LAGetSi	Landesamt für Arbeitsschutz, Gesundheitsschutz und technische Sicherheit
LBG	Landesbeamtengesetz
LSG	Landessozialgericht
LVwA	Landesverwaltungsamt
MuSchG	Mutterschutzgesetz
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PartIntG	Gesetz zur Regelung von Partizipation und Integration
POLIKS	Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung
PSSG	Personalstrukturstatistikgesetz
SGB	Sozialgesetzbuch
SDM	Standard-Datenschutzmodell
StGB	Strafgesetzbuch
StPO	Strafprozessordnung

TKG	Telekommunikationsgesetz
TV-L	Tarifvertrag der Länder
UIG	Umweltinformationsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VBB	Verkehrsverbund Berlin-Brandenburg
VDV	Verband Deutscher Verkehrsunternehmen
WP	Working Paper
ZDRL	Zahlungsdiensterichtlinie

Einleitung

Am 25. Mai 2018 hieß es „Und Action, bitte!". Die Datenschutz-Grundverordnung (DS-GVO) wurde wirksam. Und trotz aller Unkenrufe in einer im Vorfeld recht überhitzt geführten öffentlichen Debatte, die Ängste schürte und vermeintliche Fallstricke skandalisierte, läuft sie erstaunlich reibungslos. Natürlich gibt es Kinderkrankheiten und Unsicherheiten in und mit dem neuen EU-weit verbindlichen Datenschutzrecht. Dies kann aber bei der kompletten Neuschaffung eines Rechtsgebiets auf europäischer Ebene – und genau darum handelt es sich – noch ohne Rechtsprechung und Erfahrungswissen im Grunde auch gar nicht anders sein. Jetzt, nachdem fast ein Jahr vergangen ist, erscheint alles schon deutlich in einem anderen Licht.

Die DS-GVO hat allen Prophezeiungen zum Trotz Laufen gelernt. Dies zeigt sich vor allem an dem bis heute anhaltenden enorm hohen Beschwerdeaufkommen, der Menge an Beratungsanfragen und der Anzahl der meiner Behörde gemeldeten Datenpannen.[1] Zwar waren wir auf erhebliche Mehrarbeit eingestellt, letztlich wurden aber unsere Erwartungen, vor allem in den ersten Wochen nach dem Wirksamwerden der DS-GVO, erheblich übertroffen. Um die Flut an eingehenden Anrufen zumindest einigermaßen zu bewältigen, richteten wir anfangs eine DS-GVO-Telefon-Hotline für Ratsuchende ein, durch die die drängendsten Fragen unmittelbar beantwortet werden konnten. Und bis zum heutigen Tag stellt die Bewältigung des signifikant gestiegenen Arbeitsaufkommens eine Herausforderung dar, der meine Behörde nur dank des außerordentlichen Engagements meiner Mitarbeiterinnen und Mitarbeiter Stand hält. Eine Entspannung ist nicht in Sicht.

Es ist unverkennbar, dass das neue Regelwerk den Datenschutz stärker in den Fokus der Verantwortlichen gerückt und vor allem auch die Bürgerinnen und Bürger enorm für den Datenschutz sensibilisiert hat. Diese Entwicklung werte ich als Erfolg, zumal die Zeiten an der Schwelle zur Digitalisierung unserer kompletten

1 Siehe 1.2 und 1.3

Lebenswelt keineswegs leicht sind für den Datenschutz. Sich dem Hype der Digitalisierung zu unterwerfen, ist Mainstream, und Bedenken oder Hinweise auf Probleme und Unverträglichkeiten werden nur allzu gern als Behinderung dieser modernen Entwicklung abgetan.

Dabei entscheiden immer öfter Algorithmen darüber, welche Nachrichten man liest, welche Partnerin bzw. welchen Partner man trifft oder sogar welche Partei man wählt. Und auch in die öffentliche Verwaltung haben unter Zuhilfenahme von Algorithmen und sogenannter künstlicher Intelligenz zustande gekommene automatisierte Entscheidungen Einzug gehalten. All dies geschieht bislang äußerst intransparent. Doch nur wer die Datengrundlage, die Handlungsabfolge und die Gewichtung der Entscheidungskriterien kennt, kann die Rechtmäßigkeit von Entscheidungen überprüfen. Aus diesem Grund halte ich es für dringend erforderlich, auch automatisierte Entscheidungen nachvollziehbar, kontrollierbar und verständlich zu gestalten. Ich begrüße es daher sehr, dass ein Großteil der Mitglieder der Konferenz der Informationsfreiheitsbeauftragten in Deutschland auf Anregung der Informationsfreiheitsbeauftragten von Berlin, Bremen und Schleswig-Holstein in einem Positionspapier Anforderungen dafür formuliert hat, öffentliche Stellen noch konsequenter als bisher zu einem transparenten und verantwortungsvollen Einsatz von Algorithmen und künstlicher Intelligenz zu verpflichten.[2]

Die Digitalisierung stellt die Demokratie und den Rechtsstaat auf eine extreme Bewährungsprobe. Ein gelegentliches kritisches Innehalten ist damit wichtiger denn je, angesichts des hohen Anpassungsdrucks in unserem hochbeschleunigten Alltag aber auch ungemein schwierig. Umso bedeutsamer ist es, bereits Kinder im Grundschulalter über den Umgang mit ihren eigenen Daten aufzuklären, ihnen zu vermitteln, wie sie selbst darauf Einfluss nehmen können, was mit ihren Daten geschieht.[3] Wichtigste Voraussetzung dafür ist, kritisch und objektiv gegenüber allen Informationen und Botschaften aus dem Netz zu bleiben und sich eine Grundkenntnis der Internetmechanismen anzueignen. Meine Behörde hat sich deshalb nicht nur die Vermittlung von Medienkompetenz, sondern auch von Medienmündigkeit auf die Fahne geschrieben. Es ist unser Ziel, dass mehr

2 Siehe 13.1

3 Siehe 5.5

und mehr Kinder digitale Medien nicht nur kompetent bedienen, sondern diese auch reflektiert gebrauchen. Dies schließt im Übrigen auch ein, sie gegebenenfalls nicht zu gebrauchen – beispielsweise Suchmaschinen, die Suchanfragen nicht löschen und Nutzungsprofile erstellen. Auf unserer Kinder-Webseite bieten wir unterschiedlichste Aufklärungsmaterialien für Grundschulkinder, Eltern und auch Lehrerinnen und Lehrer an. Und auch mithilfe der gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Familie im November 2018 herausgegebenen Neuauflage der Broschüre „Ich suche dich. Wer bist Du?“[4] hoffen wir, einen Beitrag dazu leisten zu können, dass Kinder klug und selbstbewusst die Online-Welt entdecken.

Es zeigt sich: Gestaltung ist der Schlüssel! Datenschutz ist keine Bremse für den Fortschritt, er ist vielmehr das notwendige Korrektiv, um die technischen Entwicklungen im Einklang mit unseren Grundrechten voranzubringen. Eine Entwicklung dient nur dann den Menschen, wenn deren Rechte nicht leichtfertig zur Disposition gestellt werden. Auch die neue europäische Datenschutz-Grundverordnung ist genau so zu verstehen. Sie wurde von den europäischen Institutionen nicht entwickelt, um das Leben der Menschen zu formalisieren und ihre Entfaltungsmöglichkeiten zu begrenzen. Es ist genau umgekehrt: Die Datenschutz-Grundverordnung ist die europäische Antwort auf eine sich immer rasanter und global entwickelnde Digitalisierung aller Lebensbereiche. Sie bietet den Bürgerinnen und Bürgern erstmals europaweit durchsetzbare Instrumentarien, um ihre Rechte auch gegenüber global agierenden Unternehmen durchzusetzen. Natürlich ist das nicht leicht und Vieles muss auch noch im Einzelnen präzisiert werden. Aber es ist ein extrem wichtiger Schritt und nach meiner festen Überzeugung der einzig Erfolg versprechende Weg. Meine Behörde und ich werden uns deshalb weiterhin tatkräftig einmischen, wenn es darum geht, Lösungen zu finden, um unsere demokratischen und freiheitlichen Rechte zu bewahren und diese auch in der Zukunft zu gewährleisten.

Berlin, den 28. März 2019

Maja Smoltczyk
Berliner Beauftragte für Datenschutz und Informationsfreiheit

4 Abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/medienkompetenz/2018-BlnBDI-Broschuere_Soziale_Netzwerkde.pdf

1 Schwerpunkte

1.1 Bearbeitung grenzüberschreitender Fälle nach der DS-GVO

Durch die Datenschutz-Grundverordnung (DS-GVO) hat sich die Arbeit unserer Behörde grundlegend geändert. Dies gilt insbesondere für die Bearbeitung von Beschwerden, die an uns herangetragen werden.[1]

Neu ist, dass wir nicht nur Beschwerden gegen Berliner Unternehmen und Behörden bearbeiten. Nach der Datenschutz-Grundverordnung hat jede betroffene Person das Recht, sich insbesondere bei einer Aufsichtsbehörde in dem Mitgliedstaat der Europäischen Union (EU) zu beschweren, wo sie ihren gewöhnlichen Aufenthaltsort oder ihren Arbeitsplatz hat oder wo es zu dem mutmaßlichen Verstoß gekommen ist, wenn sie der Auffassung ist, dass eine Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DS-GVO verstößt.[2] Es kommt nicht mehr darauf an, dass die verarbeitende Stelle im Zuständigkeitsbereich der Aufsichtsbehörde niedergelassen ist. Vielmehr soll sich eine betroffene Person europaweit grundsätzlich an jede Datenschutz-Aufsichtsbehörde wenden können.

Alle eingehenden Beschwerden – aber auch alle Fälle, die wir von Amts wegen aufgreifen – werden von uns daher zunächst darauf geprüft, ob sie eine sog. grenzüberschreitende Datenverarbeitung[3] betreffen. Dies kann der Fall sein, wenn die oder der Verantwortliche in mehr als einem Mitgliedstaat der EU niedergelassen ist und die Verarbeitung in mehreren dieser Niederlassungen erfolgt. Selbst wenn die oder der Verantwortliche nur eine Niederlassung in der EU hat, kann eine grenzüberschreitende Verarbeitung vorliegen, wenn die Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann. Es reicht also aus, wenn sich etwa die Dienstleistung eines deutschen

1 Zur allgemeinen Bearbeitung von Beschwerden siehe 1.2.
2 Art. 77 Abs. 1 DS-GVO
3 Art. 4 Nr. 23 DS-GVO

Online-Händlers an Bürgerinnen und Bürger in Deutschland und Österreich richtet und möglicherweise erheblich in deren Datenschutzrechte eingreift.

Ergeben sich Anhaltspunkte für eine grenzüberschreitende Datenverarbeitung, werden alle erforderlichen Angaben zu dem Fall in ein elektronisches Informationssystem aller europäischen Aufsichtsbehörden (IMI) eingestellt. Diese prüfen, ob sie in dem Fall die federführende oder betroffene Aufsichtsbehörde sind, und melden sich entsprechend zurück. Auch uns erreichen über diesen Weg Fälle, in denen wir die federführende oder eine betroffene Aufsichtsbehörde sind. Um dies festzustellen, sind eine ständige Beobachtung des Informationssystems und eine systematische Prüfung der dort gemeldeten Fälle erforderlich.

Die federführende Aufsichtsbehörde übernimmt die weiteren Ermittlungen in dem jeweiligen Fall. Die Aufsichtsbehörde, bei der die Beschwerde ursprünglich eingegangen ist, ist in jedem Fall eine betroffene Aufsichtsbehörde. Sie hat die Beschwerdeführerin bzw. den Beschwerdeführer regelmäßig über den Stand der Bearbeitung zu unterrichten.[4] Auch hierzu dient der elektronische Informationsaustausch zwischen den Aufsichtsbehörden. Notwendige Übersetzungen werden durch die Aufsichtsbehörden geleistet, sodass für die Betroffenen keinerlei Nachteile entstehen.

Nach Abschluss der Ermittlungen entwirft die federführende Aufsichtsbehörde eine abschließende Entscheidung in dem Beschwerdefall und teilt diese allen betroffenen Aufsichtsbehörden mit. Diese haben vier Wochen Zeit, um den Entwurf zu prüfen.[5] Innerhalb dieser Frist können sie Einspruch gegen den Entwurf einlegen.

Wird kein Einspruch erhoben, erlässt die federführende Aufsichtsbehörde die Entscheidung gegenüber der oder dem Verantwortlichen. Diese/r ergreift die erforderlichen Maßnahmen, um die Verarbeitung in allen Niederlassungen in der EU mit der Entscheidung der Aufsichtsbehörde in Einklang zu bringen.[6] Die Aufsichtsbehörde, bei der die Beschwerde eingegangen ist, benachrichtigt die Beschwerdeführerin oder den Beschwerdeführer über den Ausgang des Verfahrens.

4 Art. 77 Abs. 2, Art. 57 Abs. 1 lit. f DS-GVO

5 Art. 60 Abs. 4 DS-GVO

6 Art. 60 Abs. 10 DS-GVO

Legt eine betroffene Aufsichtsbehörde Einspruch gegen den Entwurf ein, so muss sie diesen begründen. Kommt kein Einvernehmen zustande, leitet die federführende Aufsichtsbehörde ein Streitbeilegungsverfahren vor dem Europäischen Datenschutzausschuss ein.[7] Dieses Verfahren soll zur einheitlichen Anwendung der DS-GVO in der gesamten EU beitragen. Der Europäische Datenschutzausschuss fasst dann einen verbindlichen Beschluss in der jeweiligen Angelegenheit.[8] Dieser Beschluss umfasst alle Aspekte, die Gegenstand des Einspruchs waren, insbesondere die Frage, ob ein Verstoß gegen die DS-GVO vorliegt. Die federführende Aufsichtsbehörde trifft dann auf der Grundlage des Beschlusses unverzüglich, jedoch spätestens innerhalb eines Monats nach dessen Mitteilung, die Entscheidung gegenüber der oder dem Verantwortlichen.[9] Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, muss entsprechend die Beschwerdeführerin oder den Beschwerdeführer unterrichten.

Auch wir selbst haben als federführende Aufsichtsbehörde bereits Entwürfe für Entscheidungen mit den betroffenen Aufsichtsbehörden im beschriebenen Verfahren abgestimmt. Gegen die Entwürfe sind keine Einsprüche erhoben worden, sodass die Vorgänge auf Arbeitsebene erledigt werden konnten. Unsere Entscheidungen haben wir demzufolge gegenüber den grenzüberschreitend agierenden Verantwortlichen mit Sitz in Berlin erlassen. Die Beschwerdeführer wurden über das Ergebnis ihrer Eingabe informiert.

1.2 Bearbeitung von Beschwerden nach der DS-GVO

Die Bearbeitung von Beschwerden über Datenschutzverstöße von öffentlichen oder privaten Stellen zählte bereits vor Anwendung der DS-GVO zu den gesetzlichen Aufgaben der Aufsichtsbehörden. Auch nach dem nun geltenden europäischen Recht gehört es zu deren Pflichten, sich mit Beschwerden von betroffenen

7 Art. 60 Abs. 4 DS-GVO
8 Art. 65 Abs. 1 lit. a DS-GVO
9 Art. 65 Abs. 6 DS-GVO

Personen zu befassen, den Gegenstand der Beschwerde zu untersuchen und der betroffenen Person das Ergebnis dieser Untersuchung mitzuteilen.[10]

Durch die mit Anwendung der DS-GVO stark gestiegene Aufmerksamkeit für das Thema Datenschutz erhöhte sich auch die Zahl der Eingaben und Beschwerden bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit um rund das Vierfache. Es ist davon auszugehen, dass sich die Anzahl der Eingaben zukünftig auf einem vergleichbar hohen Niveau stabilisiert, da bisher kein nennenswerter Rückgang der Eingaben zu verzeichnen ist. Dies liegt insbesondere daran, dass sich die Zuständigkeit unserer Behörde erheblich erweitert hat. Zuvor waren wir lediglich für die Bearbeitung von Beschwerden gegen Berliner Behörden und Unternehmen zuständig. Das sog. Marktortprinzip weitet die Zuständigkeit unserer Behörde auf alle Stellen aus, die Berliner Bürgerinnen und Bürgern Waren und Dienstleistungen anbieten oder ihr Verhalten beobachten.[11]

Durch den mit der DS-GVO auf europäischer Ebene geschaffenen Rechtsrahmen muss bei der Bearbeitung von Beschwerden mittlerweile nicht nur die Zuständigkeitsverteilung der Aufsichtsbehörden für den Datenschutz innerhalb Deutschlands, sondern ganz Europas mitgedacht werden. Die DS-GVO möchte es Bürgerinnen und Bürgern erleichtern, sich ohne unnötige Hürden für den Schutz ihrer Daten einzusetzen, indem sie es ihnen ermöglicht, in ihrer eigenen Muttersprache und bei der Aufsichtsbehörde vor Ort ihre Beschwerden einzureichen. Es ist nunmehr Aufgabe der Aufsichtsbehörden, die Zuständigkeiten untereinander zu klären und konstruktiv zusammenzuarbeiten. Wenn es sich um eine grenzüberschreitende Beschwerde handelt (bspw. weil es betroffene Personen in mehreren EU-Staaten gibt oder ein Unternehmen in mehreren Staaten agiert), erfolgt deren Bearbeitung in Abstimmung mit den Aufsichtsbehörden der betroffenen Länder.[12] Für Bürgerinnen und Bürger, die sich über Berliner Unternehmen und Behörden beschweren, bleibt unsere Behörde jedoch über das gesamte Verfahren hinweg die Ansprechpartnerin vor Ort und informiert regelmäßig über den jeweiligen Sachstand.[13]

10 Art. 57 Abs. 1 lit. f DS-GVO
11 Art. 3 Abs. 2 DS-GVO
12 Siehe 1.1
13 Art. 78 Abs. 2 DS-GVO

Wir erhalten Beschwerden und Eingaben maßgeblich per E-Mail, häufig per Post und zu einem Teil per Fax oder persönlicher Vorsprache. Viele Bürgerinnen und Bürger nutzen erfreulicherweise auch das unter www.datenschutz-berlin.de/beschwerde.html bereitgestellte Beschwerdeformular für ihre Eingabe, was uns die Bearbeitung in den meisten Fällen erleichtert. Aufgrund der hohen Zahl von Eingaben ab Ende Mai dieses Jahres verzögerten sich zwischenzeitlich die von uns üblicherweise innerhalb von zwei Wochen versendeten Eingangsbestätigungen um einige Zeit. Der anfängliche Rückstau konnte trotz des nicht proportional zum Eingabevolumen angestiegenen Personalschlüssels in der Servicestelle Bürgereingaben durch Wochenendarbeit und die zeitweise Abordnung von Beschäftigten aus anderen Bereichen vorerst beseitigt werden. Allerdings führte dies dazu, dass Arbeit in den betroffenen anderen Bereichen liegen blieb, da hier kein Personalausgleich vorhanden war. Angesichts der erheblichen Zunahme von Eingaben ist eine ordnungsgemäße und zeitnahe Bearbeitung der Bürgerbeschwerden mit den vorhandenen Personalmitteln nicht mehr leistbar.

Inhaltlich orientieren sich die Beschwerden nah an denjenigen Rechten, die den betroffenen Personen von der DSGVO (wie auch zuvor in ähnlichem Umfang vom Bundesdatenschutzgesetz a. F.) garantiert werden, beschränken sich jedoch nicht auf diese. Viele Berlinerinnen und Berliner interessieren sich für die bei privaten Firmen wie öffentlichen Stellen zu ihrer Person gespeicherten Daten und stellen einen Antrag auf Selbstauskunft,[14] der leider häufig nicht, nicht vollständig oder nicht korrekt in der vorgeschriebenen Frist beantwortet wird. Oftmals wird gleichzeitig auch die Löschung der eigenen Daten beantragt; auch dieses von der DS-GVO garantierte Recht[15] wird leider häufig verletzt. Einige Internetunternehmen sehen zwar eine Löschungsmöglichkeit im Hinblick auf das Kundenkonto vor. Allerdings wird der hinterlegte Datenbestand in einigen Fällen weiter gespeichert und genutzt. Viele Personen beschweren sich auch über die generell ausufernde Erhebung ihrer Daten durch Ämter, private Unternehmen, Arztpraxen oder sonstige Personen (wie z. B. ihren Vermieter oder ihre Vermieterin). In zahlreichen Fällen steht diesen Bürgerinnen und Bürgern ein Widerspruchsrecht gegen die Verarbeitung der eigenen Daten zu,[16] bei dessen Durchsetzung wir den Betroffenen

14 Art. 15 DS-GVO
15 Art. 16, 17 DS-GVO
16 Art. 21 DS-GVO

genauso zur Seite stehen wie beim Verstoß datenverarbeitender Stellen gegen die Pflicht zur Information betroffener Personen über stattfindende Datenverarbeitungen.[17]

Das für betroffene Personen mit der DS-GVO neu geschaffene Recht auf Datenübertragbarkeit, wonach verantwortliche Stellen die Mitnahme der eigenen Daten ermöglichen müssen,[18] oder das Recht, nicht allein aufgrund einer automatisierten Datenverarbeitung einer bestimmten Entscheidung unterworfen zu werden,[19] machen bisher nur einen sehr geringen Teil der Eingaben aus.

In vielen Fällen steht nicht zwangsläufig ein böser Wille hinter einem eventuell vorliegenden Verstoß gegen Datenschutzrechte. Oftmals werden uns durch Beschwerden mitgeteilte Rechtsverstöße kurz nach unserer Einschaltung beseitigt. Bei weniger schwerwiegendem oder umgehend beseitigtem Fehlverhalten durch den Verantwortlichen belassen wir es in der Regel bei einer Verwarnung und verzichten auf weitere Maßnahmen.[20] Bei schwerwiegenderen Verstößen können wir zu anderen Maßnahmen wie Bußgeldern greifen.[21]

Nicht zuletzt dienen die eingehenden Beschwerden uns auch als Messinstrument dafür, was Bürgerinnen und Bürger gerade besonders häufig belastet. Gleichzeitig sind sie ein Gradmesser dafür, in welchen Geschäftsfeldern oder Bezirken aufgrund einer Vielzahl von Eingaben gerade eine negative Entwicklung zu beobachten und ggf. – mit den uns gegebenen Mitteln – auch aufzuhalten ist. Wir ermutigen daher alle Berlinerinnen und Berliner dazu, uns weiterhin durch die Meldung von Datenschutzverstößen bei deren Bekämpfung zu unterstützen.[22]

17 Art. 12, 13 DS-GVO
18 Art. 20 DS-GVO
19 Art. 22 DS-GVO
20 Art. 58 Abs. 2 lit. b DS-GVO
21 Siehe Kapitel 11
22 datenschutz-berlin.de/beschwerde.html.

1.3 Informationspflicht bei Datenpannen

Das neue Recht[23] sieht eine deutliche Erweiterung der Informationspflichten im Vergleich zur früheren Rechtslage[24] vor und gilt jetzt gleichermaßen für nicht öffentliche und öffentliche Stellen des Landes Berlin.[25] Früher waren im nicht öffentlichen Bereich nur bestimmte Kategorien von Daten wie Gesundheitsdaten und Bankkontoinformationen von der Meldepflicht umfasst, im öffentlichen Bereich bestand eine Meldepflicht bereits für alle Datenarten, in beiden Bereichen bestand die Meldepflicht aber nur bei drohenden schwerwiegenden Beeinträchtigungen der Rechte Betroffener.[26] Nunmehr ist gegenüber der Aufsichtsbehörde sowohl im öffentlichen als auch im nicht öffentlichen Bereich jede Verletzung des Schutzes personenbezogener Daten meldepflichtig. Diese Datenschutzverletzung ist definiert als „Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden".[27] Nach neuer Rechtslage sind also nicht nur die im früheren Sprachgebrauch gängigen „Datenlecks" durch Verlust der Vertraulichkeit umfasst, sondern auch der Verlust der Verfügbarkeit durch Vernichtung oder der Verlust der Integrität durch Veränderung von personenbezogenen Daten. Unerheblich ist, ob es sich um sensitive Daten handelt, die nach Art. 9 DS-GVO einem besonderen Schutz unterliegen. Der Verantwortliche ist nur dann nicht meldepflichtig gegenüber der Aufsichtsbehörde, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.[28]

23 Art. 33, 34 DS-GVO

24 Zu § 42a Bundesdatenschutzgesetz (BDSG) a. F. siehe JB 2010, 12.2; zu § 18a Berliner Datenschutzgesetz (BlnDSG) a. F. siehe JB 2011, 11.2.1

25 Die korrespondierenden Vorschriften für die Bereiche Polizei und Justiz sind §§ 51, 52 BlnDSG in Umsetzung der sog. JI-Richtlinie (EU) 2016/680; siehe hierzu JB 2017, 3.1

26 § 42a BDSG a. F.; § 18a Abs. 1 BlnDSG a. F.

27 Art. 4 Nr. 12 DS-GVO

28 Siehe hierzu Kurzpapier Nr. 18 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, „Risiko für die Rechte und Freiheiten natürlicher Personen", abrufbar unter www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/kurzpapiere/

Diese deutliche Verschärfung der Rechtslage war wahrscheinlich der Hauptgrund für den massiven Anstieg der Meldung von Datenpannen bei uns. Während im gesamten Jahr 2017 51 Meldungen[29] bei uns eingegangen waren, gab es im Berichtszeitraum 357 Meldungen, davon 332 Meldungen seit 25. Mai 2018.[30] Die Anzahl der Meldungen hat sich auf diesem hohen Niveau eingependelt, ein Rückgang ist nicht erkennbar. Für uns ist eindeutig, dass der Datenschutz auch wegen dieser erweiterten Meldepflichten stärker in den Fokus der Verantwortlichen gerückt ist, zumal bei Verstößen gegen die Meldepflicht Sanktionsregelungen[31] vorgesehen sind. Dagegen dürfen die durch die Meldung erhaltenen Informationen nicht dazu genutzt werden, die der Meldung zugrunde liegende Datenschutzverletzung zu sanktionieren.[32] Mehrfache gleichgelagerte Verstöße, insbesondere solche, die auf strukturelle Mängel beim Verantwortlichen zurückgeführt werden können, könnten uns aber zu einer Betriebsprüfung veranlassen.

Beispielhaft seien folgende Meldungen skizziert, die uns erreicht haben: So teilte eine Jugendhilfeeinrichtung den Diebstahl eines USB-Sticks mit biografischen Daten der stationär betreuten Jugendlichen mit, ein Betriebsarzt verschickte einen Befund an den falschen Adressaten und zwei Hotels konnten nach einem Hackerangriff auf eine Buchungsplattform nicht ausschließen, dass Kreditkartendaten an Unbefugte gerieten. Weitere zahlreiche Meldungen betrafen die Nutzung von offenen E-Mail-Verteilern, wodurch nicht nur die persönlichen, u. U. „sprechenden" E-Mail-Adressen[33] wechselseitig kundgetan wurden, sondern zugleich sensible Daten wie die Tatsache der Gewerkschaftszugehörigkeit (so geschehen bei einer Gewerkschaft). Zunehmend erreichten uns auch Meldungen zu fremdinstallierter Schadsoftware wie Krypto-Trojanern. Damit werden die in den technischen Systemen liegenden Dateien von Unbefugten verschlüsselt, um für die

29 44 Meldungen im nicht öffentlichen Bereich, 7 Meldungen im öffentlichen Bereich

30 295 Meldungen im nicht öffentlichen Bereich, 37 Meldungen im öffentlichen Bereich (Stand: 31. Dezember 2018)

31 Nach Art. 83 Abs. 4 lit. a i. V. m. Art. 33 DS-GVO beträgt die Geldbuße bis zu 10 Mio. Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist.

32 Siehe § 43 Abs. 4 BDSG. Die Bestimmung ist Ausdruck des verfassungsrechtlichen Verbots des Zwangs zur Selbstbezichtigung und „Nachfolgeregelung" von § 42a Satz 6 BDSG a. F.

33 E-Mail-Adressen werden als „sprechend" bezeichnet, wenn sie Vor- und Nachnamen enthalten.

Entschlüsselung Geld zu erpressen – bei medizinischen Daten in einer Arztpraxis aus naheliegenden Gründen geradezu ein GAU.[34]

1.3.1 Pflichten gegenüber der Aufsichtsbehörde

Rechtsgrundlage für die Meldepflicht des Verantwortlichen gegenüber uns als Aufsichtsbehörde ist Art. 33 DS-GVO. Danach meldet der Verantwortliche die Datenschutzverletzung unverzüglich und möglichst binnen 72 Stunden, nachdem sie ihm bekannt wurde. Diese Frist umfasst die Wochenenden und Feiertage.[35] Eine spätere Meldung muss eine Begründung für die Verzögerung enthalten. In den allermeisten Fällen erfolgte die Meldung uns gegenüber fristgerecht, bei verspäteten Meldungen zumeist mit nachvollziehbarer Begründung für die Verspätung. In einem Fall war sie jedoch nicht akzeptabel: So war die Berufung einer öffentlichen Stelle auf Urlaub, Krankheit, erhöhtes Arbeitsaufkommen, ungeklärte Zuständigkeiten und mehrfach für notwendig erachtete interne Rücksprachen auch in der Summe nicht geeignet, die zweimonatige Verspätung der Meldung zu rechtfertigen. Wir haben organisatorische Verbesserungen angemahnt, die den reibungslosen und fristgerechten Meldeweg bei der verantwortlichen Stelle künftig gewährleisten.

Zu beachten ist, dass Verantwortliche nicht verpflichtet sind, alle Informationen zur gleichen Zeit bereitzustellen. Vielmehr können die Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung gestellt werden.[36]

Zur Erleichterung des Meldevorgangs haben wir ein Formular mit Ausfüllhilfe ins Internet eingestellt, das von Verantwortlichen inzwischen ganz überwiegend genutzt wird. Eine Leitlinie des Europäischen Datenschutzausschusses (EDSA) gibt

34 **G**rößter **A**nzunehmender **U**nfall

35 Art. 3 Abs. 3 Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine, ABl. Nr. L 124 vom 8. Juni 1971, S. 1 f.

36 Art. 33 Abs. 4 DS-GVO

wertvolle Hinweise zur Auslegung der neuen Regelungen und darüber hinaus Beispiele für meldepflichtige Vorfälle.[37]

1.3.2 Pflichten gegenüber den Betroffenen

Nach Art. 34 DS-GVO muss der Verantwortliche die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten benachrichtigen, wenn die Datenpanne voraussichtlich zu einem hohen Risiko für die betroffene Person führt. Während die Mitteilung an uns als Aufsichtsbehörde im Fall einer Datenpanne also den Regelfall darstellt, ist dies die Benachrichtigung der Betroffenen eher nicht. Denn im ersten Fall wird „nur" ein Risiko, im zweiten Fall aber ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person vorausgesetzt.

Hierfür kommt es auf eine Gefahrenprognose an, die vor allem das abstrakte Missbrauchsrisiko (anhand der Art der betroffenen Daten) und die konkrete Missbrauchsgefahr (anhand der konkreten potenziellen Auswirkungen der Datenschutzverletzung) berücksichtigt. Ein solches hohes Risiko kann, wenn es sich um die früheren „Katalogdaten"[38] handelt, vom Verantwortlichen nicht von vornherein ausgeschlossen werden. Vielmehr bedarf es einer (dokumentierten) Begründung, warum bei diesen Daten voraussichtlich kein hohes Risiko für die Betroffenen besteht. Nicht ausreichend ist z. B. die häufige Begründung, dass es dem Dieb eines hochwertigen Laptops nur um das weiter zu veräußernde Gerät ging, die Daten zuvor aber mit Sicherheit gelöscht würden. Dass ein Verantwortlicher dies aber nicht beeinflussen kann, liegt auf der Hand; er kann das hohe Risiko also nicht ausschließen. Deshalb raten wir insbesondere bei sensitiven Daten zu einer vorsorglichen Benachrichtigung der Betroffenen.

37 Formular, Ausfüllhilfe und Leitlinie (WP 250 rev. 01) sind abrufbar unter www.datenschutz-berlin.de/wirtschaft-und-verwaltung/meldung-einer-datenpanne/.

38 Das sind die Datenkategorien im früheren § 42a BDSG, also sensitive Daten wie z. B. Gesundheitsdaten, Daten, die einem Berufsgeheimnis unterliegen, Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten bzw. auf einen diesbezüglichen Verdacht beziehen, sowie Bankkonto- und Kreditkarteninformationen.

Auch in den übrigen Fällen empfehlen wir den Verantwortlichen grundsätzlich, die Betroffenen – ungeachtet einer etwaigen Benachrichtigungspflicht nach Art. 34 DS-GVO – über den Vorfall zu informieren. Unser Anliegen bei dieser Empfehlung ist es, dass gegenüber den Betroffenen möglichst schnell größtmögliche Transparenz hergestellt wird – nicht nur, weil der Transparenzgedanke eine der Säulen der DS-GVO ist. Unsere Erfahrungen zeigen, dass Betroffene es bei allem Unmut über den Datenschutzverstoß ganz überwiegend anerkennen, wenn der Verantwortliche zu seinem Fehler steht und sie von sich aus und vor allem zeitnah informiert. Die Mehrzahl der Verantwortlichen ist unserer Empfehlung gefolgt.

In bestimmten Fällen besteht trotz voraussichtlich hohen Risikos keine Pflicht zur Benachrichtigung der Betroffenen.[39] Das ist z. B. der Fall, wenn der abhandengekommene Datenträger ausreichend verschlüsselt war. Wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre, hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die Betroffenen vergleichbar wirksam informiert werden. Von dieser Möglichkeit haben mehrere Verantwortliche auf unseren Hinweis hin Gebrauch gemacht. So hat ein Aussteller bei einer Automesse, nachdem auf dem Postweg Anträge mit Kontoinformationen von Abo-Interessenten abhandengekommen waren, auf seiner Homepage über mehrere Wochen eine entsprechende Information bereitgehalten. Ein Professor einer Hochschule hat nach dem während der Pause erfolgten Diebstahl seines Laptops aus dem Seminarraum einen Aushang im Fachbereich angebracht, mit dem auch auf das Abhandenkommen von Zeugnisdaten hingewiesen wurde. Auch eine Anzeige in einer Tageszeitung kann als wirksame öffentliche Bekanntmachung in Frage kommen.

Im Ergebnis haben sich die meisten Verantwortlichen im Anschluss an die Meldung bei uns kooperativ verhalten.

39 Art. 34 Abs. 3 DS-GVO

1.4 Datenschutz-Zertifizierung – Der Weg zum Datenschutz-Siegel

Wenn Unternehmen ihre Kunden und Geschäftspartner davon überzeugen wollen, dass sie Datenschutz ernst nehmen und umsetzen, dann bieten ihnen Datenschutz-Siegel dafür einen Weg. Diese Siegel können von privaten Zertifizierungsstellen ausgestellt werden. Wir beteiligen uns an dem Prozess, Zertifizierungsstellen für ihre Tätigkeit zuzulassen und zu überwachen.

Wenn Kunden oder Geschäftspartner entscheiden, sich auf eine Geschäftsbeziehung mit einem Unternehmen einzulassen, haben sie häufig das Bedürfnis, sich einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen zu verschaffen. Unternehmen, die in einen gesetzeskonformen oder besonders datenschutzfreundlichen Betrieb ihrer Datenverarbeitungen investiert haben, möchten dies nach außen darstellen. Datenschutz-Zertifikate und -Siegel kommen beiden Bedürfnissen entgegen.

Auch schon vor der Gültigkeit der Datenschutz-Grundverordnung (DS-GVO) gab es solche Zertifikate. Doch blieb oft intransparent, welche Aussagekraft sie tatsächlich besitzen und wie gründlich die Aussteller der Zertifikate die zertifizierte Dienstleistung oder das zertifizierte Produkt tatsächlich geprüft haben.

Die DS-GVO schafft hier Transparenz: Zertifizierungsstellen müssen sich einem Akkreditierungsprozess stellen. Die Kriterien, die sie bei der Zertifizierung anlegen, bedürfen der Genehmigung durch die Aufsichtsbehörden und ggf. des Europäischen Datenschutzausschusses und sind öffentlich verfügbar. Wenn eine Zertifizierungsstelle eine Datenverarbeitung positiv beurteilt und zertifiziert, dann muss sie dies der zuständigen Aufsichtsbehörde mitteilen. Sieht diese die Zertifizierungskriterien nicht als erfüllt an, so kann sie die Ausstellung der Zertifikate unterbinden oder ausgestellte Zertifikate widerrufen lassen. Auch die Akkreditierung einer Zertifizierungsstelle kann widerrufen werden.

Im Ergebnis ist allen geholfen: Bürgerinnen und Bürger können leichter einschätzen, ob Produkte, Prozesse und Dienstleistungen von Unternehmen ein ausreichendes Datenschutzniveau bieten. Auch Unternehmen, die Auftragsverarbeiter

wie Cloud-Dienstleister oder Aktenvernichter beauftragen wollen, erhalten durch die Zertifikate die Sicherheit für sich und ihre Kunden, DS-GVO-konforme Dienstleistungen zu nutzen, selbst dann, wenn der Auftragsverarbeiter außerhalb der EU ansässig ist. Der Nachweis datenschutzkonformer Datenverarbeitung wird dadurch erleichtert.

Unternehmen, die selbst Verarbeiter oder Auftragsverarbeiter sind, können durch die Zertifikate aufzeigen, dass sie datenschutzkonforme Dienstleistungen anbieten. Dieser erleichterte Nachweis der Beachtung datenschutzrechtlicher Anforderungen kann Wettbewerbsvorteile bringen.

1.4.1 Zertifizierung und Akkreditierung

Ein aussagekräftiges Zertifikat steht am Ende eines umfangreichen Zertifizierungsprozesses.

Aus dem Zertifikat geht hervor,

- welcher Gegenstand, d.h. welches Produkt, welcher Prozess oder welche Dienstleistung (Zertifizierungsgegenstand) zertifiziert wurde,
- wo man nachlesen kann, welche Eigenschaften der Zertifizierungsgegenstand mindestens gewährleisten muss,
- in welchem Rahmen das Zertifikat gilt,
- wann es ausgestellt wurde und wie lange es gilt sowie
- wer die Zertifizierung durchgeführt hat.

Das Zertifikat weist die Vereinbarkeit des Zertifizierungsgegenstandes mit den Anforderungen der DS-GVO aus. Zertifizierbar nach der gegenwärtigen Gesetzeslage[40] sind Produkte, Prozesse und Dienstleistungen, bei denen personenbezogene Daten verarbeitet werden.

40 Art. 43 Abs. 1 lit. b DS-GVO verweist auf EN-ISO/IEC 17065/2012, die Anforderungen an Stellen vorsieht, die Produkte, Prozesse und Dienstleistungen zertifizieren.

Um die notwendige Qualität und damit auch Vertrauenswürdigkeit zu gewährleisten, sieht die DS-GVO vor, dass nur ausreichend qualifizierte Zertifizierungsstellen Datenschutz-Zertifikate ausstellen dürfen. Die Qualifizierung der Zertifizierungsstellen wird durch deren vorherige Akkreditierung und eine regelmäßige Überwachung gewährleistet.

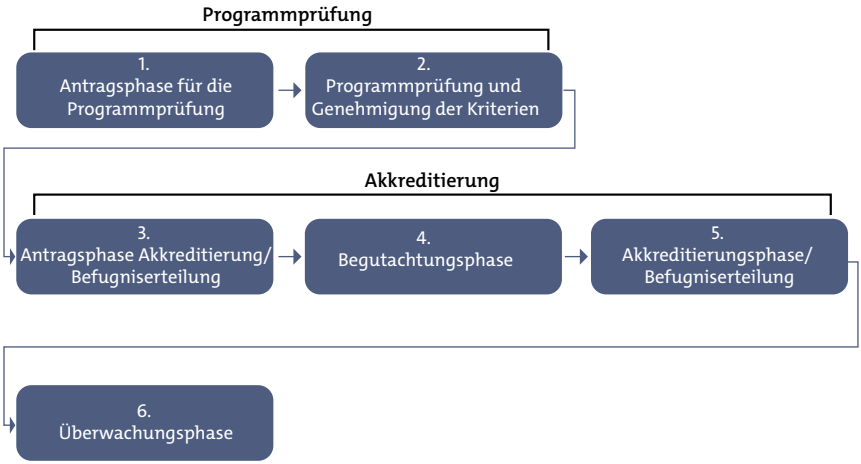
Akkreditierung bedeutet, dass eine potenzielle Zertifizierungsstelle selbst eine Prüfung bestanden hat und damit die Erlaubnis zum Zertifizieren bekommt. Um akkreditiert zu werden, muss die Zertifizierungsstelle zunächst die Kriterien benennen, die sie für ihre Zertifizierungen als Maßstab anlegen möchte. Diese Kriterien legt sie der Aufsichtsbehörde vor, die sie bewertet und genehmigt, wenn sie ausreichen, um eine gesetzeskonforme Datenverarbeitung festzustellen. Hauptmaßstab ist hierbei die DS-GVO. Weitere gesetzliche Regelungen müssen je nach der Art des Zertifizierungsgegenstands und den Umständen seines Einsatzes zusätzlich berücksichtigt werden. Dies können das BDSG, die Landesdatenschutzgesetze und bereichsspezifische Vorschriften sein, z. B. aus dem Sozialrecht oder berufsrechtliche Regelungen zum Schutz der Geheimnisse von Patientinnen und Patienten. Über die gesetzlichen Regelungen hinaus können die Zertifizierungskriterien auch auf nationale und internationale Normen Bezug nehmen, z. B. auf die Normen der Internationalen Organisation für Standardisierung (ISO) für die Sicherheit von Informationstechnik.

Zum anderen muss die Zertifizierungsstelle Anforderungen in Bezug auf eine ausreichende fachliche Qualifikation ihrer Beschäftigten, eine geeignete organisatorische Struktur sowie auf sauber definierte Prozesse und Unparteilichkeit bzw. Unabhängigkeit erfüllen. Dafür gibt es eine allgemeine internationale Norm, die EN-ISO/IEC 17065/2012, die für die Akkreditierung von Zertifizierungsstellen in ganz verschiedenen Sachgebieten gilt, vom Bio-Landbau bis zu Baustoffen für die Errichtung von Gebäuden. Es war eine wichtige Aufgabe der deutschen und anderen europäischen Aufsichtsbehörden im Jahr 2018, diese Norm um Anforderungen zu ergänzen, die spezifisch für die Datenschutz-Akkreditierung gelten sollen. Die Berliner Aufsichtsbehörde hat sich hieran intensiv beteiligt. Erarbeitet wurde eine vorläufige ergänzte Fassung der Norm, die nunmehr (Stand Dezember 2018) dem Europäischen Datenschutzausschuss zur Stellungnahme zugeleitet wurde.

1.4.2 Ablauf des Akkreditierungsprozesses

Bei dem Prozess der Akkreditierung von Zertifizierungsstellen arbeiten die Aufsichtsbehörden und die Deutsche Akkreditierungsstelle (DAkkS) eng zusammen.[41] Die DAkkS steuert den Gesamtprozess der Akkreditierung, nimmt die Anträge entgegen, übernimmt die formalen Prüfungsschritte. Die Aufsichtsbehörden prüfen und genehmigen die Zertifizierungskriterien, überprüfen neben den praktischen Gegebenheiten insbesondere die Unabhängigkeit der Antragsteller und ihr Fachwissen und entscheiden zusammen mit der DAkkS, ob eine Akkreditierung erteilt wird oder nicht. Nach einer positiven Entscheidung erteilen sie den Antragstellern die Befugnis, als Zertifizierungsstelle tätig zu werden.

Im Einzelnen verläuft die Akkreditierung wie folgt:



Dem eigentlichen Akkreditierungsverfahren ist eine Programmprüfung vorgeschaltet. Im Rahmen der Programmprüfung geht es um die Zertifizierungskriterien (**was** soll das zu zertifizierende Unternehmen nach Vorstellung der Zertifizierungsstelle tun?) und das vorgesehene Vorgehen der Zertifizierungsstelle (**wie** will die Zertifizierungsstelle feststellen, ob die Kriterien eingehalten werden?).

41 Art. 43 DS-GVO, § 39 BDSG

Die Kriterien und die Begleitprozesse bilden zusammen das Zertifizierungsprogramm, daher der Name dieser Phase.

Die deutschen Aufsichtsbehörden arbeiten bei der Erstellung der Anforderungen und Verfahren für die Beurteilung von Zertifizierungskriterien und -programmen ebenfalls eng zusammen. Dadurch soll eine Vergleichbarkeit von Akkreditierungen der einzelnen Aufsichtsbehörden erzielt werden. Ferner soll durch ein systematisches Vorgehen bei der Programmprüfung die notwendige Qualität der Zertifizierungsprogramme mit ihren Zertifizierungskriterien gewährleistet werden. Damit wird zugleich auch die Prüftransparenz gesichert.

Wenn ein Europäisches Datenschutz-Siegel angestrebt wird, ist zusätzlich eine Genehmigung der Zertifizierungskriterien durch den Europäischen Datenschutzausschuss erforderlich.[42]

Der eigentliche Akkreditierungsprozess beginnt mit der Einsendung des Akkreditierungsantrags an die DAkkS. Bei der Überprüfung des Antrags bindet diese die zuständige Aufsichtsbehörde als Befugnis erteilende Behörde in das Akkreditierungsverfahren ein.

An die Dokumentenprüfung schließt sich die Begutachtung an. Im Zuge der Begutachtung prüft die zuständige Aufsichtsbehörde gemeinsam mit der DAkkS durch ein Begutachterteam die Erfüllung der Anforderungen an die Zertifizierungsstelle vor Ort. Schließlich überzeugt sich das Begutachterteam von der Qualität der Tätigkeit der Zertifizierungsstelle durch ihre Begleitung bei der Auditierung eines exemplarischen Kunden.

Nach Dokumentenprüfung und Begutachtung bewertet ein Akkreditierungsausschuss die Begutachtungsergebnisse und entscheidet über die Erteilung der Akkreditierung. Dieser Ausschuss besteht zu zwei Dritteln aus Mitgliedern der zuständigen Aufsichtsbehörde und zu einem Drittel aus Mitgliedern der DAkkS. Die DAkkS bescheinigt den erfolgreichen Abschluss der Akkreditierungsphase durch einen Akkreditierungsbescheid und die Akkreditierungsurkunde. Die Akkreditie-

42 Art. 42 Abs. 5 Satz 2, Art. 70 Abs. 1 lit. o DS-GVO

rung wird anschließend in das Verzeichnis der akkreditierten Stellen der DAkkS aufgenommen.

Eine Akkreditierung erfolgt gemäß Art 43 Abs. 4 DS-GVO befristet für maximal fünf Jahre und kann bei fortbestehendem Vorliegen der Kriterien verlängert werden.

Auf Grundlage der erfolgreichen Akkreditierung kann die zuständige Aufsichtsbehörde der Zertifizierungsstelle die Befugnis erteilen, bundesweit mit dem Zertifizierungsprogramm ohne weitere Anerkennungsverfahren anderer Aufsichtsbehörden tätig zu sein.

Die Kompetenz einer Stelle wird auch nach einer erteilten Akkreditierung in regelmäßigen Abständen durch die DAkkS und die zuständige Aufsichtsbehörde überwacht. Auf diesem Weg wird sichergestellt, dass die Zertifizierungsstelle die jeweiligen Akkreditierungsanforderungen dauerhaft erfüllt. Werden bei den Kontrollbegutachtungen Abweichungen festgestellt, kann dies zur Einschränkung, Aussetzung oder Aufhebung der Akkreditierung führen. Dies kann auch Auswirkungen auf bereits erteilte Zertifikate haben.

1.4.3 Beobachtung der Zertifizierung und Fortentwicklung der Anforderungen

Auch die erteilten Zertifizierungen sind durch die Aufsichtsbehörden regelmäßig zu überprüfen.[43] Hierzu informieren die akkreditierten Zertifizierungsstellen die zuständige Aufsichtsbehörde über die Erteilung, Verlängerung oder den Widerruf beantragter Zertifizierungen.[44] Werden die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt, kann die zuständige Aufsichtsbehörde die Zertifizierungsstelle anweisen, eine Zertifizierung nicht zu erteilen oder zu widerrufen.[45]

Auch Akkreditierungen werden im Rahmen von Zwischenprüfungen regelmäßig überprüft. Dies schließt Prüfungen auf Dokumentenebene und vor Ort ein.

43 Art. 57 Abs. 1 lit. o DS-GVO
44 Art. 43 Abs. 1 Satz 1, Abs. 5 DS-GVO
45 Art. 58 Abs. 2 lit. h DS-GVO

Damit sind die Aufsichtsbehörden künftig dauerhaft in die Prozesse von Akkreditierung und Zertifizierung involviert. Die Anforderungen an Kriterien und Programme müssen regelmäßig an die künftigen Entwicklungen angepasst werden. Dafür haben die Datenschutzaufsichtsbehörden einen Arbeitskreis eingerichtet, der an der kontinuierlichen Entwicklung des Akkreditierungsprozesses im Bereich Datenschutz arbeitet.

Durch regelmäßige Arbeitstreffen mit der DAkkS wird eine reibungslose Zusammenarbeit gewährleistet. Aktuelle Entwicklungen im Bereich der Akkreditierung und des Datenschutzes können zeitnah berücksichtigt werden.

Nicht nur durch die Beteiligung an den Zertifizierungsprozessen, sondern auch durch das Erstellen von Informationsmaterialien und durch Vorträge leistet die Berliner Beauftragte für Datenschutz und Informationsfreiheit einen Beitrag zur Erfüllung des gesetzlichen Auftrags,[46] die Einführung von datenschutzspezifischen Zertifizierungsverfahren zu fördern.

Zertifikate, Datenschutz-Siegel und -prüfzeichen werden künftig ein Qualitätsmerkmal für Verarbeitungen personenbezogener Daten sein. Damit wird den Bürgerinnen und Bürgern ein Instrument zur besseren Orientierung in einem sowohl dynamischen als auch grundrechtsrelevanten Bereich an die Hand gegeben. Unternehmen können damit die Ausrichtung ihrer Prozesse, Produkte und Dienstleistungen an den Anforderungen der DS-GVO belegen. Durch die Genehmigung von Zertifizierungskriterien, das Akkreditierungsverfahren, die Erteilung der Befugnis, als Zertifizierungsstelle tätig zu werden, sowie durch die regelmäßige Kontrolle der akkreditierten Unternehmen und Überwachung der erteilten Zertifizierungen durch die Aufsichtsbehörden und die DAkkS wird künftig die Qualität von Zertifikaten im Bereich Datenschutz gesichert.

46 Art. 42 Abs. 1 DS-GVO

1.5 Werbung nach der DS-GVO

Zahlreiche Beschwerden erreichen uns von Bürgerinnen und Bürgern, die in ihrem Briefkasten an sie adressierte Werbesendungen vorfinden oder auch Werbung per E-Mail, Telefax, SMS oder als Anruf erhalten, obwohl sie den Werbenden zuvor keine Einwilligung dafür erteilt haben. Mitunter hatten sie noch gar keinen Kontakt zu den Werbenden und fragen sich, woher diese ihre Kontaktdaten erhalten haben. Auch Werbende, die unsicher sind, wie sich die Datenschutz-Grundverordnung auf geplante Werbemaßnahmen auswirkt und ob und in welchem Umfang sie Daten künftig für Werbemaßnahmen verwenden dürfen, wenden sich verstärkt mit Beratungsanfragen an uns.

1.5.1 Definition

Der Begriff der Werbung umfasst nach europäischer Definition alle Maßnahmen von Unternehmen, Selbstständigen, Verbänden und Vereinen mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen zu fördern.[47] Damit ist außer der unmittelbar produktbezogenen Werbung auch die mittelbare Absatzförderung – beispielsweise in Form der Imagewerbung oder des Sponsorings – erfasst. Unter den Werbebegriff fallen neben klassischen Werbebroschüren und -katalogen auch Weihnachts- und Geburtstagspost, Newsletter und Kundenzufriedenheitsabfragen.[48]

Die verschiedenen Anspracheformen bzw. Kommunikationskanäle von persönlich adressierter Werbung per Post, E-Mail, Fax oder in telefonischer Form sind datenschutzrechtlich unterschiedlich zu beurteilen.

47 Art. 2 lit. a der Richtlinie 2006/114/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über irreführende und vergleichende Werbung (ABl. EU L 376 S. 21)

48 Siehe Urteil des Bundesgerichtshofs (BGH) vom 12. September 2013 – I ZR 208/12 sowie BGH-Urteil vom 10. Juli 2018 – VI ZR 225/17, abrufbar unter http://www.bundesgerichtshof.de/DE/Entscheidungen/entscheidungen_node.html

1.5.2 Neuregelungen

Mit Inkrafttreten der DS-GVO sind die bisherigen detaillierten Regelungen zur Werbung entfallen.[49] Die DS-GVO enthält keine spezielle Systematik für die Zulässigkeit von Werbung, daher sind im Grundsatz die in ihr enthaltenen allgemeinen Bestimmungen für die Verarbeitung personenbezogener Daten anzuwenden. Nach wie vor gilt, dass Werbung nur dann erlaubt ist, wenn entweder eine gesetzliche Erlaubnis oder eine Einwilligung der beworbenen Person vorliegt.

Die Verarbeitung von personenbezogenen Daten durch Werbende kann rechtmäßig sein, wenn diese zur Wahrung der berechtigten Interessen der Werbenden oder von Dritten erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der Werbeempfänger überwiegen. Dies gilt in besonderem Maße auch dann, wenn es sich bei der betroffenen Person um ein Kind handelt.[50] Die betroffene Person darf dabei der Direktwerbung nicht widersprochen haben. Die Datenschutz-Grundverordnung sieht ein explizites Widerspruchsrecht vor.[51]

In jedem konkreten Einzelfall ist zudem eine Abwägung der Interessen der Werbenden bzw. der Dritten als auch der Betroffenen vorzunehmen. Direktwerbung kann grundsätzlich als eine einem berechtigten Interesse dienende Verarbeitung personenbezogener Daten betrachtet werden.[52] Jedoch ist für die erforderliche Interessenabwägung stets auch zu fragen, was Beworbene objektiv vernünftigerweise erwarten können oder dürfen. Entscheidend ist daher, ob die Verarbeitung personenbezogener Daten für bestimmte Bereiche der Sozialsphäre typischerweise akzeptiert oder abgelehnt wird und ob es der Vernunft entspricht, Nachteile für das Selbstbestimmungsrecht hinzunehmen.

Die Werbenden müssen nachweisen können, dass sie diese Interessenabwägung tatsächlich durchgeführt haben und dass das Ergebnis zu ihren Gunsten ausfällt. Weiterhin müssen sie die in die Abwägung einfließenden Interessen gegenüber den Betroffenen ausdrücklich benennen.[53] Dies kann beispielsweise im Rahmen

49 § 28 Abs. 3 BDSG a. F.
50 Art. 6 Abs. 1 lit. f DS-GVO
51 Art. 21 DS-GVO
52 Erwägungsgrund 47 DS-GVO
53 Art. 5 Abs. 2, Art. 13 Abs. 1 lit. d DS-GVO

der Datenschutzerklärung erfolgen. Informieren die Werbenden im Zeitpunkt der Datenerhebung transparent und umfassend über eine vorgesehene werbliche Nutzung der Daten, geht die Erwartung der Beworbenen in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden. Allerdings kann durch Transparenz der gesetzliche Abwägungstatbestand nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO nicht beliebig erweitert werden, da die Erwartungen an dem objektiven Maßstab der Vernunft gemessen werden müssen.

In diesem Zusammenhang sind stets auch die allgemeinen Grundsätze der DS-GVO[54] zu beachten. So muss die Datenverarbeitung fair und nachvollziehbar (Nennung der Quellen der Daten) sein.

Sofern es anhand eines Selektionskriteriums zu einer Einteilung in Werbegruppen kommt und sich kein zusätzlicher Erkenntnisgewinn aus der Gruppierung ergibt, wird die Interessenabwägung in der Regel zugunsten der Werbenden ausfallen. Schutzwürdige Interessen dürften hingegen in der Regel nicht überwiegen, wenn im Nachgang zu einer Bestellung allen Kundinnen und Kunden gleichermaßen postalisch ein Werbekatalog oder ein Werbeschreiben zum Kauf weiterer Produkte der Werbenden zugesendet wird.

Die Erstellung von Werbeprofilen oder die Entnahme von Daten aus sozialen Netzwerken für Zwecke der Direktwerbung wird hingegen nur nach vorheriger Einwilligung erlaubt sein. Eingriffsintensivere Maßnahmen, wie automatisierte Selektionsverfahren zur Erstellung detaillierter Profile, Verhaltensprognosen bzw. Analysen, die zu zusätzlichen Erkenntnissen führen, sprechen ebenfalls dafür, dass das Interesse der Beworbenen am Ausschluss der Datenverarbeitung überwiegt. In diesen Fällen handelt es sich um sog. Profiling, das die Einholung einer Einwilligung vor der Datenverarbeitung erforderlich macht. Ein Hinweis auf ein bestehendes Widerspruchsrecht reicht in diesen Fällen nicht aus.

Hinsichtlich der Übermittlung von Daten für Werbezwecke an Dritte sowie der Nutzung von Fremdadressen ist im Regelfall davon auszugehen, dass den Interessen der beworbenen Personen ein höherer Stellenwert einzuräumen ist als dem Interesse der Werbenden bzw. von Dritten an der Übermittlung bzw. Nutzung von

54 Art. 5 Abs. 1 DS-GVO

Fremdadressen zur Werbung. Die Erwartungshaltung der betroffenen Personen wird auch davon bestimmt, ob eine maßgebliche und angemessene Beziehung zwischen ihnen und den Werbenden besteht, z. B. eine Kundenbeziehung. Bei einer Weitergabe von personenbezogenen Daten an außerhalb dieser Kundenbeziehung stehende Dritte ist dies regelmäßig nicht der Fall. Normalerweise werden Kundinnen und Kunden nicht erwarten, dass ihre Kontaktdaten von Unternehmen, bei denen sie z. B. eingekauft haben, an Adresshändler zu Werbezwecken verkauft werden, ohne dass sie gefragt werden.

1.5.3 Einwilligung

Eine Verarbeitung zu Werbezwecken kann auch weiterhin auf eine freiwillige und unabhängige Einwilligung der beworbenen Person gestützt werden.

Die Einwilligung muss dabei durch eine eindeutige bestätigende Handlung in schriftlicher, elektronischer oder auch mündlicher Form vorgenommen werden.[55] Stillschweigen, bereits voreingestellte, angekreuzte Kästchen oder auch eine Untätigkeit der betroffenen Person genügen dafür nicht. Zu beachten sind in diesem Zusammenhang jedoch insbesondere die neuen Informations- und Dokumentationspflichten der Verantwortlichen.[56] Den betroffenen Personen sind die Informationen in transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache vorzulegen.[57] Die beworbene Person muss zudem immer auf die Möglichkeit eines Widerrufs hingewiesen werden.[58]

Eine Einwilligung kann insbesondere dann unwirksam sein, wenn ein starkes Ungleichgewicht zwischen den Verantwortlichen und den betroffenen Personen besteht.[59] Auch kann die Kopplung einer Dienstleistung mit einer hierfür nicht notwendigen Datenverarbeitung gegen die Freiwilligkeit einer Einwilligung spre-

55 Erwägungsgrund 32 DS-GVO

56 Siehe dazu auch das Working Paper (WP 260) der Art.29-Gruppe, abrufbar unter http://ec.europa.eu/newsroom/article29/news-overview.cfm

57 Art. 12 Abs. 1 DS-GVO

58 Art. 7 Abs. 3 sowie Art. 21 Abs. 3 und 4 DS-GVO

59 Erwägungsgrund 43 DS-GVO

chen.[60] Die Wirksamkeit der Einwilligung wird auch dann verneint, wenn die Beworbenen diese nicht nach einzelnen Verarbeitungsvorgängen getrennt erteilen können, obwohl dies im konkreten Fall angebracht wäre.

Es obliegt den Werbenden, die Einhaltung der Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung und das Vorliegen einer rechtswirksamen Einwilligung nachzuweisen.[61] Zwar enthält die DS-GVO anders als das alte Bundesdatenschutzgesetz diesbezüglich kein Schriftformerfordernis mehr. Um jedoch dieser Verpflichtung nachkommen zu können, ist anzuraten, sich regelmäßig um eine Einwilligung in Schriftform mit handschriftlicher Unterschrift oder mindestens in Textform (z. B. E-Mail) zu bemühen. Für das elektronische Erklären einer Einwilligung ist zum Nachweis das sog. Double-Opt-In-Verfahren geboten (je nach konkreter Art des Kontaktes: E-Mail oder SMS), wobei die rechtlichen Nachweis-Anforderungen bei der Protokollierung zu berücksichtigen sind. Festzuhalten sind der Inhalt der Einwilligung und das gesamte Opt-In-Verfahren.[62]

1.5.4 Zweckänderung

Personenbezogene Daten, welche ursprünglich nicht zu Werbezwecken erhoben wurden, können dennoch für Werbezwecke verwendet werden, sofern der neue Zweck mit der ursprünglichen Zweckbestimmung vereinbar ist.[63] Dazu müssen Verantwortliche einen sog. Kompatibilitätstest unter Berücksichtigung der in der DS-GVO geregelten Kriterien durchführen.[64] Anderenfalls ist eine Einwilligung erforderlich.

60 Art. 7 Abs. 4 DS-GVO

61 Art. 5 Abs. 2 und Art. 7 Abs. 1 DS-GVO

62 Art. 5 Abs. 2 DS-GVO und BGH-Urteil vom 10. Februar 2011, I ZR 164/09, abrufbar unter http://www.bundesgerichtshof.de/DE/Entscheidungen/entscheidungen_node.html

63 Art. 6 Abs. 4 DS-GVO

64 Erwägungsgrund 50 DS-GVO

1.5.5 Gesetz gegen den unlauteren Wettbewerb und DS-GVO

Unabhängig vom Datenschutzrecht sind bei E-Mail-Werbung und sonstiger Werbung mit elektronischer Post sowie bei Telefon- und Faxwerbung die Vorschriften des Gesetzes gegen den unlauteren Wettbewerb (UWG) zu beachten, die auch nach den Neuregelungen der DS-GVO weiterhin anwendbar bleiben. Diese regeln, in welchen Fällen von einer unzumutbaren Belästigung der Beworbenen auszugehen und eine Werbung dieser Art unzulässig ist. Wenn das UWG für bestimmte Werbeformen und Kontaktwege eine unzumutbare Belästigung erkennt, ist dies im Rahmen der Interessenabwägung der DS-GVO zu berücksichtigen.

E-Mail-Werbung und sonstige Werbung mit elektronischer Post sowie Telefon- bzw. Faxwerbung gegenüber Verbraucherinnen und Verbrauchern ist dementsprechend grundsätzlich nur nach ausdrücklicher gesonderter Einwilligung zulässig. Anderes kann bei E-Mail-Werbung dann gelten, wenn die betroffenen Personen bereits einmal Kundinnen oder Kunden des Unternehmens waren, mit gleichartigen Produkten beworben werden und ihnen eine Möglichkeit des Widerspruchs eingeräumt wird.[65]

1.5.6 Werbewiderspruch beachten

Der Werbewiderspruch einer betroffenen Person kann sich datenschutzrechtlich gegen die Dateneigner und/oder die Werbenden als Verantwortliche richten. Beide müssen diesen Werbewiderspruch künftig berücksichtigen, z. B. durch Aufnahme in eine Werbesperrdatei. Die Verantwortlichen haben für die effektive Durchsetzung des Widerspruchsrechts der betroffenen Person zusammenzuwirken, beispielsweise durch Weiterleitung des Widerspruchs. Die Umsetzung des Widerspruchs muss unverzüglich erfolgen.

65 Art. 7 Abs. 3 UWG

Die Versendung von persönlich adressierter Werbung per Post ist nur dann erlaubt, wenn entweder eine Einwilligung oder eine gesetzliche Erlaubnis dazu vorliegt. Bei E-Mail-Werbung und sonstiger Werbung mit elektronischer Post sowie Telefon- und Faxwerbung sind zusätzlich die Vorgaben des UWG zu beachten.

1.6 Das neue Berliner Datenschutzgesetz – Hoffentlich nicht der letzte Stand

Mit dem Wirksamwerden der Datenschutz-Grundverordnung am 25. Mai 2018 war der Reformprozess des europäischen Datenschutzrechts keinesfalls beendet. Vielmehr ergab sich daraus ein enormer Anpassungsbedarf des Bundes- und Landesrechts, der bis zum heutigen Tage noch nicht vollständig abgeschlossen ist.[66] Das Berliner Datenschutzrecht wird maßgeblich durch das Berliner Datenschutzgesetz (BlnDSG) bestimmt, welches am 31. Mai 2018 vom Berliner Abgeordnetenhaus beschlossen wurde. Es regelt die Voraussetzungen, unter denen die öffentlichen Stellen des Landes Berlin personenbezogene Daten grundsätzlich verarbeiten dürfen.

Neben der Anpassung des allgemeinen Berliner Datenschutzrechts an die DS-GVO wurde mit diesem Gesetz auch die EU-Datenschutzrichtlinie für Polizei- und Justizbehörden, die sog. JI-Richtlinie EU 2016/680, in nationales Recht umgesetzt. Damit wird auch die Verarbeitung personenbezogener Daten durch die Polizei- und Justizbehörden neu geregelt. Wie bisher wird das BlnDSG allerdings auch weiterhin durch diverse bereichsspezifische Regelungen in verschiedenen Spezialgesetzen ergänzt.[67]

Unsere Behörde war in den Gesetzgebungsprozess intensiv involviert. Wir haben mehrere schriftliche Stellungnahmen abgegeben und uns mehrfach in den entsprechenden Ausschusssitzungen sowie im Plenum kritisch geäußert.

66 Siehe 1.8
67 Siehe 1.8

Leider konnten wir uns nicht mit allen unseren Anliegen durchsetzen. Im Ergebnis ist leider festzustellen, dass das Berliner Datenschutzgesetz an einigen Stellen die in der DS-GVO garantierten Rechte der Bürger beschneidet.[68] In der Stärkung der Betroffenenrechte liegt jedoch gerade ein zentrales Anliegen der Europäischen Datenschutzreform. Betroffenenrechte versetzen die Menschen in die Lage, selbstbestimmt Datenschutz wahrzunehmen. Anhand von Informationen und Auskünften sollen sie selbst Transparenz über die zu ihrer Person verarbeiteten Daten herstellen können. Dies ist Voraussetzung dafür, durch Berichtigungen und Löschungen die Richtigkeit der gespeicherten Daten durchsetzen zu können. Umso bedauerlicher ist es, dass der Berliner Gesetzgeber in diesem Bereich Einschränkungen vorgenommen hat, die von der DS-GVO nicht mehr gedeckt sind: Z. B. werden danach Auskunftsrechte nicht nur dann eingeschränkt, wenn durch die Auskunftserteilung die Verfolgung von Straftaten oder die Sicherheit des Landes gefährdet wäre, wie es die europäischen Regelungen vorsehen.[69] Vielmehr soll die Auskunftsverweigerung auch bei vergleichsweise unbedeutenden Bußgeldverfahren zulässig sein, wie etwa beim Halten im Parkverbot.[70]

Hinzu kommt, dass bestimmte Entscheidungen über eine Auskunftsverweigerung nicht einmal mehr durch die unabhängige Datenschutzaufsichtsbehörde überprüfbar sind. Dies ist nach dem neuen Berliner Gesetz immer dann der Fall, wenn einzelne Senatsmitglieder eine Auskunft mit der Begründung verweigern, dass eine potenzielle Gefährdung des Bundes oder der Länder bestehe.[71] Eine Überprüfung der Stichhaltigkeit dieser Begründung ist nach der neuen gesetzlichen Berliner Regelung ebenso wenig möglich wie eine Kontrolle der Rechtmäßigkeit der konkreten Datenverarbeitung durch die Betroffenen selbst oder stellvertretend durch unsere Behörde.

Auch weitere Befugnisse der Datenschutzaufsichtsbehörde wurden vom Berliner Abgeordnetenhaus deutlich eingeschränkt. Gerade im öffentlichen Bereich ist es fraglich, ob wir unsere Aufgabe effektiv wahrnehmen können. So wurde uns ins-

68 §§ 23 ff. BlnDSG
69 Art. 23 Abs. 1 DS-GVO
70 § 24 Abs. 1 Satz 2 Nr. 2 BlnDSG
71 § 24 Abs. 3 BlnDSG

besondere die in der DS-GVO verankerte Befugnis verweigert, Bußgelder gegenüber Behörden und sonstigen öffentlichen Stellen zu verhängen.[72]

Im Bereich der JI-Richtlinie ist der Berliner Gesetzgeber sogar noch weiter gegangen und hat entgegen der Formulierung der Richtlinie unserer Behörde lediglich ein Beanstandungsrecht eingeräumt.[73] Sollte der Adressat einer Beanstandung nicht Folge leisten, besteht demnach lediglich die Möglichkeit, den zuständigen parlamentarischen Ausschuss anzurufen, der seinerseits ebenfalls über keine rechtlich verbindlichen Abhilfebefugnisse verfügt. Die Aufnahme auf die Tagesordnung muss dabei keineswegs kurzfristig erfolgen, sodass eine Datenschutzverletzung unter Umständen längere Zeit fortbesteht, ohne konkret eingreifen zu können. Die Möglichkeit, eine gerichtliche Klärung herbeizuführen, besteht ebenfalls nicht. Diese Regelung widerspricht den Vorgaben der JI-Richtlinie, die voraussetzt, dass die Aufsichtsbehörde in die Lage versetzt werden muss, rechtsverbindliche Weisungen auszusprechen.[74] Als Beispiele für solch wirksame Befugnisse werden exemplarisch genannt z. B. die Befugnis, Datenverarbeiter anzuweisen, Verarbeitungsvorgänge in Einklang mit den Datenschutzgesetzen zu bringen, und die Befugnis, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen. Entgegen der Festlegung der JI-Richtlinie,[75] wonach die Aufsichtsbehörde die Anwendung der nach dieser Richtlinie erlassenen Vorschriften sowie deren Durchführungsvorschriften überwachen und durchsetzen soll, verfügt unsere Behörde daher nicht über die erforderlichen Befugnisse, diese Aufgabe wirksam zu erfüllen.

Es bleibt zu hoffen, dass das BlnDSG bei einer zum Ende der Wahlperiode in Aussicht genommenen Evaluierung in den von uns kritisierten Punkten nachgebessert wird.

72 § 28 BlnDSG
73 § 13 Abs. 2 BlnDSG
74 Art. 47 Abs. 2 JI-Richtlinie
75 Art. 46 Abs. 1 lit. a JI-Richtlinie

Bei der Anpassung des BlnDSG an die DS-GVO und an die JI-Richtlinie hat es der Gesetzgeber verpasst, ein mutiges Signal in Richtung Grundrechtsschutz zu setzen. Die in der DS-GVO enthaltenen Betroffenenrechte wurden eingeschränkt. Die Befugnisse der Behörde, die zur Sicherung dieser Rechte berufen ist, wurden beschnitten.

1.7 Facebook-Fanpages und die gemeinsame Verantwortlichkeit für Datenverarbeitungen

Der Europäische Gerichtshof hat im Juni 2018[76] festgestellt, dass Fanpage-Betreiberinnen und -Betreiber bei Facebook gemeinsam mit Facebook für die Verarbeitung personenbezogener Daten der Besucherinnen und Besucher der Fanpage verantwortlich sind. Die Entscheidung beruht zwar auf der vor dem 25. Mai 2018 geltenden Datenschutz-Richtlinie. Die Erwägungen lassen sich aber in die DS-GVO-Zeit übertragen, da die Definition der gemeinsam Verantwortlichen sich nicht geändert hat. Im Gegensatz zur alten Rechtslage sieht die DS-GVO für die gemeinsam Verantwortlichen allerdings zusätzliche Anforderungen in Art. 26 DS-GVO vor. Danach sind diese verpflichtet, in einer Vereinbarung transparent festzulegen, wer welche Verpflichtungen nach der DS-GVO erfüllt. Darüber hinaus muss die Vereinbarung die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den betroffenen Personen gebührend widerspiegeln, außerdem muss der wesentliche Inhalt der Vereinbarung den betroffenen Personen zur Verfügung gestellt werden.

1.7.1 Anhörungsverfahren in Berlin

Die Entscheidung des EuGH ist richtungsweisend, weil es danach für die datenschutzrechtliche Verantwortung unerheblich ist, ob die an der Verarbeitung personenbezogener Daten beteiligten Akteure rechtlich bzw. wirtschaftlich „auf Augenhöhe“ agieren oder z. B. infrastrukturell voneinander abhängig sind. Im Er-

76 Urteil des EuGH vom 5. Juni 2018, Rechtssache C-210/16 Wirtschaftsakademie Schleswig-Holstein

gebnis können sich Verantwortliche daher nicht hinter großen Plattformen und Infrastrukturanbieterinnen und -anbietern „verstecken", deren Angebote sie nutzen.[77] Auch mehrere Monate nach der Veröffentlichung des Urteils des EuGH konnten wir allerdings nicht erkennen, dass Fanpage-Betreiberinnen und -Betreiber in Berlin, insbesondere auch öffentliche Stellen, Konsequenzen aus dem Urteil gezogen hätten. Auch von Facebook war nichts Offizielles zu vernehmen, insbesondere wurde weiterhin keine nach der DS-GVO erforderliche Vereinbarung zur gemeinsamen Verantwortung vorgelegt.[78]

Im September stellte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einem Beschluss[79] fest, dass der Betrieb einer Fanpage, wie von Facebook angeboten, ohne Vereinbarung nach Art. 26 DS-GVO rechtswidrig ist. Darüber hinaus wies die DSK darauf hin, dass Fanpage-Betreiberinnen und -Betreiber (unabhängig davon, ob es sich um öffentliche oder nichtöffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und diese nachweisen können müssen.[80]

Kurz darauf veröffentlichte Facebook eine Ergänzungsvereinbarung, die sich auf eine gemeinsame Verantwortung bezog. Wir haben allerdings Zweifel, dass die Informationen, die Facebook bisher und im Zusammenhang mit der veröffentlichten Ergänzungsvereinbarung zur Verfügung gestellt hat, ausreichend sind, um Rechenschaft über die Rechtmäßigkeit der Verarbeitung der Daten von Besucherinnen und Besuchern der Fanpage ablegen zu können. Wir haben daher eine Reihe von Stellen der Berliner Landesverwaltung, politische Parteien sowie Unternehmen und Organisationen u. a. aus der Handels-, Verlags- und Finanzbranche in Berlin angeschrieben. Derzeit hören wir diese zu den datenschutzrechtlichen Fra-

77 Der EuGH macht deutlich, dass der Umstand, dass Organisationen und Personen die von Facebook eingerichtete Plattform nutzen, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, diese nicht von der Beachtung ihrer Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien kann, Urteil des EuGH vom 5. Juni 2018, Rechtssache C-210/16, Rn. 40

78 Siehe Art. 26 DS-GVO

79 „Beschluss der DSK zu Facebook Fanpages" Düsseldorf, 5. September 2018, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/20180905_dskb_facebook_fanpages.pdf

80 Siehe die in Art. 5 Abs. 2 DS-GVO festgelegte Rechenschaftspflicht

gestellungen an. Insbesondere wollen wir wissen, welche konkreten Datenverarbeitungen erfolgen, auf welcher Rechtsgrundlage die Datenverarbeitung erfolgt und wie die Information der betroffenen Personen sichergestellt wird.[81]

1.7.2 Auslegung und Reichweite der gemeinsamen Verarbeitung personenbezogener Daten

Im Rahmen des Fanpage-Verfahrens stellte der EuGH darauf ab, dass Facebook sog. „Seiten-Insights" für die Seitenbetreiberinnen und -betreiber erstellt, also Statistiken über die Besucherinnen und Besucher der Seite und die Art der Nutzung. Für das Gericht spielte es eine große Rolle, dass die Fanpage-Betreiberinnen und -Betreiber durch das Festlegen bestimmter Parameter (z. B. Auswertungen nach Alter und Geschlecht) entsprechend ihrem Zielpublikum an der Erstellung der Statistiken durch Facebook mitwirken.[82] Offen blieb, ob sich die gemeinsame Verantwortung der Seitenbetreiberinnen und -betreiber über die Erstellung solcher Seiten-Insights hinaus auch auf sich anschließende bzw. weitere Datenverarbeitungen durch Facebook erstrecken soll. Dagegen spricht, dass der EuGH die Seiten-Insights und die Parametrierung durch die Seitenbetreiberinnen und -betreiber in den Vordergrund stellte. Allerdings sah der EuGH, offenbar unabhängig von der Parametrierung, gerade bei solchen Besucherinnen und Besuchern der Fanpage, die nicht bei Facebook registriert sind, eine erhöhte Verantwortung der Seitenbetreiberinnen und -betreiber. In diesen Fällen, so der EuGH, löse das bloße Aufrufen der Fanpage automatisch die Verarbeitung ihrer personenbezogenen Daten aus.[83] Das Gericht legte somit den Begriff der verantwortlichen Verarbeitung personenbezogener Daten weit aus.[84]

81 Den Fragenkatalog im Anhörungsverfahren haben wir unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/informationen/2018-BlnBDI-Fragenkatalog_Fanpages.pdf veröffentlicht.

82 Urteil des EuGH vom 5. Juni 2018, Rechtssache C-210/16, Rn. 39

83 Urteil des EuGH vom 5. Juni 2018, Rechtssache C-210/16, Rn. 41

84 Entsprechend wies der EuGH in der Entscheidung darauf hin, dass es nicht erforderlich sei, dass jede bzw. jeder gemeinsam Verantwortliche Zugang zu den betreffenden personenbezogenen Daten hat, vgl. Urteil des EuGH vom 5. Juni 2018, Rechtssache C-210/16, Rn. 38

Der EuGH bekräftigte diese Auslegung in einer weiteren Entscheidung aus dem letzten Jahr. Kurz nach der Fanpage-Entscheidung urteilte das Gericht,[85] dass eine Religionsgemeinschaft gemeinsam mit ihren als Verkünderinnen und Verkünder tätigen Mitgliedern Verantwortliche für die Verarbeitung personengezogener Daten ist. In diesem Fall ließ der EuGH es für die datenschutzrechtliche Verantwortung ausreichen, dass die Religionsgemeinschaft die Verkündungstätigkeit organisiert, koordiniert und die Mitglieder dazu ermuntert.[86]

Eine weitere gerichtliche Klärung des Begriffs der gemeinsamen Verantwortung ist nicht fern. In einem aktuellen Verfahren muss der EuGH sich mit der Frage der Einbindung von Social Plugins[87] in Webseiten und mit der Verantwortung für die dadurch ausgelöste Datenverarbeitung auseinandersetzen. Im Dezember hat der Generalanwalt seine Schlussanträge in dem Verfahren veröffentlicht.[88] Er kommt zu dem Schluss, dass die Betreiberinnen und Betreiber von Webseiten mit den Dritten, deren Plugins sie in ihre Webseiten eingebunden haben, als gemeinsam Verantwortliche anzusehen sind. Der Generalanwalt stellt dabei auf die Erhebung und Übermittlung von personenbezogenen Daten ab, die durch die Plugins veranlasst werden, schlägt aber gleichzeitig vor, die gemeinsame Verantwortlichkeit auf solche Phasen in einer Gesamtkette von Datenverarbeitungsvorgängen zu beschränken, in denen ein beteiligter Akteur tatsächlich einen Beitrag zur Entscheidung über die Mittel und Zwecke der Datenverarbeitung leistet. Im Falle der Social Plugins beschränkt sich die gemeinsame Verantwortlichkeit des in Rede stehenden Webseitenbetreibers nach den Vorschlägen des Generalanwaltes daher auf die Phase der Erhebung und Übermittlung. Ausgenommen bleiben dann die Weiterverarbeitungen durch die Dritten, die die Plugins bereitgestellt haben. Es bleibt spannend, was der EuGH daraus macht.

Festgehalten werden kann bereits jetzt, dass die Veranlassung einer Verarbeitung personenbezogener Daten ausreichend sein kann, um eine datenschutzrechtliche Verantwortlichkeit zu begründen. Dies hat Folgen für das Zusammenwirken

85 Urteil des EuGH vom 10. Juli 2018, Rechtssache C-25/17

86 Urteil des EuGH vom 10. Juli 2018, Rechtssache C-25/17, Rn. 75

87 Rechtssache C-40/17: In dem Verfahren geht es um den „Gefällt mir"-Button von Facebook.

88 Schlussanträge des Generalanwalts Michal Bobek vom 19. Dezember 2018 in der Rechtssache C-40/17

von Webseitenbetreiberinnen bzw. -betreibern und Dritten, z. B. wenn Pixel in die Webseiten eingebunden werden oder Dritten ermöglicht wird, Cookies auf den Endgeräten der Nutzerinnen und Nutzer abzulegen.

1.8 Berliner Landesgesetze – Fit für Europa?

Mit dem Wirksamwerden der DS-GVO zum 25. Mai 2018 musste im Land Berlin geprüft werden, ob und in welchem Umfang die zahlreichen Landesgesetze an die europarechtlichen Vorschriften anzupassen sind. Die DS-GVO enthält mehr als 70 sog. Öffnungsklauseln für den nationalen Gesetzgeber, die es auch weiterhin erlauben, die Verarbeitung personenbezogener Daten in speziellen Vorschriften zu regeln oder beizubehalten. Die für die Anpassung des Datenschutzrechts federführende Senatsverwaltung für Inneres und Sport hat die Hauptverwaltungen aufgerufen, die in ihrer Zuständigkeit liegenden Fachgesetze diesbezüglich zu überprüfen, um Änderungen in ein Artikelgesetz zur Anpassung des Datenschutzrechts an die DS-GVO aufnehmen zu können. In diesem Prozess standen wir mit einigen Fachverwaltungen in engem Kontakt und haben diese intensiv beraten.

Mit der Senatsverwaltung für Europa und Kultur konnten wir bereits Ende 2017 den Änderungsbedarf u. a. hinsichtlich des Archivgesetzes des Landes Berlin sowie des Kulturdatenverarbeitungsgesetzes abstimmen, die diesen dann an die Innenverwaltung weitergegeben hat. Auch die Senatskanzlei haben wir hinsichtlich der Anpassung des Berliner Hochschulgesetzes sowie der Studierendendatenverordnung beraten.

Die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung haben wir insbesondere zur Anpassung des Gesundheitsdienstegesetzes, des Landeskrankenhausgesetzes, des Heilberufekammergesetzes und des Landesgleichstellungsgesetzes beraten.

Für den Bereich des öffentlichen Gesundheitsdienstes fehlen seit vielen Jahren die notwendigen Regelungen zur Verarbeitung personenbezogener Daten, insbesondere sensitiver Gesundheitsdaten. Trotz intensiven Austauschs mit den zuständigen Stellen zur Frage des Erlasses einer entsprechenden Verordnung lag

zum Ende des Jahres 2017 immer noch kein Entwurf vor.[89] Wir konnten nunmehr gegenüber der Gesundheitsverwaltung erreichen, dass im Zuge der ohnehin notwendigen Überprüfung und Anpassung der Vorschriften im Gesundheitsdienstegesetz die Gelegenheit wahrgenommen wurde, die bislang fehlenden Verarbeitungsbefugnisse für den öffentlichen Gesundheitsdienst unmittelbar ins Gesetz aufzunehmen. Sofern die Senatsverwaltung für Inneres die vorgeschlagenen Änderungen übernimmt, ist ein wesentlicher Schritt erreicht, um die Datenverarbeitung im öffentlichen Gesundheitsdienst auf eine rechtssichere Grundlage zu stellen.

Intensiv begleitet haben wir auch die aktuelle Schulrechtsreform. Die Senatsverwaltung für Bildung, Jugend und Familie hat die Gelegenheit ergriffen, in diesem Zuge auch das Berliner Schulgesetz an die Datenschutzvorgaben der DS-GVO anzupassen.[90]

Zum jetzigen Zeitpunkt – fast ein Jahr nach Wirksamwerden der DS-GVO – sind daher leider lediglich das Schulgesetz und das Heilberufekammergesetz novelliert in Kraft getreten und damit – weitgehend[91] an die europarechtlichen Vorgaben angepasst worden. Für alle anderen Fachgesetze steht das parlamentarische Gesetzgebungsverfahren noch aus.

Wir fordern die Senatsverwaltung für Inneres auf, das Gesetzgebungsverfahren für das Anpassungsgesetz zügig auf den Weg zu bringen, um einen europarechtskonformen Zustand im Land Berlin herzustellen.

89 JB 2017, 7.1

90 Näheres zur Novellierung des Schulgesetzes unter JB 2018, 5.1

91 JB 2018, 5.1

2 Digitale Verwaltung

2.1 Digitalisierungsprojekte in Berlin

Aus der Praxis

Das Berliner E-Government-Gesetz (EGovG Bln) soll u. a. dazu beitragen, den Bürgerinnen, Bürgern und der Wirtschaft digitale Verwaltungsleistungen nutzungsfreundlich und sicher zur Verfügung zu stellen. Die Umsetzung geht zügig voran.

Seit März bietet das Service-Konto Berlin die Möglichkeit, Verwaltungsleistungen medienbruchfrei elektronisch in Anspruch nehmen zu können.[92] Derzeit können zwar erst einige wenige Online-Dienste genutzt werden,[93] es ist jedoch geplant, sukzessive alle Online-Dienste an das Service-Konto anzubinden und perspektivisch einen Großteil aller Verwaltungsleistungen darüber anzubieten. Wir haben die Einführung des Service-Kontos intensiv begleitet und die federführende Senatsverwaltung für Inneres und Sport im Hinblick auf die Umsetzung der datenschutzrechtlichen Vorgaben unterstützt.

Der Entwurf eines Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen der Berliner Verwaltung (Onlinezugangsgesetz Berlin)[94] wurde auf Vorlage des Senators für Inneres und Sport vom Senat zur Kenntnis genommen und soll nach Befassung im Rat der Bürgermeister ins Parlament eingebracht werden. Damit sind die Weichen gestellt, mittels einer einmaligen Registrierung im Service-Konto nicht nur Verwaltungsleistungen des Landes Berlin elektronisch in Anspruch nehmen zu können, sondern auch die anderer Bundesländer und des Bundes über dessen Portalverbund.

Nach dem Berliner E-Government-Gesetz ist die Berliner Verwaltung verpflichtet, ihre Akten spätestens ab dem 1. Januar 2023 elektronisch zu führen.[95] Dabei

92 JB 2017, 2.1

93 Beantragung eines Bewohnerparkausweises, eines Kita-Gutscheins für Bürgerinnen und Bürger sowie die Nutzung des Einheitlichen Ansprechpartners Berlin für Unternehmen

94 JB 2017, 2.1, S. 46

95 § 7 Abs. 1 Satz 1 EGovG Bln, siehe auch JB 2016, 2.1

ist durch geeignete technisch-organisatorische Maßnahmen nach dem jeweiligen Stand der Technik sicherzustellen, dass die Grundsätze ordnungsgemäßer Aktenführung und die für die Berliner Verwaltung geltenden Standards, insbesondere im Hinblick auf Datenschutz und Datensicherheit, eingehalten werden.

Die elektronische Akte ermöglicht eine schnellere und effizientere Vorgangsbearbeitung, was nicht nur den Bürgerinnen und Bürgern zugutekommt, sondern auch den Beschäftigten der Berliner Verwaltung. Durch sie sollen Akten und sonstige Unterlagen innerhalb von Behörden und untereinander elektronisch übermittelt werden können. Hierbei ist in jedem Fall eine sichere, dem aktuellen Stand der Technik entsprechende Kommunikationsinfrastruktur einzusetzen. Insbesondere sind die übermittelten Daten vor Einsichtnahme durch Unbefugte sowie vor Veränderung zu schützen.[96] Perspektivisch soll es Bürgerinnen und Bürger zudem ermöglicht werden, über das Service-Konto Berlin den Stand der Vorgangsbearbeitung selbst abzurufen, wodurch zum einen eine schnellere Benachrichtigung der Betroffenen gewährleistet wird, zum anderen aber auch die Beschäftigten der Behörden von Nachfragen entlastet werden.

Da in der elektronischen Akte naturgemäß auch besonders sensitive Daten zu verarbeiten sind, müssen auch technisch-organisatorische Maßnahmen ergriffen werden, die die Verarbeitung von Daten mit hohem Schutzbedarf ermöglichen. Wir haben die federführende Senatsverwaltung für Inneres und Sport bei der Schutzbedarfsfeststellung intensiv begleitet. Darüber hinaus waren wir an der Vorbereitung der landesweiten Ausschreibung der elektronischen Akte beratend beteiligt und konnten auf diesem Wege sicherstellen, dass datenschutzrechtliche Vorgaben und Aspekte bereits im Zuge der Ausschreibung Berücksichtigung finden. Es ist geplant, das Ausschreibungsverfahren im Jahr 2019 durchzuführen.

Das Service-Konto sowie die elektronische Akte werden flankiert vom neuen Basisdienst „Digitaler Antrag", der künftig eine medienbruchfreie Antragstellung mit einheitlichem Erscheinungsbild und Bedienkonzept für alle elektronischen Anträge in der Berliner Verwaltung ermöglichen soll. Wie bei der elektronischen Akte gilt auch hier, dass wegen der potenziellen Verarbeitung besonders sensitiver Daten technisch-organisatorische Maßnahmen ergriffen werden müssen, die

96 § 7 Abs. 2 EGovG Bln

die Verarbeitung von Daten mit hohem Schutzbedarf ermöglichen. Auch hier haben wir die Schutzbedarfsfeststellung begleitet und weitere datenschutzrechtliche Hinweise eingebracht.

In Verbindung mit der Einführung der elektronischen Aktenführung und Vorgangsbearbeitung werden in den Berliner Behörden weiterhin in nicht unerheblichem Umfang Papierunterlagen anfallen, insbesondere im Bereich der Eingangspost. Um diese Unterlagen in den elektronisch gestützten Arbeitsablauf einbeziehen zu können, sind Papierunterlagen unter Wahrung der Grundsätze ordnungsgemäßer Aktenführung und -aufbewahrung in ein elektronisches Format zu übertragen.[97] Dabei sind in jedem Fall die Vorgaben der Technischen Richtlinie zum ersetzenden Scannen des Bundesamts für Sicherheit in der Informationstechnik[98] einzuhalten. Um eine berlinweit einheitliche, sichere und wirtschaftliche Lösung zu finden, wurde von der Senatsverwaltung für Inneres und Sport das Projekt „Dokumenten-Input-Management (DIM)" initiiert. Auch dieses Projekt werden wir begleiten.

Die Einführung digitaler Verwaltungsleistungen muss für Bürgerinnen und Bürger transparent, sicher und datenschutzgerecht erfolgen.

2.2 Beihilfe Online

Aus der Praxis

Das Fachverfahren Beihilfeantrag Online (BAO) soll es beihilfeberechtigten Beschäftigten und Versorgungsempfängern des Landes Berlin ermöglichen, online über Webbrowser oder App Anträge auf Beihilfe zu stellen, den Bearbeitungsstatus zu verfolgen und Bescheide zu empfangen. Zudem soll es möglich sein, Stammdatenänderungen zu melden. Im Rahmen der Antragstellung werden stufenweise die Funktionalitäten zur Verfügung gestellt.

Bereits vor vier Jahren wurden wir vom Landesverwaltungsamt darüber informiert, dass die Voraussetzungen für die Beantragung des BAO geschaffen werden sollen. In dieser frühen Projektphase hatten wir dem Landesverwaltungsamt mit-

97 § 8 EGovG Bln

98 BSI TR-03138 Ersetzendes Scannen (RESISCAN)

geteilt, welche Unterlagen für eine systematische und abschließende Beurteilung des Verfahrens benötigt werden. Dies sind z. B. ein IT-Sicherheitskonzept sowie Konzepte für die Organisation der Zugriffsberechtigungen, der Protokollierung erfolgter Datenzugriffe sowie der Löschung der Daten.

Nach ersten erheblichen Verzögerungen erhielten wir Unterlagen, die jedoch noch nachbearbeitet oder vervollständigt werden mussten bzw. Schritt für Schritt nach Fertigstellung nachgereicht wurden. Im Mai 2018 wurde das Projekt wieder aufgenommen. Bei einem ersten Workshop wurde die Bedeutung des Vorhabens bekräftigt und der Entschluss gefasst, das Projekt fortzuführen. Seitdem schreitet das Projekt mit unserer Beteiligung zügig voran.

Die ab 25. Mai 2018 mit der Datenschutz-Grundverordnung (DS-GVO) veränderte Rechtslage bedeutet für das Projekt, dass eine Datenschutz-Folgenabschätzung durchgeführt werden muss, da aufgrund der mit dem Verfahren verarbeiteten Arztrechnungen der Beihilfeberechtigten eine umfangreiche Verarbeitung von Gesundheitsdaten[99] und damit besonders sensitiver Daten erfolgt. Eine Datenschutz-Folgenabschätzung ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten.[100] Eine Datenschutz-Folgenabschätzung muss der jeweilige Verantwortliche durchführen, in diesem Fall das Landesverwaltungsamt.

In einer ersten Phase erfolgte dementsprechend die Bewertung der Risiken des Verfahrens mit Hilfe des Standard-Datenschutzmodells (SDM).[101] Hierbei wurden Risiken festgestellt, für die geeignete Abhilfemaßnahmen getroffen werden müssen. Im Rahmen der Weiterführung der Datenschutz-Folgenabschätzung muss nun geprüft werden, ob die vorgesehenen Maßnahmen die Risiken hinreichend mildern.

99 Art. 35 Abs. 3 lit. b DS-GVO

100 Weitere Hinweise unter https://www.datenschutz-berlin.de/wirtschaft-und-verwaltung/datenschutz-folgenabschaetzung/

101 SDM: Das Standard-Datenschutzmodell bietet eine Unterstützung zur Datenschutzberatung und -prüfung sowie zur Erstellung einer Datenschutz-Folgenabschätzung auf der Basis einheitlicher Gewährleistungsziele (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientlierungshilfen/2018-SDM.pdf).

Weitere Fortentwicklungen des Verfahrens, wie die Entwicklung einer benutzerfreundlichen App für mobile Geräte, sind geplant. Hierfür muss dann ebenfalls eine Betrachtung der Risiken im Rahmen einer Datenschutz-Folgenabschätzung erfolgen.

Eine datenschutzgerechte Planung und Ausgestaltung des zukunftsorientierten Verfahrens Beihilfeantrag Online konnte unter unserer Begleitung auf den Weg gebracht werden. Die sich anschließenden Schritte und die zukünftige Planung werden wir weiterhin aufmerksam verfolgen.

3 Inneres

3.1 Drohbriefe an die linke Szene mit Daten aus Polizeidatenbanken

Zu Beginn des Jahres haben wir durch Pressemeldungen erfahren, dass bei verschiedenen Einrichtungen der linksautonomen Szene Briefe eingegangen sind, die u. a. Namen und Fotos von mehreren konkreten Personen enthielten. In den Briefen waren insgesamt 45 Personen namentlich benannt und zu 21 dieser Personen waren Lichtbilder und Informationen aufgeführt, die augenscheinlich nur von Polizei- oder Justizbehörden stammen konnten. Als Absender gab sich ein „Zentrum für politische Korrektheit" aus und drohte damit, die Daten dieser Personen sowie ihrer Familienangehörigen an die Polizei oder rechtsextreme Gruppen weiterzugeben.

Unmittelbar nach Erscheinen der Medienberichte nahmen wir Kontakt mit der Polizei auf und baten um kurzfristige Stellungnahme, welche Maßnahmen die Polizei zur Sachverhaltsaufklärung ergriffen habe. Als erste Ermittlungsmaßnahmen empfahlen wir die Überprüfung der erfolgten Zugriffe auf die Einträge in den polizeilichen Datenbanken zu den in dem Drohbrief genannten Personen.

Die Polizei teilte uns daraufhin mit, dass sie ein Ermittlungsverfahren gegen Unbekannt wegen Verstoßes gegen das Berliner Datenschutzgesetz (BlnDSG) und der Verletzung von Privatgeheimnissen eingeleitet habe. Gemäß unserer Empfehlung sei eine Protokolldatenabfrage zur Feststellung veranlasst worden, um zu klären, ob Daten der Betroffenen in zeitlicher Nähe zur Briefversendung aus den Polizeidatenbanken abgerufen wurden und ob der Abruf ggf. dienstlich begründet war. Die Auswertung der Datenabfragen sowie weitere Untersuchungen unter Einbindung des Kriminaltechnischen Instituts hätten jedoch zu keinen Erkenntnissen geführt.

Wir empfahlen der Polizei weitere konkrete Maßnahmen, die von dem ermittelnden Landeskriminalamt teilweise auch berücksichtigt wurden. Insbeson-

dere empfahlen wir die Untersuchung eines Original-Exemplars der versendeten Briefe unter folgenden Gesichtspunkten: Identifizierung der Seriennummer des verwendeten Druckers anhand des Druckbildes (sog. „Machine Identification Code"), Rückschlüsse auf die Herkunft des Briefes durch Analyse des verwendeten Papiers und Ermittlung der Verfasserin bzw. des Verfassers des Briefes durch ggf. abgebildete Fingerabdrücke.

Als sich zwischenzeitlich betroffene Personen vertraulich an uns wandten, konnten wir kurzzeitig Einsicht in einen Original-Brief nehmen und dabei feststellen, dass dieser Farbfotos in guter Auflösung enthielt. Dies sprach gegen die von der Polizei anfangs geäußerte Vermutung, dass bei der Erstellung der Briefe Fotokopien verwendet wurden.

Angesichts der uns vorliegenden Informationen stellten wir am 26. März 2018 Strafantrag gegen Unbekannt wegen Verstoßes gegen das Berliner Datenschutzgesetz.[102] Im weiteren Verlauf unserer Prüfung erhielten wir leider nur noch begrenzt Auskunft von der Berliner Polizei. Mitte April wurde uns erstmals mitgeteilt, dass aufgrund einer Anweisung der Staatsanwaltschaft die weitere Kommunikation direkt über den zuständigen Staatsanwalt zu führen sei. Wir mussten sowohl die Polizei als auch die Staatsanwaltschaft wiederholt darauf hinweisen, dass der Polizeipräsident in Berlin als datenverarbeitende Stelle gegenüber der BlnBDI auskunftspflichtig ist, auch wenn die Staatsanwaltschaft strafprozessual ein Ermittlungsverfahren führt.[103]

Nach mehrmaligem Nachfragen erhielten wir im August von der Polizei die Information, dass ein Polizeibeamter des Landes Berlin als Tatverdächtiger ermittelt wurde und dieser die Fertigung des Briefes eingeräumt habe. Die Staatsanwaltschaft teilte uns schließlich Anfang Oktober mit, gegen den Beschuldigten sei ein Strafbefehl erlassen worden, der bereits seit Ende August rechtskräftig sei. Da wir jedoch bislang immer noch keine Kenntnis darüber haben, woher die in den versendeten Briefen enthaltenen personenbezogenen Daten stammen und wie der Verfasser der Briefe an diese gelangt ist, dauert unsere Prüfung weiter an.

102 § 32 Abs. 3 BlnDSG a. F. i. V. m. § 32 Abs. 1 Nr. 2 Alt. 1 und Nr. 1 Alt. 1 BlnDSG a. F.
103 § 54 BlnDSG

Die Verwendung der Drohbriefe ist ein besonders schwerwiegender Vorfall. Sie stellt nicht nur eine Straftat dar, sondern beschädigt darüber hinaus das Vertrauen der Öffentlichkeit in die Sicherheitsorgane, deren Aufgabe insbesondere die Verhütung von Straftaten ist.

3.2 Verarbeitung personengebundener Hinweise in polizeilichen Datenbanken

Seit einigen Jahren erstellt und nutzt die Berliner Polizei wieder bestimmte polizeiliche Bewertungen von Personen, sog. personengebundene Hinweise (PHW), nachdem sie diese zuvor über zwanzig Jahre lang aufgrund von Kritik der Konferenz der Datenschutzbeauftragten des Bundes und Länder nicht für ihre Arbeit verwendet hatte.[104] Der Wiedereinführung der Hinweise haben wir erfolglos widersprochen.

Zu den personengebundenen Hinweisen, die bundeseinheitlich verwendet werden, gehört die Angabe „Psychische und Verhaltensstörungen" (PSYV), die bis zu einem entsprechenden Beschluss der Innenministerkonferenz im Jahr 2015 noch „geisteskrank" hieß.[105] Solche personengebundenen Hinweise sollen insbesondere dem Schutz der betroffenen Person bzw. der Eigensicherung von Polizeibeamtinnen und -beamten dienen.[106]

Aufgrund von Anfragen von Bürgerinnen und Bürgern zur Speicherung personengebundener Hinweise in polizeilichen Datenbanken haben wir die Senatsverwaltung für Inneres und Sport nun erneut zu dieser Thematik angeschrieben und darauf hingewiesen, dass wir weiterhin erhebliche Zweifel an der Rechtmäßigkeit der Speicherung des Hinweises „Psychische und Verhaltensstörungen" haben. Ein solcher Hinweis ist aus unserer Sicht nicht für polizeiliche Zwecke erforderlich und für die Betroffenen äußerst stigmatisierend.

104 JB 2012, 3.8

105 Siehe Drs. 17/2406 des Abgeordnetenhauses Berlin

106 Siehe § 16 Abs. 6 Nr. 1 Bundeskriminalamtgesetz (BKAG)

Insbesondere ist nicht ersichtlich, weshalb die Aufnahme eines solches Hinweises zur Gefahrenabwehr oder Eigensicherung durch die Polizei notwendig sein soll. Im Regelfall gehen von psychisch erkrankten Personen keine Gefahren aufgrund ihrer Erkrankung aus, die es polizeilich abzuwehren gilt. Soweit im Einzelfall solche Gefahren dennoch bekannt sein sollten, wäre zudem die Aufnahme des ebenfalls möglichen personengebundenen Hinweises „gewalttätig" denkbar und ausreichend.

Der personengebundene Hinweis „Psychische und Verhaltensstörungen" sollte mangels Erforderlichkeit aus der Liste der Hinweise, die in polizeilichen Datenbanken durch die Berliner Polizei zu ihrer Aufgabenerfüllung vergeben werden können, herausgenommen werden.

3.3 Sicherheitslücke bei der polizeilichen Datenbank POLIKS?

Ein Polizist beschwerte sich bei uns darüber, dass unbefugte Zugriffe auf die polizeiliche Datenbank POLIKS aufgrund nicht ausreichender Sicherheitsvorgaben möglich seien. Man könne durch mehrfache Eingabe eines falschen Kennworts einen beliebigen Zugang zu POLIKS sperren und sodann über eine telefonische Hotline ohne weitere Hürden diesen Zugang wieder entsperren und sich ein neues Kennwort geben lassen.

In der daraufhin eingeleiteten Prüfung wurde uns bestätigt, dass ein Zugang zu POLIKS gesperrt werde, wenn mehrfach ein falsches Passwort eingegeben werde. Zur Entsperrung könnten sich die betroffenen Nutzerinnen und Nutzer dann an die zentrale IT-Administration wenden. Diese hebe eine Kontensperrung auf, wenn die Meldung durch die Vorgesetzte oder den Vorgesetzten der oder des Betroffenen bestätigt werde. Nach Aufhebung der Sperre sei das Kennwort unverändert; es werde kein neues vergeben. Gegen dieses Verfahren haben wir keine datenschutzrechtlichen Bedenken.

Benötigt die Nutzerin oder der Nutzer nach einer Kontosperrung hingegen ein neues Kennwort, muss sie oder er sich nach Auskunft der Polizei an die jeweils

zuständige örtliche IT-Administration wenden, die nach einer Identifikation der betroffenen Person ein neues Kennwort vergebe. Das konkrete Identifikationsverfahren sei dabei nicht berlinweit einheitlich geregelt. Die polizeiinterne Passwortrichtlinie enthält nach unserer Feststellung hierzu ebenfalls keine konkreten Angaben, sondern lediglich das allgemeine Erfordernis eines Identitätsnachweises. Dieser erfolgt nach Aussage der Polizei entweder durch Vorlage des Dienstausweises, Verifizierung durch den Vorgesetzten oder persönliche Bekanntheit der oder des Betroffenen.

Wir forderten daraufhin, dass eine behördenweit einheitliche Regelung geschaffen und durchgesetzt werden muss, die eine sichere Identifikation der oder des jeweils Betroffenen garantiert. Insbesondere sollte genau festgelegt sein, wann welche der beschriebenen Mittel zur Identitätsprüfung bei einer Passwortneuvergabe Anwendung finden und wie diese jeweils konkret erfolgen soll. Um spätere Überprüfungen – insbesondere im Fall eines Missbrauchsverdachts – zu ermöglichen, sollte die Vergabe von neuen Passwörtern sowie die Art der Identitätsprüfung zudem bei den jeweiligen örtlichen IT-Administrationen dokumentiert werden. Weiterhin haben wir empfohlen, regelmäßig stichprobenartig Kontrollen der örtlichen Passwortneuvergaben vorzunehmen.

Die Polizei hat die Überarbeitung ihrer Passwortrichtlinie zugesagt.

Der unbefugte Zugang zu Daten in POLIKS ist bußgeldbewehrt und stellt sogar eine Straftat dar, wenn er mit Schädigungs- oder Bereicherungsabsicht erfolgt.[107] Die Polizei ist als Verantwortliche verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen im Hinblick auf eine Passwortneuvergabe zu treffen, um bei der Verarbeitung personenbezogener Daten in POLIKS ein dem Risiko angemessenes Schutzniveau zu gewährleisten.[108] Hierdurch wird auch Ordnungswidrigkeiten und Straftaten vorgebeugt.

107 §§ 70, 29 BlnDSG
108 § 50 Abs. 1 BlnDSG

3.4 Kontrolle des Akkreditierungsverfahrens beim G20-Gipfel

Im Juli 2017 fand in Hamburg der G20-Gipfel[109] statt. Um Zutritt zum Pressezentrum zu bekommen, benötigten Journalisten eine Akkreditierung des Bundespresseamts. Voraussetzungen für eine Akkreditierung waren der Nachweis der journalistischen Tätigkeit und eine Sicherheitsüberprüfung. Nachdem es im Vorfeld des G20-Gipfels zu Ausschreitungen gekommen war, nahmen die Sicherheitsbehörden eine neue Bewertung der Lage vor, in deren Folge auch die bereits erteilten Akkreditierungen überprüft wurden. Auf Empfehlung des Bundeskriminalamts entschied das Bundespresseamt, insgesamt 32 Journalistinnen und Journalisten die Akkreditierung wieder zu entziehen. Betroffene beschwerten sich insbesondere darüber, dass die Empfehlungen des BKA auf der Basis von Informationen zu Strafermittlungsverfahren ausgesprochen wurden, die teilweise jahrelang zurücklagen.

Die Erkenntnisse des BKA waren überwiegend auf Daten zurückzuführen, die von den Landespolizeibehörden im bundesländerübergreifenden Informationssystem INPOL eingestellt worden waren. Daher haben wir eine Prüfung hinsichtlich der Speicherung von Daten in INPOL durch die Berliner Polizei eingeleitet.

Voraussetzung für die Übermittlung von Daten an das BKA bzw. für die Speicherung von Daten in die vom BKA betriebenen Datenbanken ist zum einen das Vorliegen von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung.[110] Hierbei ist eine sog. „Erheblichkeitsprüfung“ durchzuführen. Zum anderen dürfen personenbezogene Daten von Beschuldigten und von Personen, die einer Straftat verdächtig sind, nur unter bestimmten Voraussetzungen verarbeitet werden. Anhand einer sog. „Negativprognose“ ist zu prüfen, ob wegen der Art oder Ausführung der Tat oder der Persönlichkeit des Betroffenen Grund zur Annahme besteht, dass zukünftig Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind.[111]

109 Gipfeltreffen der Gruppe der zwanzig wichtigsten Industrie- und Schwellenländer
110 § 2 Abs. 1 Bundeskriminalamtgesetz (BKAG)
111 § 8 Abs. 2 BKA-alt bzw. jetzt § 18 Abs. 1, 2 BKAG

Im Zusammenhang mit der Dokumentation und Durchführung der Erheblichkeitsprüfungen sowie der Negativprognosen haben wir strukturelle Fehler der Berliner Polizei festgestellt. Sie hat die bei Einstellung der Daten vorzunehmenden Prüfungen bzw. Abwägungen nicht dokumentiert, sondern erst nachträglich für die Beantwortung unserer Anfrage formuliert. Mangels einzelfallbezogener Dokumentation war für uns daher nicht erkennbar, ob die nach dem BKAG erforderlichen Prüfungen durch die Berliner Polizei durchgeführt worden sind, bevor Datensätze bei INPOL eingespeist wurden, und ob die gesetzlich vorgegebenen Voraussetzungen vorlagen.

Darüber hinaus lagen der Polizei in einigen Fällen keine Rückmeldungen der Staatsanwaltschaft zum Ausgang der Verfahren vor, sodass die Rechtmäßigkeit der weiteren Datenspeicherung nicht geprüft wurde. In einem Fall führte dies dazu, dass in INPOL noch ein Verfahren gespeichert war, obwohl die betroffene Person durch ein Gericht aus tatsächlichen Gründen rechtskräftig freigesprochen worden war. Hier ist ganz deutlich darauf hinzuweisen, dass eine Weiterverarbeitung von Daten unzulässig ist, wenn die betroffene Person rechtskräftig freigesprochen wurde bzw. wenn die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt wurde, sofern sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat.

Wir haben diese strukturellen Fehler bei der Berliner Polizei bemängelt und gefordert, dass in Bezug auf die Dokumentation der vorzunehmenden Prüfungen dringend Verfahrensänderungen vorzunehmen sind. Ferner haben wir gefordert, technisch-organisatorische Maßnahmen zu ergreifen, damit in INPOL keine rechtswidrige Weiterverarbeitung von personenbezogenen Daten Betroffener erfolgt.

Die Polizei hat uns inzwischen mitgeteilt, dass entsprechende organisatorische Verfahrensänderungen vorgenommen worden seien bzw. derzeit im Polizeilichen Landessystem zur Information, Kommunikation und Sachbearbeitung technisch umgesetzt würden.

Eine Speicherung und Weiterverarbeitung von personenbezogenen Daten in die vom BKA geführten Datenbanken darf nur im Rahmen der gesetzlichen Vorgaben erfolgen. Die Überprüfung, ob diese Voraussetzungen erfüllt sind, muss anhand des jeweiligen Einzelfalls durch die einmeldende Stelle bei der Berliner Polizei erfolgen. Hierfür sind geeignete technische und organisatorische Voraussetzungen zu schaffen.

3.5 Ersthelfer-App „Katretter“ der Berliner Feuerwehr

Wir begleiten die Berliner Feuerwehr bei der Einführung einer App, die die Alarmierung von Ersthelfenden in räumlicher Nähe zum Ort der Notrufe ermöglicht, wenn – wie z. B. bei einem Herz-Kreislauf-Stillstand – besonders schnelle Hilfe noch vor Eintreffen des Rettungswagens zusätzlich Leben retten kann.

Die Berliner Feuerwehr hat uns bereits in einem frühen Projektstadium beteiligt. Hierzu wurden uns eine App „Katretter“ sowie die zum Verfahren gehörenden Softwarekomponenten vorgestellt, die in Rechenzentren sowie bei den Leitstellen betrieben werden sollen. Das Katretter-System wird in Kooperation mit dem Fraunhofer Institut für Offene Kommunikationssysteme (Fokus) und der Combi-Risk GmbH entwickelt und soll in Berlin, aber auch in anderen Bundesländern, betrieben werden.

Zweck des Verfahrens ist die Alarmierung von sog. Ersthelfenden, die sich zufällig in der näheren Umgebung einer zu rettenden Person befinden. Hierzu sucht die Feuerwehr in einer ersten Projektphase freiwillige Ersthelfende aus den eigenen Reihen, die die App installieren und im Notfall Hilfe leisten. Später sollen auch Ersthelfende aus anderen medizinischen Berufsgruppen rekrutiert werden.

Konkret soll das Verfahren wie folgt ablaufen: Geht ein Notruf, bei dem die erfragten Symptome auf einen Herz-Kreislauf-Stillstand hindeuten, in der Rettungsstelle ein, so werden in das Katretter-System auf Knopfdruck der Ort und weitere Daten des Notrufes eingegeben. Das System sucht nun in den eigenen Datenbanken nach Ersthelfenden, die sich in der Nähe aufhalten, alarmiert unter Angabe

des Ortes des Notfalls nacheinander gefundene Ersthelfende, bis eine Ersthelferin bzw. ein Ersthelfer per App die Annahme des Einsatzes bestätigt. Diese Person begibt sich zum Ort des Notfalls und leistet „Erste Hilfe" bis zum Eintreffen des Rettungswagens. Nach dem Einsatz wird die Ersthelferin bzw. der Ersthelfer um Beantwortung einiger Fragen zu dem Einsatz gebeten, die der wissenschaftlichen Begleitung dienen und mögliche Überforderungen der Ersthelfenden frühzeitig aufzeigen sollen.

Aus rechtlicher Sicht war sicherzustellen, dass eine Teilnahme an dem Verfahren wirklich freiwillig erfolgt. Es darf keinerlei Druck auf Mitarbeitende der Feuerwehr ausgeübt werden, an dem Verfahren teilzunehmen. Auch die Befragung am Ende eines Einsatzes muss freiwillig sein und das Auslassen der Beantwortung einzelner Fragen erlauben. Insbesondere der letzte Punkt wird aus wissenschaftlicher Sicht oft ungern gesehen, da dies die Bewertung der Ergebnisse erschwert. Wir haben darauf hingewirkt, dass dennoch eine entsprechende Umsetzung erfolgt.

Ein weiterer wichtiger Punkt ist die technische Umsetzung des Projektes. Um Ersthelfende in der Umgebung eines Notfallortes ohne Zeitverzug ermitteln zu können, müssen die Standorte der Betreffenden zwangsläufig in einer Datenbank abgelegt und von den Apps regelmäßig aktualisiert werden.

Allerdings ist es nicht notwendig, dass in der Datenbank der exakte Standort von potenziellen Ersthelfenden gespeichert wird, da für die wenigen in Reichweite des Einsatzortes befindlichen Personen im Einsatzfall die genauen Standorte bei der App abgefragt werden können. Nach unserer Beratung werden in der Datenbank die Standorte der Ersthelfenden als Kreise mit einem Durchmesser von 500 Metern aufgeführt. An jedem Punkt in dem Kreis kann sich die bzw. der Ersthelfende mit gleicher Wahrscheinlichkeit befinden.

Zudem ist es nicht notwendig, die Eintragungen zu früheren Standorten von Ersthelfenden aufzubewahren. Dies würde zur Erstellung von Bewegungsprofilen führen und damit u. U. einen tiefen Einblick in die Lebensgewohnheiten der betreffenden Personen erlauben. Für IT-Sicherheitszwecke und zur Prüfung der Funktionalität des Verfahrens ist jedoch die Speicherung von Protokolldaten für einen Zeitraum von ca. vier Tagen erforderlich. Daher werden die Standortdaten aus diesen Protokolldaten nunmehr bereits nach wenigen Stunden entfernt.

Bei Nichtbeachtung der genannten Einschränkungen wäre das Prinzip der Datensparsamkeit verletzt. Zudem würde die Erhebung der genannten Daten Interessenten möglicherweise davon abhalten, sich für das Verfahren anzumelden. Sowohl für die „Unschärfe" der kontinuierlich gespeicherten Standorte der Ersthelfenden als auch für die Speicherdauer der Protokolle, die u. a. Standortdaten enthalten, wurden nunmehr angemessene Werte gefunden, die sowohl die Anforderungen des Datenschutzes erfüllen als auch die Funktionalität des Systems und die Prüfbarkeit der korrekten Arbeitsweise ermöglichen.

Die App „Katretter" kann Menschenleben retten. Bei richtiger Gestaltung von Software und Prozessen wird vermieden, dass genaue Bewegungsprofile der Ersthelfenden entstehen.

3.6 Ortung von Notrufen bei der Berliner Feuerwehr

Smartphones bieten die Möglichkeit, bei einem Notruf den aktuellen Standort des Geräts festzustellen und per SMS oder Internet an die jeweilige Rettungsleitstelle zu übermitteln. Die Berliner Feuerwehr möchte diese Funktionalität im Testbetrieb nutzen.

Von Smartphones per Satellitenortung[112] oder über andere Verfahren festgestellte Standortdaten sind oft wesentlich genauer als die vom Mobilfunknetz anhand der Funkzelle[113] ermittelten Standortdaten. Rettungskräfte könnten gefährdete Personen durch Nutzung dieses Systems schneller finden und somit u. U. Leben retten.

Wir wurden von der Berliner Feuerwehr um rechtliche und technische Bewertung des sog. „Advanced Mobile Location" (AML)-Verfahrens gebeten.

112 Standortermittlung mittels mehrerer Satelliten. Hierfür gibt es verschiedene Systeme, wie z. B. das amerikanische GPS oder das europäische Galileo.

113 Eine Funkzelle in einem Mobilfunknetz bezeichnet den örtlichen Bereich, der von einer Antenne eines bestimmten Mobilfunkmastes bedient wird.

Die Berliner Feuerwehr befand sich diesbezüglich bereits im Austausch mit Rettungsleitstellen anderer Bundesländer, die den Dienst ab 2019 testweise ebenfalls nutzen möchten. Angesichts der bundesländerübergreifenden Bedeutung der Fragestellungen haben wir frühzeitig die anderen Aufsichtsbehörden für den Datenschutz des Bundes und der Länder in unsere Prüfung eingebunden und mit ihnen Fragen zum Standortermittlungsdienst bei Notrufen diskutiert.

Das vorläufige Ergebnis ist, dass es derzeit noch an geeigneten Rechtsgrundlagen für die im Zusammenhang mit dem Verfahren erfolgenden Datenverarbeitungen fehlt. Insbesondere fehlt eine spezifische rechtliche Grundlage für die automatisierte Erhebung von Standortdaten einer im Notfall per Smartphone anrufenden Person durch die Notrufleitstelle der Berliner Feuerwehr. Wir haben der Berliner Feuerwehr insoweit empfohlen, auf die Schaffung einer entsprechenden Vorschrift, z. B. im Berliner Rettungsdienstgesetz, hinzuwirken. Auf die Rechtsgrundlage in der DS-GVO, die eine Datenverarbeitung zulässt, wenn dies zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist[114], sollte aus Gründen der Rechtssicherheit gemäß Erwägungsgrund 46 nur in Einzelfällen zurückgegriffen werden.

Schließlich haben wir die Feuerwehr noch darauf hingewiesen, dass die vorgelagerten Datenverarbeitungen durch das Unternehmen Google (Standortbestimmung und Übermittlung der Standortdaten an die Leitstelle) bei der Bewertung des Verfahrens nicht unberücksichtigt bleiben können. Problematisch ist, dass derzeit noch unklar ist, welche Daten Google zur Standortbestimmung nutzt und ob es sich dabei um Daten handelt, deren Erhebung rechtmäßig erfolgt ist. Hierzu soll eine weitere Klärung in Zusammenarbeit mit den anderen Aufsichtsbehörden für den Datenschutz des Bundes und der Länder erfolgen.

Zudem stellen sich auch technische Fragen. So wird bei einem der eingesetzten Verfahren zur Standortermittlung auf die vom Smartphone in der Nähe entdeckten WiFi-Basisstationen zurückgegriffen. Gegen dieses Verfahren gibt es grundlegende Bedenken, da hierfür regelmäßig die Standorte auch privater WiFi-Basisstationen in Datenbanken von Unternehmen wie Google oder Apple erfasst

114 Art. 6 Abs. 1 lit. d DS-GVO

werden, ohne dass die Unternehmen zuvor die Einwilligung der betroffenen Eigentümerinnen und Eigentümer der WiFi-Basisstationen einholen.

Bei Standortermittlungen im Falle von Notrufen kommt hinzu, dass die Betreffenden ggf. die Standortfunktionen des Smartphones bewusst abgeschaltet haben. Die Smartphones schalten jedoch im Falle eines Notrufs alle Funktionen zur Ermittlung des Standorts und den mobilen Internetzugang ein, um die Standorte der Notrufenden übermitteln zu können. Zudem kommt es hierbei zwangsläufig zu Datenübermittlungen an die Betriebssystemhersteller: Um den eigenen Standort per WiFi-Ortung[115] zu ermitteln, muss ein Smartphone bei einer sehr großen, online verfügbaren Datenbank die Standorte der vom Smartphone entdeckten WiFi-Basisstationen erfragen. Google oder Apple erfahren somit zwangsläufig, dass ein beliebiges Smartphone sich an einem bestimmten Ort aufhält. Zu beantworten ist die Frage, ob und wie die Betriebssystemhersteller diese Daten nutzen und ob die Smartphones bzw. deren Besitzerinnen oder Besitzer hierbei identifiziert werden können.

Obwohl noch nicht alle rechtlichen und technischen Fragen geklärt werden konnten, haben die Aufsichtsbehörden wegen der möglichen Rettung von Menschenleben der Einführung eines Systems zur Ortung von Notrufen durch die Endgeräte und der Übermittlung an die jeweiligen Rettungsleitstellen für einen Testzeitraum von drei Jahren zugestimmt. In diesem Zeitraum müssen die verbleibenden Fragen geklärt werden.

3.7 Videoüberwachung nach Wirksamwerden der DS-GVO

Mit Wirksamwerden der DS-GVO haben sich auch die rechtlichen Grundlagen für den Betrieb von Videoüberwachungskameras geändert. Da die DS-GVO keine spezielle Regelung zur Videoüberwachung enthält, richtet sich der Maßstab für eine datenschutzgerechte Videoüberwachung nach der Generalklausel in Art. 6 Abs. 1 lit. f DS-GVO und nach § 4 BDSG.

115 Ermittlung des Standortes eines Smartphones anhand der in Reichweite befindlichen WiFi-Basisstationen

Danach ist die Verarbeitung personenbezogener Daten (und damit die Videoüberwachung) nur zulässig, wenn sie für die Wahrung berechtigter Interessen von Verantwortlichen oder Dritten erforderlich ist und sofern nicht die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, die den Schutz personenbezogener Daten erfordern. Die DS-GVO verlangt eine Abwägung im konkreten Einzelfall sowohl im Hinblick auf die Interessen der Verantwortlichen oder Dritten als auch der Betroffenen. Diese Formulierung entspricht im Wesentlichen der alten Rechtslage.

Wesentlich konkreter und detaillierter als die alte Regelung sind allerdings die Anforderungen an die Transparenz.[116] Artikel 13 DS-GVO enthält einen langen Katalog von Pflichtinformationen, die bereitzustellen sind. Diese reichen von den Kontaktdaten der oder des Verantwortlichen und ggf. der oder des Datenschutzbeauftragten über die Interessen, die Zwecke und die Rechtsgrundlage der Datenverarbeitung bis hin zur Speicherdauer und zu Betroffenenrechten. Da all diese Informationen unmöglich auf einem herkömmlichen Warnschild Platz finden, ist hier eine abgestufte Lösung möglich. Während die wichtigsten Informationen auf das Schild selbst gehören, können die weiteren Pflichtinformationen am Ort der Videoüberwachung an einer für die betroffene Person zugänglichen Stelle (z. B. an der Rezeption, an der Kasse oder am Empfang) zur Verfügung gestellt werden. Gemeinsam mit den anderen Aufsichtsbehörden der Länder und des Bundes haben wir entsprechende Beispiele erarbeitet, welche von den Betreiberinnen und Betreibern der Videokameras genutzt werden können.[117]

Inhaltlich zeigten uns Bürgerinnen und Bürger vor allem Videoüberwachungen in gastronomischen Einrichtungen und im privaten Wohnumfeld an. In diesen Fällen bleibt es jedoch im Wesentlichen bei der alten Rechtslage. In beiden Bereichen ist eine Videoüberwachung in der Regel unzulässig. Insbesondere dürfen Videoüberwachungen grundsätzlich nicht über die Grundstücksgrenzen hinaus auf Nachbargrundstücke oder ins öffentliche Straßenland reichen.[118]

116 Art. 12 ff. DS-GVO

117 Siehe https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/videoueberwachung-nach-der-ds-gvo

118 Zu Ausnahmen und Einzelheiten siehe https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/videoueberwachung-nach-der-ds-gvo

Die Videoüberwachung des Gastraumes einer gastronomischen Einrichtung ist nach Art. 6 Abs. 1 lit. f DS-GVO i. V. m. § 4 BDSG im Regelfall datenschutzrechtlich unzulässig. Auch hier ändert sich im Vergleich zur alten Rechtslage wenig. Gastronomiebereiche sind Kundenbereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen und damit nicht mit Videokameras überwacht werden dürfen. Das dem Freizeitbereich zuzurechnende Verhalten als Gast einer gastronomischen Einrichtung geht mit einem besonders hohen Schutzbedarf der Persönlichkeitsrechte Betroffener einher. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucherinnen und -besucher und greift damit besonders intensiv in das Persönlichkeitsrecht der Gäste ein. Das schutzwürdige Interesse der Gäste überwiegt im Normalfall das berechtigte Interesse der Gewerbetreibenden an einer Überwachung, weshalb sich deren Interesse nur in seltenen Ausnahmefällen durchsetzen kann.

Zurzeit erarbeiten wir gemeinsam mit unseren Kolleginnen und Kollegen aus den anderen europäischen Datenschutzbehörden intensiv eine gemeinsame Leitlinie, die Betroffene über ihre Rechte aufklären und Kamerabetreiberinnen und -betreibern die Einhaltung der gesetzlichen Vorgaben erleichtern soll.

Die Anforderungen, die an den Betrieb einer Videoüberwachungseinrichtung gestellt werden, sind insbesondere im Bereich der Transparenzpflichten gestiegen. Betreiberinnen und Betreiber von Videoüberwachungskameras sind daher aufgefordert zu prüfen, ob ihre geplanten bzw. bestehenden Überwachungseinrichtungen den gestiegenen Anforderungen entsprechen.

3.8 Videokameras an der Alexwache

Aus der Praxis

Ende 2017 wurde zur Kriminalitätsbekämpfung und mit dem Ziel, die Polizei am Alexanderplatz sicht- und ansprechbar zu machen, die sog. Alexwache eingerichtet. Kurz nach der Eröffnung teilte uns ein Bürger mit, dass ihm aufgefallen sei, dass an den Ecken der Alexwache 360-Grad-Kameras installiert seien. Bei einem Blick in die Wache sei zudem zu sehen, dass die dort tätigen Mitarbeiterinnen und Mitarbeiter die Kameras nach Belieben schwenken und die Bilder live auf großen Monitoren beobachten könnten.

In der daraufhin von uns eingeleiteten Prüfung erklärte die Polizei, dass die Kameras lediglich die Gebäudewände und eine begrenzte Fläche neben der jeweiligen Gebäudeseite erfassten. Die Videoüberwachung werde zur polizeilichen Aufgabenerfüllung durchgeführt, denn die Alexwache sei ein gefährdetes Objekt, bei dem Straftaten drohten, die sich gegen die Polizei als solche richteten. Die Polizei verwies insoweit auf diverse Straftaten gegen Polizeidienststellen sowie Angriffe auf Polizeifahrzeuge und Polizeibeamtinnen und -beamte in jüngster Vergangenheit. In der Silvesternacht sei es zu Böllerwürfen gegen das Dienstgebäude gekommen, zudem sei bereits mehrfach an das Gebäude uriniert und es seien Graffitis gesprüht worden.

Wir teilten der Polizei mit, dass die Alexwache kein gefährdetes Objekt im Sinne des Polizeirechts ist. Unter diesen Begriff fallen vielmehr insbesondere Religionsstätten, Denkmäler, Friedhöfe und Gebäude und sonstige Bauwerke von öffentlichem Interesse.[119] Verbindendes Merkmal dieser Regelbeispiele ist, dass die Objekte selbst unmittelbar von öffentlichem Interesse sind, wobei entweder ihr Bestand als solcher von öffentlichem Interesse ist oder dieses darin begründet ist, dass das Objekt von der Öffentlichkeit genutzt wird.

Bei einer Polizeiwache ist ein solches öffentliches Interesse an dem Gebäude selbst nicht ersichtlich. Insoweit kann man sich auch nicht auf die dort verrichteten Staatsaufgaben wie Gefahrenabwehr und Strafverfolgung berufen, da dies eine Aufgabenbeschreibung der Polizei darstellt, die nicht die Kriterien der Unmittelbarkeit und des besonderen Interesses am Schutz des Objekts erfüllt. Anderenfalls wäre jedes Gebäude, in dem Staatsaufgaben erledigt werden, ein Objekt im Sinne des Polizeirechts, was den Schutzbereich der Vorschrift überspannen würde.

Die Polizei kann sich jedoch aufgrund der beschriebenen Vorfälle an der Alexwache hinsichtlich der Videoüberwachung auf die Wahrnehmung ihres Hausrechts berufen. Dies ist unter engen Voraussetzungen jeder öffentlichen Stelle in Berlin möglich.[120] Bei der Umsetzung ist neben konkreten Kennzeichnungs- und Löschpflichten insbesondere im Rahmen der Verhältnismäßigkeitsprüfung zu beachten,

119 § 24a Allgemeines Sicherheits- und Ordnungsgesetz (ASOG)
120 § 20 BlnDSG

dass der Erfassungsbereich der Kameras auf etwa einen Meter zur Gebäudefassade begrenzt ist.[121]

Die Polizei hat zwischenzeitlich unsere Rechtsposition übernommen und die erforderlichen Maßnahmen umgesetzt. U. a. wurden der Aufnahmebereich der Kameras verkleinert und Hinweisschilder angebracht, die in verständlicher Weise den Erfassungsbereich der Kameras verdeutlichen.

Es ist wichtig, dass sich die Polizei vor der Durchführung von Videoüberwachungsmaßnahmen deren eigentlichen Zweck jeweils verdeutlicht und mögliche Befugnisnormen strikt voneinander trennt. Die Normen haben unterschiedliche Voraussetzungen und entsprechend unterschiedlich schwere Auswirkungen auf die Betroffenen.

121 Siehe Urteil des AG Berlin-Mitte vom 18. Dezember 2003, Az. 16 C 427/02

4 Verkehr und Tourismus

4.1 fahrCard – Mit Lichtbild und vollem Namen?

Ein Petent wandte sich an uns, da sein bisheriges Firmenticket mit Trägerkarte gegen den elektronischen Fahrausweis, die fahrCard, getauscht wurde. Er beschwerte sich zum einen darüber, dass er im Zuge der Umstellung ein Lichtbild zur Anbringung auf der fahrCard einreichen musste, was bei der bisherigen Trägerkarte nicht erforderlich gewesen sei. Zum anderen bemängelte er, dass Kontrolleure bei Fahrausweiskontrollen nicht nur seinen vollständigen Namen, sondern auch sein Geburtsdatum einsehen könnten.

Die Anbringung des Lichtbildes ist zulässig, da es sich um eine persönliche, nicht übertragbare Zeitkarte handelt. Die BVG teilte uns hierzu mit, dass sich zum einen aus den VBB-Tarifbestimmungen ergebe, dass persönliche elektronische Fahrausweise mit einem Lichtbild zu versehen sind,[122] zum anderen sei das Lichtbild für eine effiziente Kontrolle der Nutzungsberechtigung für den Fahrausweis erforderlich. Das Lichtbild ist somit für die Erfüllung eines Vertrages zwischen dem jeweiligen fahrCard-Inhaber und der BVG erforderlich.[123]

Die BVG passte jedoch entsprechend unserer Empfehlung die Speicherung personenbezogener Daten auf der fahrCard dergestalt an, dass künftig nur noch das Geburtsjahr[124] sowie die Anfangsbuchstaben des Vor- und Familiennamens[125] erfasst werden, sodass die vollständigen Angaben für das Kontrollpersonal nicht mehr sichtbar sind.[126]

Die BVG bot dem Petenten an, seine fahrCard kostenfrei auszutauschen.

122 Anlage B zum VBB-Tarif, Ziffer 5.2.5, Unterabsatz 6
123 Art. 6 Abs. 1 Satz 1 lit. b DS-GVO
124 Sowie Tag und Monat stets als „01.01."
125 Unter Ersetzung der übrigen Buchstaben durch „*"
126 Dies entspricht der empfohlenen Kürzungsregel im VDV-Kernapplikations-Standard, auf dem auch die fahrCard basiert.

Auf elektronischen Fahrausweisen dürfen nur solche Angaben gespeichert werden, die zur Kontrolle der Gültigkeit sowie der Nutzungsberechtigung erforderlich sind. Das Geburtsdatum und der vollständige Name sind hierzu in der Regel nicht erforderlich.

4.2 Fahrschule: Datenweitergabe an einen Interessenverband

Aus der Praxis

Eine Fahrschule hatte sich an uns gewandt, da sie bereits wenige Tage nach Erhalt ihrer Betriebserlaubnis ein Werbeschreiben eines Interessenverbandes erhalten hatte, das zur Eröffnung der Fahrschule gratulierte und um eine Mitgliedschaft warb. Sie äußerte die Vermutung, dass das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) als zuständige Aufsichtsbehörde die Informationen an den Interessenverband weitergegeben haben könnte.

Das LABO bestätigte diese Vermutung und teilte mit, dass die Erteilung einer Betriebserlaubnis für Fahrschulen nicht nur aufgrund gesetzlicher Verpflichtungen z. B. dem Gewerbeamt und dem Kraftfahrtbundesamt mitgeteilt werde, sondern auf dessen Wunsch auch besagtem Interessenverband. Die Mitteilung an den Verband sei auf der Grundlage des Berliner Informationsfreiheitsgesetzes (IFG) erteilt worden.

Die Mitteilung der Erteilung der Betriebserlaubnis an den Interessenverband war zulässig. Nach dem IFG kann jeder Mensch Auskunft über den Inhalt der von der öffentlichen Stelle geführten Akten erhalten,[127] wenn keiner der dortigen Ausschlussgründe greift.[128]

Vorliegend waren bereits keine personenbezogenen Daten betroffen, da es sich bei der Fahrschule um eine juristische Person handelt.[129] Aber selbst die Mittei-

127 § 3 Abs. 1 IFG

128 § 4 Abs. 1 IFG

129 Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO nur solche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

lung, dass einer natürlichen Person eine Betriebserlaubnis für eine Fahrschule erteilt wurde, wäre zulässig gewesen. Schutzwürdige Belange stehen der Offenbarung personenbezogener Daten nach dem IFG in der Regel nicht entgegen, soweit sich aus einer Akte ergibt, dass die Betroffenen an einem Verwaltungsverfahren oder einem sonstigen Verfahren beteiligt sind, und durch diese Angaben mit Ausnahme bestimmter Kerndaten[130] nicht zugleich weitere personenbezogene Daten offenbart werden.[131] Die Tatsache, dass eine natürliche Person erfolgreich an einem Verwaltungsverfahren zur Erteilung einer Betriebserlaubnis beteiligt war, darf also in der Regel auf Antrag nach dem IFG zusammen mit den Kerndaten wie Name und Anschrift offenbart werden.

Weitere Ausschlussgründe kamen nicht in Betracht, sodass die Weitergabe der Informationen rechtmäßig war.

Die Übermittlung personenbezogener Daten bedarf stets einer Rechtsgrundlage. Hierfür kommen nicht nur gesetzliche Übermittlungspflichten in Betracht, sondern auch Bestimmungen nach dem IFG.

4.3 Pflicht zur Bestellung von Datenschutzbeauftragten bei Taxiunternehmen

Uns erreichten mehrere Anfragen von Taxiunternehmen, ob diese verpflichtet seien, eine bzw. einen betrieblichen Datenschutzbeauftragten zu bestellen.

Verantwortliche sind verpflichtet, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.[132] Unerheblich ist dabei, ob die Verarbeitung personenbezogener

130 Namen, Titel, akademischer Grad, Geburtsdatum, Beruf, Branchen- oder Geschäftsbezeichnung, innerbetriebliche Funktionsbezeichnung, Anschrift und Rufnummer, § 6 Abs. 2 Satz 1 Nr. 1 IFG

131 § 6 Abs. 2 Satz 1 Nr. 1 lit. a IFG

132 § 38 Abs. 1 BDSG ergänzend zu Art. 37 Abs. 1 lit. b und c DS-GVO

Daten als Kerntätigkeit erfolgt, vielmehr genügt hierfür die regelmäßige automatisierte Verarbeitung.

Eines der Taxiunternehmen beschäftigte im Büro sechs Mitarbeiterinnen und Mitarbeiter, die personenbezogene Daten der Fahrgäste verarbeiteten, sowie 30 Taxifahrerinnen und Taxifahrer, die Taxifahrten durchführten. Für die Frage des Vorliegens einer Bestellpflicht war daher zu prüfen, ob auch die Taxifahrerinnen und Taxifahrer ständig mit der automatisierten Verarbeitung personenbezogener Daten betraut waren.

Falls die Vermittlung von Fahraufträgen elektronisch erfolgt, z. B. per Terminal, per Funkgerät mit entsprechender Funktion oder per App auf dem Smartphone, ist die Kenntnisnahme sowie Annahme der Aufträge als automatisierte Verarbeitung personenbezogener Daten anzusehen. Etwas anderes kann allenfalls hinsichtlich solcher Aufträge gelten, die nicht elektronisch, sondern etwa per herkömmlichem Funkgerät oder in Papierform erteilt werden. Da Taxifahrerinnen oder Taxifahrer aber heutzutage in der Regel Aufträge jedenfalls auch elektronisch annehmen, ist von einer regelmäßigen automatisierten Verarbeitung auszugehen.

Taxiunternehmen sind daher verpflichtet, eine oder einen Datenschutzbeauftragten zu bestellen, wenn sie insgesamt mindestens zehn Mitarbeiterinnen und Mitarbeiter, die entweder im Büro personenbezogene Daten verarbeiten oder Taxifahrten nach elektronischer Auftragsannahme durchführen, beschäftigen.

Eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter ist immer dann zu bestellen, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten betraut sind. Es muss sich dabei nicht um eine Kerntätigkeit dieser Personen handeln, vielmehr genügt bereits die regelmäßige Verarbeitung.

4.4 Intelligente Videoüberwachung im Bahnhof Berlin-Südkreuz

Im Rahmen des gemeinsamen Pilotprojekts „Sicherheitsbahnhof Berlin Südkreuz" vom Bundesministerium des Innern, der Bundespolizei, dem Bundeskriminalamt und der Deutschen Bahn AG (DB AG) werden seit August 2017 Systeme der sog. „intelligenten" Videoüberwachung getestet. Das Projekt gliedert sich in zwei Teilprojekte:

Im ersten Pilotprojekt testete die Bundespolizei den Einsatz biometrischer Gesichtserkennungssysteme.[133] Im Vorfeld wurde hierfür eine Datenbank mit Lichtbildern von über 200 freiwillig am Projekt teilnehmenden Personen erstellt. Die Systeme sollten in speziell gekennzeichneten Innenbereichen des Bahnhofs zunächst die Gesichter vorbeigehender Fahrgäste aufnehmen, mit den zuvor in der Datenbank gespeicherten Bilddaten der Freiwilligen abgleichen und letztlich deren Gesichter bei jeder Erkennung herausfiltern und zählen. Dieser erste Test wurde im Juli 2018 abgeschlossen. Der im Abschlussbericht der Bundespolizei durch eine Kombination der drei getesteten Systeme erreichten hohen Trefferquote stand dabei eine sehr hohe Falscherkennungsrate, also eine große Zahl ausgelöster Fehlalarme, gegenüber. Jedes einzelne dieser Systeme für sich wies sogar noch eine erheblich höhere Fehlerquote auf.[134] In ihrem Abschlussbericht geht die Bundespolizei im Ergebnis für alle drei Systeme zusammen von drei bis vier falschen Treffermeldungen pro Kamera und Stunde aus; zu bestimmten Tageszeiten können die Fehlerzahlen wesentlich höher liegen.[135] Dies bedeutet, dass während des Projektes ca. 80.000 bis 100.000 Mal Personen zu Unrecht erfasst wurden.[136] Trotzdem bilanzierte die Bundespolizei, dass die Gesichtserkennungs-

133 JB 2017, 3.6

134 Siehe hierzu Analyse des Chaos Computer Clubs vom 13.10.2018

135 S. 15 des Berichts Anhang 3 – Analyse der Testdaten zum Teilprojekt 1 „Biometrische Gesichtserkennung", abrufbar unter https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile

136 Diese Zahl ergibt sich wie folgt: 365 Tage Laufzeit des Tests x 24 Stunden pro Tag x drei Kameras x drei bis vier Falschmeldungen.

systeme nach dem derzeitigen Stand der Technik ein gutes Unterstützungsinstrument für die polizeiliche Fahndung sein könnten.

Wir sehen dies definitiv anders. Unbescholtene Passantinnen und Passanten im Bahnhof Südkreuz gerieten nach den vorliegenden Ergebnissen regelmäßig in Gefahr, zum Gegenstand biometrischer Datenverarbeitung zu werden, ohne dass es dafür einen Anlass gegeben hätte. Bei einem Echtbetrieb bestünde somit ein hohes Risiko, dass eine große Zahl von Bürgerinnen und Bürger fälschlicherweise zum Gegenstand polizeilicher Ermittlungen würde. Sehr fraglich wäre auch, ob die hohe Fehlerquote nicht unweigerlich dazu führen würde, dass ein korrekter Treffer nicht als solcher erkannt würde, weil ständig viel zu viele Falschmeldungen von Hand aussortiert werden müssten. Wir haben im letzten Jahr vor der Problematik gewarnt.[137] Für die abschließende rechtliche Bewertung der Datenverarbeitung dieses ersten Teilprojekts durch die Bundespolizei ist allerdings die bzw. ab 2019 der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig.

In einem zweiten Testszenario soll voraussichtlich im zweiten Quartal 2019 die Erprobung sog. „intelligenter" Videoanalysesysteme für die Behandlung und Auswertung verschiedener Gefahrenszenarien erfolgen. Dabei sollen hilflos liegende Personen, große Menschenansammlungen und verdächtige Gegenstände automatisiert durch die Datenverarbeitungssysteme erkannt und gemeldet werden. Hierfür ist geplant, mit Hilfe von fünf bis zehn freiwilligen Personen konkrete Testszenarien im Bahnhofsbereich nachzustellen, z. B. das Abstellen eines Gepäckstücks und die Nachverfolgung der Person, die dieses Gepäckstück abgestellt hat.

Für die Durchführung des zweiten Testszenarios ist die Deutsche Bahn praktisch und datenschutzrechtlich verantwortlich und damit auch wir alszuständige Datenschutzaufsichtsbehörde für die Deutsche Bahn. Als solche haben wir dringend geraten, auf eine biometrische Datenverarbeitung zu verzichten. Denn aufgrund der Tatsache, dass sich ein biometrisches Charakteristikum meist das ganze Leben hindurch nicht verändert, birgt eine solche Datenverarbeitung erhebliche Sicherheitsrisiken. Eine Erhebung biometrischer Daten liegt nicht nur bei der Gesichtserkennung vor, sondern auch bei sonstigen Daten zu physischen, phy-

137 JB 2017, 3.6

siologischen oder verhaltenstypischen Merkmalen, wie z. B. dem individuellen Gang einer Person.[138] Bei einem Verlust der Daten können Betroffene ein Leben lang Opfer von Identitätsdiebstahl und Folgekriminalität werden. Die Erhebung biometrischer Daten ist daher immer mit einem sehr tiefen Eingriff in die Privatsphäre und einem erheblichen Risiko verbunden. Konsequenterweise ist die Verarbeitung von biometrischen Daten durch nicht-öffentliche Stellen nach der Datenschutz-Grundverordnung grundsätzlich verboten und nur in engen Ausnahmefällen zulässig.[139]

Die Deutsche Bahn hat sich bereit erklärt, bei dem Test auf die Erhebung biometrischer Daten zu verzichten. Wir begleiten das Projekt eng, um sicherzustellen, dass diese Vorgabe und andere datenschutzrechtliche Vorschriften eingehalten werden.

Die Verarbeitung biometrischer Daten ist mit erheblichen Risiken verbunden. Daher sollte diese von Sicherheitsbehörden äußerst sparsam und nur dann eingesetzt werden, wenn sie nicht zu fehleranfällig ist und nach Abwägung aller Aspekte ein messbarer Mehrwert für die Sicherheit der Bürgerinnen und Bürger die Einschränkungen des Rechts auf informationelle Selbstbestimmung deutlich überwiegt. Nicht öffentlichen Stellen ist die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung von Personen grundsätzlich verboten und nur in engen Ausnahmefällen erlaubt.

4.5 Vernetztes und automatisiertes Fahren – Welche Datenschutzrisiken entstehen durch die neuen Techniken?

Der technische Fortschritt zeigt sich auch im Automobilbereich sehr deutlich. Neben der Elektromobilität sind insbesondere das vernetzte und autonome Fahren wichtige Zukunftsfelder. Doch die Verbesserungen für die Verkehrssicherheit und der erhöhte Komfort für die Nutzer der Fahrzeuge können zu datenschutzrechtli-

138 Art. 4 Nr. 14 DS-GVO
139 Art. 9 DS-GVO

chen Risiken führen, da die technischen Hilfsmittel auch zunehmend Daten über die Fahrer bzw. die Fahrzeuginsassen erfassen. Negative Auswirkungen wären z. B. die Erstellung von Bewegungs-, Verhaltens- oder Nutzungsprofilen.

Im Automobilbereich haben sich in den letzten Jahren mögliche datenschutzrechtliche Risiken gleichzeitig mit dem technischen Fortschritt deutlich erhöht. Dies beginnt bereits bei Autovermietern, die ihre Fahrzeuge heutzutage zur Diebstahlsvermeidung meist permanent per GPS überwachen. Ebenso betrifft dies Assistenzsysteme, welche zur Gewährleistung der entsprechenden Fahrsicherheitsfunktionen auch zahlreiche personenbeziehbare Daten aus dem Fahrzeug abrufen und auswerten. Ein weiteres Beispiel sind moderne Fahrzeuge, die bereits heute in der Lage sind, in Echtzeit Daten miteinander auszutauschen und in Zukunft sogar vollautomatisch fahren sollen.

Viele dieser modernen Techniken dienen der Erhöhung der Verkehrssicherheit, schnellerem Informationsgewinn für Rettungskräfte und verbessertem Komfort für die Nutzenden und sind somit grundsätzlich begrüßenswert. Wichtig ist hierbei jedoch, dass die Prozesse der Datenverarbeitung für die Betroffenen transparent erfolgen, sodass die Fahrzeughalterinnen und -halter und die Fahrerinnen und Fahrer aktiv entscheiden können, mit welchen Erhebungen und Verarbeitungen persönlicher Daten sie einverstanden sind. Ebenso müssen in der Vergangenheit erteilte Einwilligungen – z. B. zur Erhebung des Fahrzeugstandorts – auch wieder spezifisch zurückgezogen werden können. Technische Lösungen, bei denen man nur zwischen der umfassenden Einwilligung in alle Datenverarbeitungen oder dem kompletten Verzicht auf intelligente Mobilitätsdienste wählen kann, sind nicht akzeptabel. Diese Forderungen sind durch die seit dem 25. Mai 2018 geltende DS-GVO auch gesetzlich verankert, denn nach den in ihr formulierten Prinzipien „Privacy by Design“ und „Privacy by Default“ sind technische Systeme und die Voreinstellungen der Geräte so datenschutzfreundlich wie nach dem Stand der Technik möglich zu gestalten.[140] Des Weiteren sind geeignete technisch-organisatorische Maßnahmen zu treffen, um ein dem jeweiligen Risiko angemessenes Schutzniveau für die Sicherheit der Datenverarbeitung zu gewährleisten.[141]

140 Art. 25 DS-GVO
141 Art. 32 DS-GVO

Dies ist umso wichtiger, als große Datenmengen für die Funktionen des automatisierten und vernetzten Fahrens verarbeitet werden. So kann in einem modernen vernetzten Fahrzeug z. B. nicht nur erfasst werden, mit welcher Geschwindigkeit sich das Fahrzeug bewegt und wie viele Personen sich im Fahrzeug befinden. Auch zahlreiche weitere Informationen können erfasst werden, z. B. ob der Fahrer bereits Müdigkeitserscheinungen zeigt, wie sich sein Beschleunigungsverhalten darstellt oder welche Sitz- und Komforteinstellungen die Fahrzeuginsassen jeweils gewählt haben. Oder auch, welche Strecken zuletzt gefahren worden sind, wie groß der Abstand zu anderen Fahrzeugen ist, in welchem Zustand die Reifen sind oder ob das Fahrzeug auf trockener oder glatter Strecke unterwegs ist. Dies sind nur einige Beispiele für eine Vielzahl erzeugter Daten, welche durch Steuergeräte oder Sensoren im Innen- und Außenbereich der Fahrzeuge permanent erfasst, gespeichert und verarbeitet werden. Ein Teil dieser Daten wird direkt nach Erhebung und Auswertung wieder verworfen, viele Daten werden jedoch durchaus auch längerfristig gespeichert (z. B. zuletzt gefahrene Strecken, persönliche Einstellungen der verschiedenen Nutzer eines Fahrzeugs, Nutzung von Navigations- und Mediendiensten, Diagnosedaten des Fahrzeugs etc.).

Eine besondere Bedeutung kommt in diesem Zusammenhang Ortungs- und Positionsdaten zu. Diese werden nicht nur von verschiedenen Navigations- und Komfortdiensten im Fahrzeug verarbeitet, sondern u. a. auch durch das Notrufsystem „eCall", das seit Oktober 2015 in Europa verpflichtend für alle neuen Modelle von Pkws und leichten Nutzfahrzeugen vorgeschrieben ist. Bei einem Unfall wird das Fahrzeug automatisch lokalisiert und die lokale Rettungsleitstelle kann mit dem Fahrer über eine Mobilfunkeinheit kommunizieren. Die Funkeinheit ist hier jeweils mit einer eigenen SIM-Karte ausgestattet, die fest im Auto verbaut ist. Der eCall-Notruf in seiner Basisfunktion unterliegt strengen Vorschriften zur Wahrung des Datenschutzes, mögliche Zusatzdienste durch Dritte (z. B. Fahrzeughersteller) sind hiervon hingegen nicht erfasst. Somit besteht hier das Risiko eines unbefugten Abrufs von Daten über das Fahrzeug oder das Fahrverhalten der Nutzer insbesondere durch private Datenverarbeiter, deren Dienste in moderne Fahrzeugsysteme eingebettet sind.

Vernetzte und automatisierte Fahrzeuge nutzen darüber hinaus eine Vielzahl weiterer Sensoren, um permanent die eigene Position im Vergleich zu anderen Fahr-

zeugen sowohl zur Vorbeugung und Vermeidung von Unfällen als auch zur optimalen Routenplanung sicherzustellen.

Darauf aufbauend plant die Automobilindustrie auch bereits, kooperative Systeme für PKW und LKW einzusetzen, durch die Fahrzeuge und sogar die Verkehrsinfrastruktur in die Lage versetzt werden, sich selbstständig untereinander zu verständigen. Dies ermöglicht z. B. frühzeitige Stauwarnungen und die Berechnung geeigneter Alternativrouten durch das jeweilige Navigationssystem. Bordsysteme warnen vor möglichen Gefahren auf der Strecke oder suchen auf Wunsch den nächsten freien Parkplatz. Lastkraftwagen könnten automatisch vernetzt in Kolonnen fahren, um treibstoffsparend und umweltschonend an ihr Ziel zu gelangen.

Erste Testeinsätze dieser sog. Car-to-X-Kommunikation gibt es bereits und sollen in den nächsten Jahren sicherlich sukzessive weiter ausgebaut werden. Ermöglicht wird dies u. a. auch durch den Aufbau der nächsten Generation von deutlich leistungsstärkeren Mobilfunknetzen, der sog. 5G-Netze[142]. Die deutlich schnelleren Datenraten im mobilen Internet ermöglichen die Vernetzung von Fahrzeugen und Verkehrsinfrastruktur, produzieren gleichzeitig jedoch auch höhere Risiken durch die Übertragung personenbeziehbarer Informationen zum Mobilfunkgerät (z. B. Nummer der verwendeten SIM-Karte, IMEI-Nummer des Mobilfunkgeräts) oder durch Informationen zum Fahrzeug (z. B. ID des vernetzten Fahrzeugs, Kennzeichen, Fahrzeug-Identnummer). Aus den gewonnenen Daten lassen sich u. a. Bewegungs- und Nutzungsprofile erstellen. Auch die Häufigkeit der Nutzung eines Fahrzeugs und die Anzahl unterschiedlicher Fahrzeugführer ließe sich daraus ggf. ermitteln.

Aufbauend auf den bereits beschriebenen Szenarien haben sich inzwischen auch weitere Nutzungsmöglichkeiten in anderen Geschäftszweigen entwickelt, die genau betrachtet werden müssen. So bietet die Versicherungsindustrie z. B. seit einigen Jahren verstärkt optionale Telematiktarife[143] an, welche durch eine genaue Aufzeichnung und Analyse aller Fahrstrecken und zahlreicher Details (z. B. Häufigkeit der Fahrten, durchschnittliche Fahrtlänge und -dauer, Uhrzeit der Fahrten, gewählte Ziele, Fahrstil etc.) umfangreiche Rückschlüsse auf das jeweilige Fahr-

142 5G steht hierbei für „5. Generation" der Mobilfunknetze.

143 Diese werden im Englischen oft auch als „Pay as you Drive"-Tarife bezeichnet.

verhalten der Kundinnen und Kunden zulassen. Versicherungsnehmern, die freiwillig in die dafür notwendige Datenaufzeichnung einwilligen, wird im Gegenzug ein Rabatt auf ihren individuellen Versicherungsbeitrag in Aussicht gestellt. Der europäische Verband der Versicherer hat auch bereits Interesse daran bekundet, dass seine Mitgliedsunternehmen zukünftig ggf. auch Zugriff auf die eCall-Daten ihrer Kundinnen und Kunden erhalten sollen, um Versicherungstarife noch genauer anpassen zu können.

Grundsätzlich sind neue Techniken zur Erhöhung der Verkehrssicherheit und beschleunigten Versorgung von Unfallopfern sowie zur Verbesserung des Verkehrsflusses sicher begrüßenswert. Gleichwohl dürfen bei allen Vorteilen auch die Risiken der neuen Technologien nicht außer Acht gelassen werden. Nahezu jede Technik birgt auch entsprechende Gefahren des Datenmissbrauchs. So beugt die permanente Ortung eines Fahrzeugs zwar möglicherweise Diebstählen vor, ermöglicht jedoch auch die Erstellung von Bewegungsprofilen. Bei der Aufladung von Elektroautos wird zu Abrechnungszwecken regelmäßig auch mindestens eine personenbeziehbare ID der Kundin oder des Kunden durch den jeweiligen Anbieter erfasst, um den Ladevorgang bei der Abrechnung zuordnen zu können. Telematikangebote wiederum müssen meist zahlreiche Daten aus Fahrzeugen sammeln, damit die Technik effektiv funktioniert. Damit einher geht oftmals automatisch eine technische Überwachung der Fahrerinnen und Fahrer. Hinsichtlich der vernetzten und automatisierten Fahrzeuge der Zukunft sind die Automobilindustrie und die mit ihr verbundenen Industriezweige (z. B. Zulieferbetriebe und Versicherungsunternehmen) ebenso wie Politik und Verwaltung somit aufgefordert, technischen Fortschritt und Datenschutz vernünftig in Einklang zu bringen.

Im Sinne der Verbesserung der Verkehrssicherheit und für den erhöhten Komfort der Kunden sind viele der neuen Technologien im Automobilbereich durchaus begrüßenswert. Jedoch sollte hier stets zwischen dem zu erwartenden Nutzen durch die Technik und möglichen Risiken für den Datenschutz abgewogen werden. Neben der Datensicherheit und dem Datenschutz ist hierbei insbesondere auch die Transparenz der Anbieter gegenüber den Kundinnen und Kunden wichtig, damit diese stets umfassend darüber informiert sind, welche Daten ggf. gesammelt und für welchen Zeitraum sie gespeichert werden und welche Stellen Zugriff auf die Daten haben. Die beschriebenen Technologien

werden zukünftig auch in Berlin zum Einsatz kommen und ggf. durch Berliner Anbieter weiterentwickelt werden. Wir werden die weitere Entwicklung daher aufmerksam beobachten.

5 Jugend und Bildung

5.1 Anpassung des Berliner Schulgesetzes an die DS-GVO – Ende gut, alles gut?

Wir haben die Senatsverwaltung für Bildung, Jugend und Familie bei der Anpassung des Berliner Schulgesetzes an die DS-GVO beraten. Dieser Prozess verlief nicht von vornherein reibungslos.

Die DS-GVO entfaltet zwar unmittelbare Wirkung in allen Mitgliedsstaaten der Europäischen Union, enthält jedoch an vielen Stellen mit den sog. Öffnungsklauseln auch Gestaltungsspielräume für die nationalen Gesetzgeber. Gleichzeitig sind die Mitgliedsstaaten gefordert, alle nationalen Vorschriften, die eine Regelung zur Verarbeitung personenbezogener Daten zum Gegenstand haben, auf ihre Vereinbarkeit mit den europarechtlichen Vorgaben zu prüfen. Einer entsprechenden Prüfung war damit auch das Berliner Schulgesetz, das die maßgeblichen Datenverarbeitungsbefugnisse für die Schulen, Schulbehörden, Schulaufsichtsbehörde usw. enthält, zu unterziehen.

Der Referentenentwurf, der uns im März 2018 vorgelegt wurde, setzte die datenschutzrechtlichen Vorgaben noch sehr unzureichend um. Insbesondere enthielt der Entwurf keine mit den Vorgaben der DS-GVO zu vereinbarende Regelung zur Verarbeitung besonderer Kategorien personenbezogener Daten. Hierzu zählen z. B. Gesundheitsdaten der Schülerinnen und Schüler oder Angaben über ihre religiösen oder weltanschaulichen Überzeugungen. Des Weiteren fehlten z. B. Verarbeitungsbefugnisse für Elternvertretungen, die im Schulalltag ebenfalls mit der Verarbeitung von personenbezogenen Daten befasst sind.

Leider hat uns die Senatsverwaltung in der Folgezeit nicht weiter in den Überarbeitungsprozess eingebunden. Im Sommer 2018 mussten wir einer Pressemitteilung entnehmen, dass ein neuer Entwurf bereits dem Senat vorgelegt worden war. Darin hatte die Senatsverwaltung unsere Kritik in wesentlichen Punkten lei-

der nicht aufgegriffen. Wir haben unsere Kritikpunkte gegenüber der Senatsverwaltung dann noch einmal deutlich gemacht. Wir konnten schließlich erreichen, dass einige Vorschriften datenschutzkonform angepasst wurden. Das Schulgesetz enthält nun z. B. klare Regelungen zur Verarbeitung besonderer Kategorien personenbezogener Daten.

Also Ende gut, alles gut? – Nicht ganz.

Denn auch das nunmehr verabschiedete Gesetz enthält weiterhin vor allem eine sehr problematische Regelung. So begründet das Schulgesetz fortan u. a. eine Befugnis für die Schulaufsichtsbehörde, die Daten von Schülerinnen und Schülern unter bestimmten Voraussetzungen auch nach dem Verlassen der Schule zu verarbeiten, um sie z. B. in eine Berufsausbildung zu vermitteln.[144] Dies ist schon deshalb nicht tragbar, weil es sich bei den betroffenen Personen regelmäßig um solche handelt, die gerade nicht mehr zur Schule gehen und damit auch nicht mehr den Regelungen des Schulgesetzes unterliegen. Natürlich sollte die Schule sich um die Vorbereitung von Schülerinnen und Schülern auf das Berufsleben kümmern. Dies müsste aber während der Schulzeit geschehen, nicht danach. Es gehört nicht zu den gesetzlichen Aufgaben der Schulaufsichtsbehörde, derartige Maßnahmen für ehemalige Schülerinnen und Schüler zu organisieren, egal, ob diese Bedarf haben oder nicht, weil sie z. B. gar nicht mehr in Berlin wohnen oder sich schon längst beruflich orientiert haben. Eine solche Maßnahme kann daher nur als zusätzliche Dienstleistung zur freiwilligen Annahme angeboten werden. Eine Speicherung personenbezogener Daten Ehemaliger kann dementsprechend auch nur auf freiwilliger Basis erfolgen, nämlich dann, wenn die Betreffenden das Angebot als für sich nützlich annehmen wollen. Der Gesetzgeber sollte seine Entscheidung daher noch einmal überdenken und bei der nächsten Änderung des Schulgesetzes an dieser Stelle nachbessern.

Mit der Anpassung des Schulgesetzes an die DS-GVO ist eine wesentliche Herausforderung gemeistert – wenn auch nicht in jedem Punkt zufriedenstellend. Jetzt gilt es, auch die Schuldatenverordnung, die derzeit ebenfalls überarbeitet wird, auf den neuesten Stand zu bringen und ihr zügig Geltung zu verschaffen.

144 § 64 Abs. 7 in der Fassung des zum 1. Januar 2019 in Kraft getretenen Schulgesetzes

5.2 Umsetzung der DS-GVO in der Kinder- und Jugendhilfe

Seit dem 25. Mai 2018 sind auch bei den Jugendämtern und den zahlreichen privatrechtlich organisierten freien Trägern der Kinder- und Jugendhilfe die Vorschriften der DS-GVO anzuwenden. In der Praxis besteht ein hoher Informationsbedarf im Hinblick auf die geänderte Rechtslage.

Uns haben zahlreiche Anfragen für Beteiligungen an Informationsveranstaltungen erreicht. Nicht allen Anfragen nach Vorträgen konnten wir aufgrund unserer begrenzten Kapazitäten nachkommen. Wir haben uns darauf konzentriert, möglichst viele Multiplikatorinnen und Multiplikatoren zu erreichen. Mit dem Sozialpädagogischen Fortbildungsinstitut Berlin-Brandenburg (SFBB), das für die Fortbildung der pädagogischen Fachkräfte in der Kinder- und Jugendhilfe beider Bundesländer verantwortlich ist, haben wir im Juni 2018 eine Fachveranstaltung zur DS-GVO durchgeführt, an der über 100 pädagogische Fachkräfte teilgenommen haben.[145] Ziel war es, den Teilnehmenden einen ersten Überblick über die Auswirkungen des neuen europäischen Datenschutzrechts auf die Praxis der Kinder- und Jugendhilfe zu geben und das Verhältnis zu den Vorschriften des Sozialdatenschutzrechts zu beleuchten. Aufgrund der hohen Resonanz auf die Veranstaltung wird es im Frühjahr 2019 eine vertiefende Fachtagung geben, an der wir wieder aktiv beteiligt sind.

In der Kinder- und Jugendhilfe sind auch nach dem Wirksamwerden der DS-GVO – wie bisher – die bereichsspezifischen Vorschriften der Sozialgesetzbücher[146] anzuwenden. Während der Bundesgesetzgeber die Vorschriften des SGB I und SGB X noch vor Wirksamwerden der DS-GVO angepasst hat, steht eine solche Anpassung für das für die Kinder- und Jugendhilfe vornehmlich maßgebende SGB VIII noch aus. Für die Fachkräfte besteht die Herausforderung in der Praxis darin, die verschiedenen Regelungswerke nebeneinander anzuwenden.

145 Die Tagungsdokumentation lässt sich auf der Webseite des SFBB herunterladen, https://sfbb.berlin-brandenburg.de/sixcms/detail.php/873533/

146 Sozialgesetzbuch – Erstes Buch – Allgemeiner Teil (SGB I), Sozialgesetzbuch – Achtes Buch – Kinder- und Jugendhilfe (SGB VIII) und Sozialgesetzbuch – Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz (SGB X)

Mit der DS-GVO ergeben sich im Umgang mit Sozialdaten bei der Gewährung von Leistungen der Kinder- und Jugendhilfe (z. B. Hilfen zur Erziehung, aber auch im Umgang mit Kindeswohlgefährdungen) keine gravierenden Änderungen, da die Voraussetzungen der Zulässigkeit der Datenverarbeitung sich im Rahmen von Öffnungsklauseln für das mitgliedstaatliche Recht auch weiterhin aus den sozialdatenschutzrechtlichen Vorschriften ergeben.

Neuerungen ergeben sich aber z. B. bei den auch in der Kinder- und Jugendhilfe zu beachtenden Informationspflichten oder den erweiterten Betroffenenrechten nach der DS-GVO.[147] Wir wurden hier auf durchaus nachvollziehbare praktische Probleme aufmerksam gemacht: Gerade bei telefonischen Beratungen (z. B. in Krisensituationen) oder auch in der Beratung von Jugendlichen in prekären Situationen, für die die Hemmschwelle, Beratung anzunehmen, ohnehin hoch sein kann, besteht die Gefahr, dass schriftliche Informationserklärungen ihr Ziel verfehlen und eher abschreckend wirken. Hier kommt es darauf an, praktikable Lösungen zu finden. Diese müssen in erster Linie im Sinne der betroffenen Personen sein. Da der Transparenz und dem Aufbau einer Vertrauensbeziehung in helfenden Kontexten ohnehin eine besondere Bedeutung zukommt, halten wir es durchaus für geeignet, den Informationspflichten auch im Rahmen von erläuternden Gesprächen mit entsprechender Dokumentation nachzukommen.

Den mit der DS-GVO für die Praxis verbundenen Auswirkungen ist gerade in Bereichen, in denen sensible Daten verarbeitet werden, besondere Aufmerksamkeit zu widmen. Uns ist es ein Anliegen, die Kinder- und Jugendhilfe hier zu unterstützen.

147 Art. 13 ff. DS-GVO

5.3 Einheitliche Fachverfahren in der Berliner Jugendhilfe – Sachstandsbericht

Auch in diesem Jahr sind wieder neue Module des verwaltungsübergreifenden Fachverfahrens ISBJ-Jugendhilfe (SoPart), das als zentrales Fachverfahren in allen zwölf Berliner Jugendämtern zum Einsatz kommt[148], durch die Senatsverwaltung für Bildung, Jugend und Familie in den Echtbetrieb übernommen worden.

Das verwaltungsübergreifende Großprojekt Integrierte Software Berliner Jugendhilfe (ISBJ) begleiten wir seit vielen Jahren. Die aktuell eingeführte zentrale IT-Lösung für alle bezirklichen Jugendämter musste in diesem Jahr an die Neuerungen durch die DS-GVO angepasst werden. Z. B. war eine Datenschutzerklärung zu entwickeln, um den Informationspflichten[149] für die betroffenen Personen nachzukommen. Wir haben die für die Einführung des Fachverfahrens federführende Senatsverwaltung für Bildung, Jugend und Familie bei der Erstellung einer rechtzeitig zum 25. Mai 2018 zentral für die Bezirke zur Verfügung gestellten Erklärung datenschutzrechtlich beraten. Diese wird sicherlich aufgrund der ersten praktischen Erfahrungen mit der DS-GVO nach einer gewissen Zeit evaluiert werden müssen. Neben der Datenschutzerklärung waren einige technische Prozesse zur Gewährleistung von Betroffenenrechten („Auskunft auf Knopfdruck") in das Fachverfahren zu implementieren und Verzeichnisse für die Verarbeitungstätigkeit[150] zu erstellen. Für die neu einzusetzenden Module musste das neue Instrument der Datenschutz-Folgenabschätzung[151] angewendet werden.

In diesem Jahr wurde das neue Modul Jugendberufshilfe für die in den Jugendberufsagenturen tätigen Fachkräfte der bezirklichen Jugendämter in den Echtbetrieb übernommen. Die Zugriffsmöglichkeiten der Jugendberufshilfe innerhalb des Fachverfahrens auf die Jugendhilfedaten in den übrigen Organisationseinheiten des Jugendamtes haben wir mit der Abteilung Jugend der Senatsverwaltung

148 JB 2016, 5.4; JB 2017, 2.3
149 Art. 13 ff. DS-GVO
150 Art. 30 DS-GVO
151 Art. 35 DS-GVO

für Bildung, Jugend und Familie abgestimmt. Im Fachverfahren wird gewährleistet, dass ein Zugriff lediglich auf die erforderlichen Daten erfolgen kann.

Schließlich haben wir mit der für Jugend zuständigen Abteilung der Senatsverwaltung für Bildung, Jugend und Familie eine klarstellende Vorschrift im Ausführungsgesetz zum Kinder- und Jugendhilfegesetz (AG KJHG) mit den datenschutzrechtlichen Vorgaben zur Datenverarbeitung abgestimmt, die die Senatsverwaltung an die für die Anpassung des Landesrechts an die DS-GVO federführende Senatsverwaltung für Inneres und Sport weitergeleitet hat.[152]

Auch in diesem Jahr erfolgten die Abstimmungen mit der Jugendverwaltung unkompliziert und konstruktiv. Die Anforderungen der DS-GVO wurden – anders als in den meisten anderen Bereichen der Verwaltung – rechtzeitig zum 25. Mai 2018 umgesetzt. Es ist uns wichtig, die Umsetzung der durch die DS-GVO normierten Vorgaben für einen Datenschutz durch Technikgestaltung beim ISBJ-Fachverfahren auch in Zukunft beratend zu begleiten als positives Beispiel für die Umsetzung datenschutzrechtlicher Anforderungen.

5.4 Datenschutz in Kitas – Wie gut werden die Daten unserer Jüngsten geschützt?

Dass Kindertageseinrichtungen mit den Daten der ihnen anvertrauten Kinder datenschutzgerecht umgehen, liegt den Eltern besonders am Herzen. Doch auch in den Kindertageseinrichtungen selbst besteht vielfach Unsicherheit, wie mit den Daten der Kinder und ihrer Familien umzugehen ist.

Gerade im Zusammenhang mit dem Wirksamwerden der DS-GVO hat die Unsicherheit bei den Einrichtungen zum datenschutzgerechten Umgang mit personenbezogenen Daten noch einmal zugenommen. Der Umgang mit Fotos, die Gestaltung von Einwilligungserklärungen, aber auch der Einsatz neuer Technologien wie z. B. Apps, mit denen Bring- und Abholzeiten der Kinder elektronisch erfasst oder den Eltern Informationen aus dem Kitaalltag zugänglich gemacht werden

152 Zur Anpassung des Landesrechts siehe JB 2018, 1.8

können, führt immer wieder zu datenschutzrechtlichen Fragen bei den Eltern, aber auch bei den Einrichtungen. Sowohl die Beratungsersuchen als auch die Beschwerden in diesem Bereich beziehen sich oftmals genau auf diese Themen.

Im Rahmen von Beschwerden ist es unser Anliegen, für die Zukunft datenschutzgerechte Verfahrensweisen zu erreichen. Allerdings ist es uns im Rahmen unserer Kapazitäten z. B. vielfach nicht möglich, Einwilligungserklärungen abstrakt daraufhin zu überprüfen, ob sie im Einklang mit den datenschutzrechtlichen Vorschriften stehen. Am häufigsten erreichen uns Fragen zum Umgang mit Foto- und Videoaufnahmen von Kindern im Kitaalltag. Der Handlungsleitfaden „Datenschutz bei Bild-, Video- und Tonaufnahmen – Was ist in der Kindertageseinrichtung zu beachten?“[153], den wir zu Beginn des Jahres gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Familie herausgegeben haben[154], hat in der Praxis große Resonanz gefunden, auch über das Land Berlin hinaus. Unser Anliegen war es, den pädagogischen Fachkräften mit dem Handlungsleitfaden in praxisgerechter Weise einen Überblick über die komplexe Rechtslage zu geben. Wir haben im Interesse der Verständlichkeit bewusst weitgehend darauf verzichtet, konkrete Vorschriften und Gesetze zu zitieren. Da die strengen Anforderungen an die Wirksamkeit von Einwilligungserklärungen auch vor Wirksamwerden der DS-GVO im deutschen Datenschutzrecht verankert waren, entspricht der Text des Handlungsleitfadens inhaltlich auch den Anforderungen der DS-GVO. Da wir jedoch zunehmend um Erläuterung gebeten werden, inwieweit die Broschüre die Rechtslage auch nach dem Wirksamwerden der DS-GVO abdeckt, haben wir uns entschieden, ein ergänzendes Informationsblatt zu erstellen. In diesem werden die einschlägigen Artikel der DS-GVO konkret benannt. Mit der nächsten Neuauflage werden wir die entsprechenden Vorschriften dann in den Text integrieren.

Die Rückmeldungen auf den Handlungsleitfaden zeigen, dass er den Einrichtungen eine Hilfestellung für mehr Rechtssicherheit im Umgang mit Datenschutzfragen im Kitaalltag bietet. Wir planen, das Informationsangebot für Kindertageseinrichtungen in Zukunft noch zu erweitern.

153 Der Handlungsleitfaden ist abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/informationsmaterialien/2018-BlnBDI_Flyer_Datenschutz_Inhalt_Web.pdf.

154 JB 2014, 4.1; JB 2015, 6.4; JB 2017, 6.5

5.5 Datenschutz und Medienkompetenz – Kinderwebseite www.data-kids.de online

Aus der Praxis

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat es sich zum Ziel gesetzt, bei Kindern so früh wie möglich Bewusstsein für den Schutz ihrer Daten zu wecken. Seit 2016 arbeiten wir deswegen an altersgerechten Materialien, um Kinder bereits im Grundschulalter darüber aufzuklären, wie sie von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen können und wie sie sich insbesondere im Netz verhalten sollten.[155]

Entwicklungspsychologisch sind Kinder etwa ab sieben Jahren in der Lage, auch längerfristige Folgen abzuschätzen. Es kann davon ausgegangen werden, dass Kinder ab der 3. Klasse ein Bewusstsein für Datenschutzfragen entwickeln können. Je früher wir sie dabei begleiten, desto medienkompetenter und damit mündiger und verantwortungsbewusster können sie am gesellschaftlichen Leben teilhaben, von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen und Kompetenzen für die digitale Welt ausbilden.

Mit unserer Kinderwebseite www.data-kids.de starteten wir im Frühjahr 2018 ein Angebot, auf dem Kinder die wichtigsten Begriffe rund um den Datenschutz kennenlernen können. Eine Roboterfamilie begleitet sie dabei durch die Datenschutzwelt und erklärt, was es mit dem Recht auf informationelle Selbstbestimmung auf sich hat. In ersten Materialien für Lehrkräfte erklären wir, was Cookies und das Recht am eigenen Bild sind und wie die Kinder ihre Daten selbst schützen können.

Damit die Kinder sich mit den Robotern identifizieren können, riefen wir zu einem Wettbewerb auf, in dem sich Grundschulkinder Namen für die Roboterkinder überlegen sollten. Gewonnen hat die damalige Klasse 3b der Grundschule am Tegelschen Ort.[156]

Nachdem wir die Grundstrukturen und wichtigsten Inhalte der Webseite erstellt und die Figuren entwickelt hatten, stellten wir in der zweiten Jahreshälfte unsere

155 JB 2017, 6.6
156 Siehe auch 14.5

Webseite, auch mithilfe von Rückmeldungen aus Grundschulen, auf den Prüfstand.

Im kommenden Jahr werden wir das Kinderangebot weiter optimieren, um die Zielgruppe noch besser zu erreichen. Konkret werden wir die vorhandenen Materialien auf kindgerechte Sprache prüfen und, wo notwendig, anpassen. Die Elemente der Webseite werden wir interaktiv und spielerisch, in jedem Fall aber grafisch noch ansprechender gestalten.

Unser Ziel ist es, die Webseite zu einem umfassenden Angebot zu erweitern, mit dem Lehrkräfte, Eltern und Kinder ihre Datenschutzkompetenz effektiv stärken können.

5.6 Elterngeld Digital – Ein innovatives Projekt?

Bereits 2017 hat uns die Senatsverwaltung für Bildung, Jugend und Familie in das vom Bundesministerium für Familie, Senioren, Frauen und Jugend initiierte Projekt „Elterngeld Digital“ einbezogen. Antragstellenden soll es ermöglicht werden, Anträge auf Auszahlung von Elterngeld über ein vom Bundesministerium bereitgestelltes Internetportal digital einzureichen.

Ziel des Projektes „Elterngeld Digital“ soll die digitale Abwicklung der Gewährung von Elterngeld an die Leistungsbeziehenden sein. Da das Bundeselterngeld zwar eine Leistung des Bundes ist, die Abwicklung jedoch durch die Elterngeldstellen der Länder erfolgt, sind diese für die Entscheidung über die Anträge zuständig. Die Senatsverwaltung für Bildung, Jugend und Familie hat sich bereit erklärt, an dem Pilotprojekt des Bundes teilzunehmen. Hinsichtlich der Frage der Rechtmäßigkeit der Verarbeitung von Sozialdaten durch das Land Berlin sind auch wir an dem Projekt beteiligt.

Während auf Berliner Seite alles gut vorbereitet war, lief das Projekt vonseiten des Bundes eher schleppend an. Mit einer einjährigen Verzögerung wurde das Projekt im Herbst 2018 nun mit dem sog. Antragsassistenten gestartet. Eltern können ihre Anträge zwar mit Hilfe des Assistenten Online ausfüllen, müssen ihn jedoch weiterhin per Post an ihre zuständige Elterngeldstelle schicken. Eine vollstän-

dige Digitalisierung der Antragstellung scheitert derzeit noch daran, dass eine Rechtsgrundlage im Bundeselterngeld- und Elternzeitgesetz (BEEG) fehlt.[157] Das Bundesministerium für Familie ist datenschutzrechtlich Verantwortlicher für die im Rahmen der Antragstellung im Internetportal anfallenden Sozialdaten und benötigt insoweit eine Rechtsgrundlage für die Verarbeitung. Da die Erhebung der Daten mit dem Antragsassistenten vonseiten des Bundes erfolgt, ist dieser auch für die Authentifizierung der Antragstellenden und die Einholung der notwendigen Einwilligungserklärungen verantwortlich. Wir mussten daher der Senatsverwaltung letztlich mitteilen, dass wir das vorgesehene Verfahren mangels Zuständigkeit leider nicht datenschutzrechtlich bewerten können.

Die flächendeckende Einführung digitaler Angebote ist durchaus wünschenswert. Allerdings halten wir es für notwendig, die datenschutzrechtlichen und technischen Anforderungen der DS-GVO schon bei der Entwicklung und der Implementierung von Verfahren zu berücksichtigen, um Leistungen dann auch von vornherein vollständig digital anbieten zu können.

5.7 Bitte lächeln! Video- und Audioaufzeichnungen im Unterricht zu Forschungszwecken

Aus der Praxis

Der Schulunterricht ist ein beliebtes Forschungsfeld. In der Regel werden die Schülerinnen und Schüler sowie die Lehrkräfte in diesem Zusammenhang gebeten, Fragebögen der Forscherinnen und Forscher auszufüllen. Vermehrt möchten Wissenschaftlerinnen und Wissenschaftler aber auch zusätzlich Audio- und Videoaufnahmen von einzelnen Unterrichtsstunden oder -einheiten anfertigen, um auf deren Grundlage weitere Erkenntnisse für die Bildungsforschung zu gewinnen. Dies wirft datenschutzrechtliche Probleme auf, die von den Verantwortlichen bereits bei der Konzeption der Studie bedacht und einer Lösung zugeführt werden sollten.

157 Eine Rechtsgrundlage im BEEG soll mit dem 2. Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU – geschaffen werden.

Die Unterschiede zu klassischen Erhebungsformen, wie derjenigen mittels Fragebogen, liegen auf der Hand. Die mit klassischen Mitteln durchgeführten Erhebungen erfolgen regelmäßig pseudonymisiert. Dies bedeutet bei Fragebögen, dass diese nicht mit den Namen der teilnehmenden Personen versehen sind, sondern jeweils mit einer Identifikationsnummer bzw. einem Code. Beim Filmen des Unterrichts ist ähnlich vorzugehen. Bei der Aufzeichnung einer Unterrichtsstunde sollte den Forschenden z. B. ein Sitzplan vorliegen, der anstelle von Namen der jeweiligen Schülerinnen und Schüler ebenfalls Codes enthält. Auf diese Weise können bei kombinierten Erhebungen z. B. auch die Aufzeichnungen mit den Antworten im Fragebogen verknüpft werden. So kann sichergestellt werden, dass bei einer einige Zeit später stattfindenden Folgebefragung die Antworten aus beiden Befragungsdurchgängen derselben Person zugeordnet und verglichen werden können, ohne dass die Forscherinnen und Forscher für diesen Zweck auch den Namen der oder des Befragten kennen müssen.

Um personenbezogene Daten handelt es sich selbstverständlich auch bei diesen mit Identifikationsnummern bzw. Codes versehenen Datensätzen. Denn zumeist verbleibt eine Liste in der Schule, aus der sich ergibt, welche Befragten sich hinter welchen Nummern verbergen. Anhand dieser Liste kann nach wie vor die Zuordnung der Pseudonyme und damit auch der Antworten zu einer konkreten Person vorgenommen werden. Diese Liste muss daher gelöscht werden, sobald die Aufbewahrung für die Durchführung der Studie nicht mehr erforderlich ist.

Doch auch mit der Löschung dieser Zuordnungsliste ist es nicht immer getan, da unter Umständen auch konkrete Antwortkombinationen durchaus zu einer Identifizierbarkeit der teilnehmenden Person führen können.

Bei Video- und Audioaufnahmen ist eine Identifizierbarkeit immer gegeben. So sind auf diesen Aufnahmen naturgemäß die Gesichter und Stimmen der Schülerinnen und Schüler sowie die der Lehrkräfte zu erkennen, sodass diese Daten unabhängig von der Zuordnung über eine Nummer stets personenbezogen bleiben. Daraus ergeben sich datenschutzrechtliche Anforderungen, die von Beginn an zu berücksichtigen sind:

Die datenschutzrechtliche Grundlage für die Verarbeitung der in Rede stehenden Daten ist regelmäßig die Einwilligung der betroffenen Personen bzw. ihrer Perso-

nensorgeberechtigten. Damit geht einher, dass diese Personen sich auch im Klaren darüber sein müssen, worin sie tatsächlich einwilligen. Die Zwecke der Datenverarbeitung müssen ausreichend klar sein und verständlich dargestellt werden. Dies gilt im besonderen Maße für Informationen, die sich an Kinder richten.[158] Im Zusammenhang mit Videoaufnahmen von anonymisierten Daten zu sprechen, verbietet sich aus den genannten Gründen generell. Zudem steht den betroffenen Personen das Recht zu, ihre einmal erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Die Verantwortlichen müssen also einen Weg finden, sicherzustellen, dass die Aufnahmen im Falle eines Widerrufs tatsächlich für zukünftige Verwendungen gelöscht oder jedenfalls in einer Weise unkenntlich gemacht werden, die eine Identifizierung der betreffenden Person ausschließt.

Ebenso muss von den Verantwortlichen frühzeitig problematisiert werden, wie mit dem Inhalt der Aufzeichnungen umzugehen ist. Denn eine Identifizierung ist nicht allein anhand der Stimme oder des Gesichts möglich. Auch die aufgezeichneten Äußerungen selbst bzw. die Interaktionen im Klassenverband geben mitunter Aufschluss über die Identität der handelnden Personen. So dürfte es gerade im Schulunterricht regelmäßig vorkommen, dass die Schülerinnen und Schüler von der Lehrkraft mit Namen aufgerufen werden oder die Schülerinnen und Schüler umgekehrt die Lehrkraft mit deren Namen ansprechen.

Nicht zuletzt ist sicherzustellen, dass Schülerinnen und Schüler, für die keine Einwilligung vorliegt, nicht ebenfalls von der Aufzeichnung erfasst werden. Sie lediglich außerhalb des Sichtfeldes der Kamera zu positionieren, reicht hier in der Regel nicht aus. Denn trotz der Vermeidung von Bildaufnahmen werden bei diesem Vorgehen dennoch deren Stimmen aufgezeichnet, wenn die Betroffenen sich am Unterricht beteiligen.

Der Einsatz von Video- und Audioaufnahmen zu Forschungszwecken wirft neue Problemfelder auf, die bereits bei der Konzeption von Studien zu berücksichtigen sind.

158 Art. 12 Abs. 1 Satz 1 DS-GVO

6 Gesundheit und Pflege

6.1 Urteil zum Qualitätssicherungsverfahren der Kassenärztlichen Vereinigung Berlin

Nachdem wir vor mittlerweile acht Jahren das damalige Qualitätssicherungsverfahren der Kassenärztlichen Vereinigung (KV) im Hinblick auf die Erhebung personenidentifizierender Patientendaten beanstandet haben,[159] ist nunmehr in einem parallel dazu geführten Sozialgerichtsverfahren zwischen dem beschwerdeführenden Arzt und der KV am 9. Mai 2018 das Urteil des Landessozialgerichts (LSG) Berlin-Brandenburg in Potsdam ergangen.[160] In dem zugrunde liegenden Fall hatte der betreffende Arzt die von der KV geforderte Übermittlung von identifizierenden Patientendaten abgelehnt und sich mit einer entsprechenden Beschwerde an uns gewandt.

Das LSG Potsdam hat in zweiter Instanz festgestellt, dass die Qualitätsprüfungs-Richtlinie des Gemeinsamen Bundesausschusses, die eine Pseudonymisierung der Patientendaten nicht ausdrücklich vorsieht, gegen den zu diesem Zeitpunkt (2011) geltenden § 299 Abs. 1 Satz 1 Nr. 1 und 2, Abs. 2 Sozialgesetzbuch – Fünftes Buch – Gesetzliche Krankenversicherung (SGB V) verstoßen hat. Die Regelung des SGB V schrieb in der alten Fassung die Pseudonymisierung der Patientendaten zum Zwecke der Qualitätssicherung ausdrücklich vor. Damit wurde unsere gegenüber der KV Berlin vertretene Rechtsauffassung bestätigt, dass lediglich pseudonymisierte Patientendaten an die KV übermittelt werden dürfen.

Das Urteil des Landessozialgerichts ist allerdings noch nicht rechtskräftig, da sowohl der Gemeinsame Bundesausschuss als auch die KV Berlin gegen das Urteil eine Nichtzulassungsbeschwerde beim Bundessozialgericht eingelegt haben. Da auch mit der neuen Regelung des § 299 SGB V eine Qualitätssicherung regelmäßig nur unter Pseudonymisierung der Patientendaten erfolgen darf, hat die KV aufgrund des Urteils entschieden, die Qualitätssicherung unter Erhebung von identi-

159 JB 2011, 7.2.8

160 LSG Berlin-Brandenburg, Urteil vom 9.5.2018 - L 7 KA 52/14

fizierenden Daten bis zur Klärung durch das Bundessozialgericht vorerst auszusetzen.

Wir sehen uns durch das Urteil in unserer Rechtsauffassung bestätigt, dass bei der Qualitätssicherung durch die KV Berlin Patientendaten nur in pseudonymisierter Form erhoben werden dürfen. Die Qualitätssicherung durch die KV ist auch unter der Maßgabe der Pseudonymisierung von Patientendaten praktikabel und unter vertretbarem Aufwand durchführbar.

6.2 Prostituiertenschutzgesetz – Datenschutzkonforme Umsetzung im Land Berlin?

Mit dem Prostituiertenschutzgesetz hat der Bundesgesetzgeber rechtliche Rahmenbedingungen für die legale Prostitution eingeführt. Geregelt wird unter anderem die Pflicht zur Anmeldung und zur gesundheitlichen Beratung der Prostituierten. Bereits im Jahr 2015 haben wir zu dem damaligen Entwurf des Prostituiertenschutzgesetzes Stellung genommen.[161] Das Gesetz ist zum 1. Juli 2017 in Kraft getreten und musste in allen Bundesländern, so auch in Berlin, umgesetzt werden. Nach der Verordnung zur Bestimmung von Zuständigkeiten zur Umsetzung des Prostituiertenschutzgesetzes vom 12. Dezember 2017 ist das Bezirksamt Tempelhof-Schöneberg von Berlin für die Anmeldung sowie die gesundheitliche Beratung nach dem Prostituiertenschutzgesetz für das Land Berlin zuständig.

Sowohl bei der Anmeldung als auch bei der Gesundheitsberatung nach dem Prostituiertenschutzgesetz werden personenbezogene Daten der Prostituierten, dabei insbesondere Daten über das Sexualleben und Gesundheitsdaten, verarbeitet. Aufgrund ihrer Sensitivität besteht für diese besonderen Kategorien personenbezogener Daten ein gesteigerter Schutzbedarf, der insbesondere vor dem Hintergrund des Wirksamwerdens der Datenschutz-Grundverordnung zum 25. Mai 2018 in der Verfahrensumsetzung zu berücksichtigen ist.

161 JB 2015, 7.1

Daher haben wir die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung um nähere Informationen zum Anmeldeverfahren sowie zur Gesundheitsberatung gebeten.

Die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung hat uns u. a. geantwortet, dass das Prostituiertenschutzgesetz datenschutzrechtliche Belange bereits berücksichtige. Auch europäische Vorgaben zum Datenschutz würden beachtet, sodass die Senatsverwaltung nicht beabsichtige, weitere inhaltliche Regelungen zu schaffen. Man erachte die bundesrechtlichen Regelungen insoweit für ausreichend. Darüber hinaus teilte uns die Senatsverwaltung mit, dass sie nur eine koordinierende Rolle habe und daher keine näheren Bestimmungen zur Ausgestaltung des Verfahrenstreffen könne. Wir mussten diesem Schreiben entnehmen, dass die Senatsverwaltung nicht beabsichtigt, die von uns geäußerten Bedenken, insbesondere hinsichtlich der Umsetzung der Vorgaben der DS-GVO im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten, aufzugreifen. Problematisch ist dies besonders vor dem Hintergrund, dass der Hinweis der Senatsverwaltung, europäische Vorgaben seien berücksichtigt worden, nicht richtig ist. Die Gesetzesbegründung bezieht sich auf die Richtlinie 95/46/EG, nicht aber auf die DS-GVO. Insbesondere wurden die Vorgaben zur Verarbeitung von Gesundheitsdaten, die aufgrund ihrer besonderen Schutzbedürftigkeit in der DS-GVO ausdrücklich geregelt sind, nicht berücksichtigt. Angesichts der besonderen Sensitivität der verarbeiteten Daten sehen wir es jedoch als äußerst wichtig an, hierauf auch bei der Einführung der Verfahrensprozesse für die Anmeldung und die Gesundheitsberatung von vorneherein zu achten.

Wir werden die Umsetzung des Prostituiertenschutzgesetzes im Land Berlin weiter im Blick haben. Wir haben das Bezirksamt Tempelhof-Schöneberg von Berlin kontaktiert und ein Angebot zur Beratung im Hinblick auf die datenschutzkonforme Umsetzung unterbreitet.

6.3 Problematische Einführung einer elektronischen Gesundheitsakte

Aufgrund von Beschwerden setzten wir uns mit dem Angebot einer elektronischen Gesundheitsakte auseinander, die Patientinnen und Patienten zur Verwaltung von medizinischen Unterlagen einsetzen können.

Der Gesetzgeber erlaubt den Krankenkassen, elektronische Gesundheitsakten zu fördern. Diese sollten dazu dienen, dass Versicherte selbstbestimmt Unterlagen zu ihrer Gesundheit verwahren und in die weitere Behandlung einbringen können. Die beteiligten Krankenkassen und Krankenversicherungen möchten diese Akten ebenfalls gern für die gezielte Ansprache ihrer Versicherten nutzen.

Das Angebot der Gesundheitsakte basiert auf Einwilligungen der Nutzerinnen und Nutzer. Dabei muss die Einwilligung für die verschiedenen Zwecke und Funktionalitäten jeweils separat und ausdrücklich erteilt werden. Das geprüfte Vorhaben ist im Laufe des Jahres dynamisch gewachsen. Dabei sind ständig neue Funktionalitäten hinzugekommen. Allerdings wurden die Nutzerinnen und Nutzer nicht hinreichend informiert und die nun notwendigen neuen Einwilligungen nicht eingeholt. Auf unsere Intervention hin wurde dieser Mangel nachträglich behoben.

Der Anbieter der geprüften Gesundheitsakte betreibt die Gesundheitsakte bei einem großen Cloud-Dienstleister. Die Versicherten erhalten eine App für ihr Mobiltelefon und steuern damit die Akte. Möchten Patienten über die Gesundheitsakte eine Unterlage von einer behandelnden Ärztin oder einem behandelnden Arzt erhalten, dann teilen sie das über die App mit und der Anbieter wendet sich per E-Mail an die betreffende Ärztin oder an den betreffenden Arzt. Der Ärztin oder dem Arzt wird die Möglichkeit gegeben, das entsprechende Dokument über ihren oder seinen Webbrowser in die Akte hochzuladen. In diesem Prozess werden die Unterlagen verschlüsselt.

Bevor Ärzte dies rechtmäßig tun können, müssen sie sich davon überzeugen, dass die Patienten diese Übertragung auch wirklich wünschen. Dafür unterschreiben die Patienten innerhalb der App eine Schweigepflichtentbindungserklärung auf dem Bildschirm ihres Mobiltelefons. Für die Ärzte ist es jedoch schwierig fest-

zustellen, ob dieses Dokument tatsächlich von der richtigen Person kommt. Der Anbieter prüft die Identität der Patienten, allerdings nicht auf eine Weise, die der Sensibilität der später verarbeiteten Gesundheitsdaten Rechnung trägt. Somit sollten Ärzte auf anderem Wege den Willen der Patienten feststellen, z. B. bei Anwesenheit der Patienten in der Praxis.

Selbstverständlich muss der Übergabeprozess der Daten sicher ausgestaltet werden. Ein unabhängiges Forscherteam hatte im konkret vorliegenden Produkt in diesem Prozess Sicherheitslücken gefunden, welche der Anbieter später behob. Das Verfahren führt allerdings zu einer neuen Schwachstelle in den Praxen der übermittelnden Ärztinnen und Ärzte: Mit dem Internet verbundene Rechner von Ärzten können Angriffsobjekte werden. Nach den von uns unterstützten Empfehlungen der Bundesärztekammer sollten Ärzte unverschlüsselte medizinische Unterlagen nicht auf Rechner überspielen, die freien Zugang zum Internet haben. Derzeit lassen sich der Gesundheitsakte jedoch nur von einem solchen Rechner aus Dokumente hinzufügen.

Schon die Tatsache, dass jemand von einer bestimmten Ärztin oder einem bestimmten Arzt behandelt wird, ist geheim zu halten, da sich daraus Rückschlüsse auf die Art einer Erkrankung ziehen lassen. Die Abfrage der Unterlagen bei den medizinischen Leistungserbringern erfolgte zum Prüfungszeitpunkt jedoch unverschlüsselt. Wir haben den Anbieter aufgefordert, dies zu ändern.

Letztendlich muss auch die Datenverarbeitung des Anbieters der Gesundheitsakte selbst hohen Sicherheitsanforderungen genügen. Das bereits genannte Forscherteam hatte weitere Lücken in der Sicherheit des Angebots gefunden. Auch im Zuge unserer Prüfung stellten wir Schwachstellen fest. Eine Datenschutz-Folgenabschätzung war zudem verspätet und unvollständig vorgenommen worden.

Wir werden im Jahr 2019 auf das Unternehmen einwirken, dass etablierte Standards für die Sicherheit derartiger Dienste durchgängig eingehalten werden und das gleiche Sicherheitsniveau erreicht wird, wie es das Gesetz von den elektronischen Patientenakten erfordert.

Elektronische Gesundheitsakten bieten Patientinnen und Patienten die Möglichkeit, ihre Gesundheitsdaten an zentraler Stelle zu speichern und zu verwalten. Die Vorteile, die sich hieraus ergeben können, dürfen jedoch nicht mit einem schwächeren Schutz der Daten bezahlt werden. Die datenschutzrechtlichen Anforderungen müssen daher bereits bei der Konzeptionierung entsprechender Angebote beachtet und umgesetzt werden.

6.4 Babylotse Plus: Ausweitung auf alle Berliner Geburtskliniken

Im Rahmen des Projekts „Babylotse" stehen für werdende Mütter Personen – sogenannte Babylotsen – zur Verfügung, die bei Bedarf Unterstützung bei schwierigen familiären Situationen leisten und die Familie im Umgang mit der neuen Situation nach der Geburt des Kindes begleiten.

Nachdem bereits im Jahr 2014 das Projekt „Babylotse" in der Charité im Rahmen eines Forschungsprojektes umgesetzt und von uns datenschutzrechtlich begleitet wurde, ist nunmehr beschlossen worden, dieses wichtige Projekt in allen Berliner Geburtskliniken einzuführen. Um die Umsetzung auch im Hinblick auf die datenschutzrechtlichen Vorgaben zu begleiten, haben wir frühzeitig Kontakt mit der zuständigen Senatsverwaltung für Gesundheit, Pflege und Gleichstellung aufgenommen. Wir haben im November 2018 die datenschutzrechtlichen Anforderungen im Begleitgremium vorgestellt und haben zugesagt, das Projekt auch im Jahr 2019 weiter zu begleiten.

Um für das Projekt „Babylotse" das Vertrauen der werdenden Mütter zu gewinnen und erfolgreich durchführen zu können, ist es neben den konkreten Hilfsangeboten wichtig, die erforderliche Vertraulichkeit zu gewährleisten und sicherzustellen, dass die datenschutzrechtlichen Vorgaben im Projekt umgesetzt werden.

6.5 Charité: Neues Recht – Alte Probleme

Auch in diesem Jahr haben wir die Behebung der Mängel begleitet, die wir vor drei Jahren bei der Charité festgestellt haben, und auf eine zügige Umsetzung der zwingend erforderlichen Maßnahmen gedrängt.[162] Eingeschaltet hat sich auch die Senatskanzlei, Abteilung Wissenschaft und Forschung, als zuständige Fachaufsicht über die Charité.

Vor Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) zum 25. Mai 2018 war die Charité verpflichtet, jedes Verfahren zur Verarbeitung von Patienten- oder Probandendaten einer Vorabkontrolle auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu unterziehen. Dieser Verpflichtung ist die Charité in der Vergangenheit nicht nachgekommen.

Diese Forderung besteht mit der DS-GVO nunmehr in Form der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung für alle neu eingeführten Verfahren mit hohen Risiken und für die Verfahren fort, für die zuvor trotz Verpflichtung keine regelgerechte Vorabkontrolle durchgeführt wurde. Wir haben im Oktober 2018 geprüft, ob die Defizite aufgearbeitet wurden. Das Ergebnis war ernüchternd:

Auch fünf Monate nach Wirksamwerden der DS-GVO hatte die Charité zu keinem Verfahren eine Datenschutz-Folgenabschätzung abgeschlossen. Lediglich bei zwei Verfahren haben die Arbeiten an der Durchführung einer Folgenabschätzung begonnen. Dabei schätzt die Charité selbst, dass sie für mehr als einhundert Verfahren solche Abschätzungen vornehmen muss.

Positiv konnten wir vermerken, dass die Charité zum Oktober 2018 wenigstens eine vollständige Übersicht der betriebenen Verfahren erstellt hat. Damit ist erstmals eine gezielte Kontrolle einzelner Vorhaben möglich. Auch der Charité hilft dieses Verzeichnis, die eigenen Datenverarbeitungen zu steuern und zu überwachen.

162 JB 2015, 8.4.1

Dennoch ist dies nur ein erster und vergleichsweise kleiner Schritt: Jedes Verfahren mit hohen Risiken ist systematisch zu beschreiben. Die Risiken müssen dabei konkret benannt und bewertet werden. Danach ist zu bestimmen, wie sie hinreichend gemindert werden.

Der Charité fehlt es bereits an der systematischen Beschreibung der einzelnen Verfahren. Es gibt einen allgemeinen Risikokatalog, aber keine Konkretisierung für den jeweiligen Verarbeitungsvorgang. Ebenso gibt es einen allgemein gehaltenen und zudem unvollständigen Katalog von zentral anzuwendenden Maßnahmen. Gebraucht werden jedoch spezifische Vorgaben sowohl für den zentralen IT-Betrieb als auch für die Verarbeitungen in dezentraler Verantwortung. Ihre Zusammenfassung sollen diese Vorgaben und Maßnahmen dann in den gesetzlich vorgeschriebenen Datenschutzkonzepten finden. Deren Fehlen hat vor drei Jahren zur Beanstandung seitens unserer Behörde geführt. Nach wie vor liegt für kein Verfahren ein solches Konzept vor.

Bei einigen konkreten technischen Sicherheitsmaßnahmen sind dagegen gewisse Fortschritte zu verzeichnen, auch wenn sie noch nicht vollständig umgesetzt sind. Dazu beigetragen hat der Informationssicherheitsbeauftragte, der Mitte des Jahres 2018 seine Arbeit in der Charité aufgenommen hat. Leider ist der Charité eine adäquate personelle Ausstattung des Datenschutzmanagements bis zum Ende des Jahres 2018 nicht gelungen.

Vor der Charité steht nach wie vor die Aufgabe, für ihre Verfahren die Risiken für die betroffenen Personen zu bewerten, die notwendigen technisch-organisatorischen Maßnahmen mit einer Risikoanalyse zu bestimmen, diese in Sicherheits- bzw. Datenschutzkonzepten zu systematisieren und schlussendlich die festgelegten Maßnahmen durchgehend umzusetzen.

6.6 Online-Dienstleister: Umgang mit personenbezogenen Daten im Medizin-Sektor

Wie in vielen Branchen zu beobachten, verlagern sich die Angebote im Bereich der Vermittlung von medizinischen Dienstleistungen zunehmend ins Internet. Durch eine Beschwerde sind wir auf einen in Berlin ansässigen Dienstleister aus diesem Bereich aufmerksam geworden, der ein breites Spektrum medizinischer Klinikdienstleistungen aus aller Welt vermittelt.

Wer Gesundheitsdaten verarbeiten will, ohne selbst medizinische Leistungen zu erbringen, benötigt regelmäßig die ausdrückliche Einwilligung der betroffenen Personen. Und nur wer über die beabsichtigte Verarbeitung, ihre Zwecke, Umstände und Risiken informiert ist, kann wirksam einwilligen. Verschiedentlich scheuen Anbieter von Online-Diensten den mit der Information und Einholung von Einwilligungen verbundenen Aufwand. Zumal sie Gefahr laufen, dass es sich eine gut informierte Person noch einmal überlegen könnte, ihr Angebot in Anspruch zu nehmen.

So handelte auch der von uns geprüfte Anbieter. Er forderte die zukünftigen Kundinnen und Kunden auf, schon einmal vorweg weitgehende Informationen über ihre Gesundheit bereitzustellen, bevor er sie mit der Information über die vorgesehene Datenverarbeitung und einem Eingabefeld für die Erklärung der Einwilligung konfrontierte. Für den Erstkontakt musste ein Erfassungsformular ausgefüllt werden, das sich in zwei Seiten aufteilte. Auf der ersten Seite sollten die zukünftigen Kunden ihr jeweiliges Anliegen beschreiben und nach Möglichkeit Patientenakte, Röntgenaufnahmen oder Fotos bereitstellen. Zu diesem Zeitpunkt klärte der Anbieter noch nicht über die Verarbeitung der sensitiven Daten auf, obwohl die erfassten Daten inklusive der für das Hochladen gewählten Dateien bereits beim Übergang zur zweiten Seite an das Unternehmen übertragen wurden. Erst auf dieser zweiten Seite wurde dann nach Hinweis auf eine ausführliche Datenschutzerklärung um eine Einwilligung gebeten.

Wir wandten uns an das Unternehmen und bemängelten die rechtswidrige Erhebung der Daten. Diese wurde zunächst durch das Unternehmen bestritten. Erst angesichts des unwiderlegbaren Nachweises räumte das Unternehmen den Feh-

ler ein und sagte zu, die Datenverarbeitung umzugestalten. Eine Überprüfung steht noch aus.

Bei der Online-Erfassung von Gesundheitsdaten darf eine Verarbeitung erst erfolgen, nachdem der vorgesehene Umgang mit den Daten erläutert wurde und die betroffene Person ihre ausdrückliche Einwilligung gegeben hat.

6.7 Ein Pflegedienst auf Wolke International

Auf einen Hinweis hin haben wir ein Pflegeunternehmen geprüft, das einen Großteil der für die Pflege notwendigen medizinischen Angaben über die zu pflegenden Personen bei internationalen Cloud-Unternehmen speicherte, deren Beschäftigte keiner gesetzlichen Schweigepflicht unterliegen.

Pflegedienstleister unterliegen der gleichen Schweigepflicht wie Ärztinnen und Ärzte. Wer sich ihnen anvertraut, soll sicher sein, dass nichts über ihre Gesundheit nach außen gelangt. Sie können wie andere Geheimnisträger Dienstleister in Anspruch nehmen. Dann muss jedoch gewährleistet sein, dass auch diese einer gleichartigen Geheimhaltungspflicht unterfallen. Für deutsche Dienstleister hat der Gesetzgeber diese Geheimhaltungspflicht geregelt.[163] Bei internationalen Dienstleistern hängt dies davon ab, inwieweit das jeweilige Land entsprechende Geheimhaltungsvorschriften erlassen hat.

Wir haben den betreffenden Pflegedienstleister aufgefordert sicherzustellen, dass Daten nur von Dienstleistern verarbeitet werden, für die diese Voraussetzung erfüllt ist.

Angehörige von Gesundheitsberufen müssen darauf achten, dass die von ihnen verarbeiteten Daten über ihre Klientinnen und Klienten auch bei den in Anspruch genommenen Dienstleistern datenschutzkonform verarbeitet werden.

163 § 203 Abs. 4 Satz 1 StGB; siehe auch JB 2017, 7.6

6.8 Klinisches Krebsregister: Überlange Aufbewahrung von Meldebögen

Zwei Jahre nach Eröffnung prüften wir von Amts wegen die Übereinstimmung der Datenverarbeitung des gemeinsamen klinischen Krebsregisters der Länder Brandenburg und Berlin mit den gesetzlichen Regelungen.

Das klinische Krebsregister erfasst flächendeckend Daten über alle an Krebs erkrankten Personen in den Ländern Brandenburg und Berlin, darunter die Diagnosen und Angaben über die Behandlung. Die im Register verarbeiteten Daten sind damit höchst sensitiv. Sie werden von den behandelnden Krankenhäusern und niedergelassenen Ärztinnen und Ärzten gemeldet. Dazu sind diese rechtlich verpflichtet. Patientinnen und Patienten haben ein beschränktes Widerspruchsrecht.

Kurz nach der Eröffnung im Jahr 2016 hatten wir bereits mit unseren Brandenburger Kolleginnen und Kollegen die Potsdamer Zweigstelle des Krebsregisters geprüft.[164] Im Nachgang hatte das Register einige der festgestellten Mängel behoben. Bei anderen steht dies noch aus. In diesem Jahr konzentrierte sich die Prüfung auf die Berliner Zweigstelle.

Im Krebsregister-Staatsvertrag zwischen den beteiligten Ländern ist detailliert vorgegeben, wie das Krebsregister mit den eingehenden Meldungen umzugehen hat. U. a. ist festgelegt, wie Daten langfristig gespeichert und wann sie gelöscht werden müssen.

Im Zuge der Prüfung mussten wir feststellen, dass das Register neben dem Hauptdatenbestand, der in einer besonders gesicherten Datenbank geführt wird, einen zweiten Datenbestand mit elektronischen Kopien von Meldebögen hält. Dort haben wir Daten gefunden, die für Betroffene aus Berlin zwei Jahre, aus Brandenburg bis in das Jahr 2004 zurückreichen. Die gesetzliche Regelung sieht demgegenüber vor, dass die Daten aus den Meldebögen innerhalb von sechs Wochen elektronisch zu erfassen sind. Nach der Erfassung sind die Meldebögen zu ver-

164 JB 2016, 1.3

nichten. Damit überschreitet die Datenspeicherung sowohl nach Art – die Namen der Patientinnen und Patienten sind nach der gesetzlichen Regelung getrennt von den medizinischen Daten zu speichern – als auch nach zeitlichem Umfang die vom Gesetz vorgegebenen Schranken.

Es zählt auch zu den gesetzlichen Anforderungen an die Registerführung, dass der Direktabruf von Daten nach festgelegtem Zeitablauf gesperrt und diese im vorgeschriebenen Turnus gelöscht werden. Trotz eines Praxisbetriebs von mittlerweile zwei Jahren konnte das Krebsregister noch kein Konzept für Sperrungen und die Löschung von Daten vorweisen.

Die höchst sensitive und flächendeckende Speicherung von Daten über Krebserkrankungen im klinischen Krebsregister muss sich streng an den gesetzlichen Vorgaben orientieren, um den Eingriff in die Rechte der Betroffenen so gering wie möglich zu halten und Risiken von Datenlecks oder Datenmissbrauch zu minimieren.

6.9 Einzelfälle

6.9.1 Ärztliche Bescheinigung zur Aufnahme in Kitas

Aus der Praxis

Wir erhielten von einem Kinderarzt den Vordruck einer Ärztlichen Bescheinigung, die für die Aufnahme in eine Kita ausgefüllt werden musste. Das Infektionsschutzgesetz sieht vor, dass vor Aufnahme in eine betreuende Kindertageseinrichtung eine Impfberatung erfolgt, die durch den behandelnden Kinderarzt bestätigt wird. Auf dem entsprechenden Formular sollten jedoch auch bereits erfolgte Schutzimpfungen konkret angegeben werden.

Die Angabe bereits erfolgter Schutzimpfungen kann jedoch nur freiwillig erfolgen, da es auch für die Durchführung der Impfungen selbst keine gesetzliche Verpflichtung gibt. Wir konnten eine Anpassung des Vordrucks erreichen, sodass alle über die reine Bestätigung der stattgefundenen Beratung hinausgehenden Angaben zukünftig ausschließlich auf freiwilliger Basis mit Einverständnis der Eltern gemacht werden.

6.9.2 Dürfen Ärztinnen und Ärzte Patientendaten gegenüber Bewertungsportalen offenbaren?

Über anonyme Bewertungsportale haben Patientinnen und Patienten die Möglichkeit, Arztbesuche und medizinische Behandlungen zu bewerten. Sofern die jeweiligen Ärztinnen und Ärzte mit diesen öffentlich zugänglichen Bewertungen nicht einverstanden sind, besteht die Möglichkeit, sie durch den Portalbetreiber überprüfen zu lassen und eigene Darstellungen des Sachverhalts einzureichen.

Wir erhielten mehrere Beschwerden, bei denen im Rahmen der Gegendarstellung identifizierende Patientendaten gegenüber dem Portalbetreiber preisgegeben wurden. Dies ist unzulässig und verstößt gegen die ärztliche Schweigepflicht. Die Ärztinnen und Ärzte können nicht davon ausgehen, dass dem jeweiligen Portalbetreiber die Identität der Patientin oder des Patienten bekannt ist, sodass eine Gegendarstellung lediglich ohne Nennung von identifizierenden Daten zulässig ist.

7 Soziales und Arbeit

7.1 Sozialhilfedaten bei der Senatsverwaltung für Integration, Arbeit und Soziales – Rechtmäßig und sicher?

Die bezirklichen Sozialämter verarbeiten Sozialdaten einer Vielzahl von Berliner Bürgerinnen und Bürgern. Die Senatsverwaltung für Integration, Arbeit und Soziales betreibt für die Bezirke ein IT-Fachverfahren, mit dem die Sozialdaten verarbeitet werden. Die Senatsverwaltung ihrerseits erstellt aus den Sozialdaten Statistiken für die unterschiedlichsten Zwecke, die insbesondere bedeutsam für die Sozialplanung im Land Berlin sind. Da auch im Rahmen der Statistikerstellung das Sozialgeheimnis gewahrt werden muss, stehen wir seit geraumer Zeit in Gesprächen mit der zuständigen Senatsverwaltung. Im Oktober 2019 haben wir Teile des Verfahrens vor Ort geprüft.

Die Bezirksverwaltungen und andere Einrichtungen im sozialen Bereich setzen im Land Berlin das IT-Fachverfahren „BASIS“ ein zur Erfassung von Daten über Personen, die Sozialleistungen beantragen und erhalten. Mithilfe des Verfahrens werden Anspruchsvoraussetzungen festgestellt, Daten zur Erbringung von Sozialleistungen verarbeitet und finanzielle Leistungen ausgezahlt.

Die Senatsverwaltung für Integration, Arbeit und Soziales betreibt das Fachverfahren zentral. Da es sich bei den verarbeiteten Daten durchweg um sensible Sozialdaten und zudem in erheblichem Umfang auch um sensitive Gesundheitsdaten handelt, die einem besonderen Schutz unterliegen, ist zum einen ein besonderes Augenmerk auf den datenschutzgerechten und sicheren Betrieb des bereits seit vielen Jahren im Einsatz befindlichen Verfahrens zu legen. Zum anderen ist zu berücksichtigen, dass der Zugriff auf die Sozialdaten durch die Senatsverwaltung zum Zwecke der Erstellung von Statistiken unter Wahrung des Sozialgeheimnis-

ses[165] und unter Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten[166] erfolgen muss.

Im Rahmen einer Vor-Ort-Prüfung bei der Senatsverwaltung haben wir uns einen Überblick über die Datenverarbeitung zur Vorbereitung und Erstellung von Statistiken verschafft. Wir mussten feststellen, dass Nachbesserungsbedarf im Hinblick auf die Einhaltung datenschutzrechtlicher Vorgaben, insbesondere auch der Vorgaben der DS-GVO, besteht.

Die Rechtsgrundlage für die Verarbeitung konnte durch die Senatsverwaltung nicht immer eindeutig benannt werden. Identifizierende Angaben der Bürgerinnen und Bürger werden bei der Vorbereitung von Statistiken gespeichert und verarbeitet, obwohl sie hierfür nicht erforderlich sind. Wir fanden Datenbestände vor, die längst hätten gelöscht werden müssen. Der Schutz gegen unbefugte oder unrechtmäßige Verarbeitung war unzureichend, eine Reihe von Verarbeitungsschritten nicht im Nachhinein nachvollziehbar. Es gab kein Datenschutz- und kein umfassendes Informationssicherheitsmanagement. Eine Datenschutz-Folgenabschätzung wurde nicht durchgeführt.

Da es sich im Sozialleistungsbereich um Sachverhalte handelt, die weit in den persönlichen Lebensbereich der betroffenen Personen hineinreichen, ist die Einhaltung datenschutzrechtlicher Vorschriften hier von elementarer Bedeutung. Es ist uns ein wichtiges Anliegen, mit der Senatsverwaltung möglichst zeitnah einen vollständig datenschutzkonformen Zustand zu erreichen.

165 § 35 Abs. 1 Sozialgesetzbuch – Erstes Buch (SGB I)
166 Art. 5 Abs. 1 DS-GVO

7.2 Ärztliche Auskunft an das Landesamt für Gesundheit und Soziales

Das Landesamt für Gesundheit und Soziales (LAGeSo) holt zur Feststellung des Grades einer Schwerbehinderung Auskünfte von den behandelnden Ärztinnen und Ärzten der Antragstellenden ein, ohne diesen die jeweilige Einwilligungs- und Schweigepflichtentbindungserklärung der Betroffenen vorzulegen.

Menschen, die in Deutschland leben oder arbeiten und bei denen ein Grad der Behinderung von mindestens fünfzig festgestellt wurde, sind schwerbehindert im Sinne des Sozialgesetzbuches. Das Versorgungsamt des LAGeSo stellt auf Antrag der Betroffenen deren Schwerbehinderteneigenschaft fest. Um zu entscheiden, ob bzw. in welchem Umfang eine Schwerbehinderung vorliegt, benötigt das LAGeSo Auskünfte von den behandelnden Ärztinnen und Ärzten. Hierfür holt das LAGeSo zwar eine Einwilligungs- und Schweigepflichtentbindungserklärung von den Antragstellerinnen und Antragstellern ein, legt diese den Ärztinnen und Ärzten jedoch nicht vor. Ein Arzt war unsicher, ob er die verlangten Auskünfte gegenüber dem LAGeSo erteilen darf und hat uns um Prüfung gebeten.

Nach der Datenschutz-Grundverordnung müssen Ärztinnen und Ärzte bei einwilligungsbasierten Datenübermittlungen nachweisen können, dass ihre Patientinnen und Patienten in die Datenweitergabe eingewilligt haben. Aus datenschutzrechtlicher Sicht ist es daher vorzugswürdig, wenn das Versorgungsamt den Ärztinnen und Ärzten die Einwilligungs- und Schweigepflichtentbindungserklärung vorlegt.

Das LAGeSo kann allerdings unter bestimmten Voraussetzungen auf die Vorlage der Erklärungen verzichten. Hierbei ist zunächst zu berücksichtigen, dass das LAGeSo die Verantwortung für die Richtigkeit der Angaben in seinem Ersuchen an die Ärzteschaft trägt, also insbesondere für das rechtswirksame Einholen der Einwilligung. Konkret bedeutet dies, das Versorgungsamt muss sicherstellen, dass die Antragstellenden die Einwilligung für einen bestimmten Fall, in Kenntnis der Sachlage sowie freiwillig erteilen, und die betroffenen Personen auf ihr Widerrufsrecht für die Zukunft hingewiesen werden. Um der in der Datenschutz-Grundverordnung geregelten Rechenschaftspflicht nachzukommen, ist es erforderlich,

dass das Versorgungsamt das Vorliegen der Erklärung jederzeit nachweisen kann. Dazu empfiehlt es sich, die Einwilligung schriftlich einzuholen.

Auch muss ein Verfahren etabliert werden, das eine zügige Übersendung der Einwilligungs- und Schweigepflichtentbindungserklärungen sicherstellt, sofern die Ärztinnen und Ärzte vor der Übermittlung die Vorlage entsprechender Erklärungen verlangen. Dies ist notwendig, um den Ärztinnen und Ärzten die entsprechende Rechtssicherheit geben zu können.

Das LAGeSo muss im Schwerbehindertenverfahren im Regelfall der Ärzteschaft nicht die Einwilligungs- und Schweigepflichtentbindungserklärungen ihrer Patientinnen und Patienten vorlegen. Wenn Ärztinnen und Ärzte aber nach der Vorlage einer entsprechenden Erklärung verlangen, so ist ihnen diese unverzüglich zugänglich zu machen.

7.3 Unzulässiger Austausch von Sozialdaten zwischen Bezirksamt und Krankenkasse

Durch eine Eingabe erfuhren wir, dass ein Bezirksamt Sozialdaten eines Sozialleistungsempfängers mit dessen Krankenkasse ausgetauscht hat. Hintergrund war, dass das Bezirksamt die Zahlung der Krankenkassenbeiträge des Betroffenen übernommen hatte.

Das Bezirksamt hat Informationen über Änderungen in der Höhe der Beiträge bei der Krankenkasse eingeholt, um die Sozialhilfeleistung entsprechend anpassen zu können. Zudem hat es die Krankenkasse über die Übernahme von Beiträgen informiert.

Dieses Vorgehen war unzulässig. Das Bezirksamt muss zwar über die Höhe der Krankenkassenbeiträge informiert sein, um die Sozialhilfe gewähren zu können. Auch ist es im berechtigten Interesse der Krankenkasse, zu wissen, welche Beiträge vom Sozialamt übernommen werden. Allerdings müssen die beteiligten Stellen datenschutzrechtliche Grundsätze beachten.

Hier hat das Bezirksamt gegen den Grundsatz der Direkterhebung verstoßen, wonach Sozialdaten direkt bei den Betroffenen zu erheben sind und nur in gesetzlichen Ausnahmefällen auch bei Dritten abgefragt werden dürfen.[167] Eine solche Ausnahme lag nicht vor. Die Anfrage bei der Krankenkasse war nicht erforderlich, da Informationen über Änderungen in der Beitragshöhe auch direkt beim Leistungsbezieher hätten erfragt werden können. Auch dürfen Sozialdaten an Dritte nur weitergegeben werden, sofern dies erforderlich ist. Diese Voraussetzungen waren nicht erfüllt. Das Bezirksamt hätte anstelle der Krankenkasse den Leistungsempfänger über die Übernahme der Beiträge informieren müssen. Der Leistungsbezieher hätte im Anschluss selbst seine Krankenkasse über die Übernahme der Beiträge durch das Bezirksamt informieren können. Wir haben das Vorgehen des Bezirksamtes bemängelt. Daraufhin hat das Bezirksamt Arbeitshinweise für eine datenschutzgerechte Verfahrensweise erstellt.

Im konkreten Fall konnten wir erreichen, dass der Grundsatz der Direkterhebung bei den Leistungsempfängern künftig beachtet wird.

7.4 Sensible Daten von Kursteilnehmenden auf einer internen Online-Lernplattform

Aus der Praxis

Durch eine Eingabe erfuhren wir, dass auf der internen Online-Lernplattform einer Ausbildungseinrichtung sensible Daten von Kursteilnehmenden – z. B. zu Lernschwächen oder zur Motivation – für Teilnehmende eines nachfolgenden Kurses verfügbar waren.

Das Vorgehen der Ausbildungseinrichtung war unzulässig. Die Einrichtung betreibt eine interne Online-Lernplattform, auf der Unterlagen der Dozenten für die Teilnehmenden der jeweiligen Kurse zum Download verfügbar sind. Bei neuen Kursen wurden in der Regel die Unterlagen aus dem vergangenen Kurs kopiert, da die Lehrenden sie nicht stets anpassen oder neu erstellen. Diese Arbeitserleichterung ist natürlich nachvollziehbar. Allerdings enthielten die Unterlagen in diesem konkreten Fall auch sensible personenbezogene Daten von Kursteilneh-

167 Siehe § 67a Abs. 2 Zehntes Buch Sozialgesetzbuch (SGB X)

menden, wie etwa deren Lernschwächen, die für die Teilnehmenden des nachfolgenden Kurses sichtbar waren. Dies darf keinesfalls passieren. Hier kam es versehentlich sogar noch zu einem weiteren Vorkommnis dieser Art, selbst nachdem die automatische Übernahme von Altskripten nach einem Hinweis einer Dozentin untersagt worden war.

Es stößt bereits auf erhebliche datenschutzrechtliche Bedenken, sensible Daten von Kursteilnehmenden in eine Unterlage aufzunehmen und für andere Mitglieder der Lerngruppe zum Download zur Verfügung zu stellen. In keinem Fall bestand eine gesetzliche Grundlage, die es erlaubt hätte, die sensiblen Daten für die Teilnehmenden des nachfolgenden Kurses zugänglich zu machen. Auf unsere Intervention hin hat die Ausbildungseinrichtung zugesichert, vergleichbare Fälle in Zukunft auszuschließen. Auch wurden auf unsere Veranlassung hin die Betroffenen über den Vorfall entsprechend den gesetzlichen Vorgaben informiert.

Arbeitsprozesse von Ausbildungseinrichtungen sind so zu gestalten, dass die personenbezogenen Daten der Kursteilnehmenden geschützt sind.

8 Beschäftigtendatenschutz

8.1 Last und Segen ehrenamtlicher Tätigkeit

Aus der Praxis

Ehrenamtlich beschäftigte Mitglieder einer Gewerkschaft erhielten von ihrer Gewerkschaft und verarbeiteten in großer Menge personenbezogene Daten von Gewerkschaftsmitgliedern zur Zurückgewinnung von Mitgliedern und zur Erbringung von Serviceleistungen im Lohnsteuerbereich. Bei den Daten handelt es sich u. a. um Namen, Anschrift, Alter, Gewerkschaftszugehörigkeit, Einkommenshöhe, Streikleistungen etc. Die ehrenamtlichen Mitglieder haben eine Datenschutzerklärung unterschrieben und wurden belehrt; weitere Vereinbarungen wurden nicht abgeschlossen.

Bei Gewerkschaftsdaten handelt es sich um sensitive Daten,[168] sie dürfen grundsätzlich an ehrenamtlich tätige Mitglieder weitergegeben werden, da diese keine Außenstehenden sind.[169] Allerdings ist für die Tätigkeit bzw. Aufgabe von Ehrenamtlichen gerade im Hinblick auf die Verarbeitung von sensiblen Gewerkschaftsdaten eine klare schriftliche Beschreibung von Rechten und Pflichten der Verantwortlichen und des jeweils ehrenamtlich Tätigen – ähnlich wie bei einem Auftragsverhältnis – geboten. Allein eine Datenschutzerklärung und Belehrung der Ehrenamtlichen sind keinesfalls ausreichend.

Häufig werden Daten von Ehrenamtlichen auch nicht in den Räumlichkeiten der Verantwortlichen, sondern beispielsweise „von zu Hause aus" auf privaten bzw. externen Rechnern, die der direkten Einflussnahme und Kontrolle der Verantwortlichen entzogen sind, verarbeitet. Dies birgt ein hohes Sicherheitsrisiko für diese empfindlichen und besonders schutzwürdigen Daten, das mit den Grundsätzen der DS-GVO unvereinbar ist.[170]

168 Art. 9 Abs. 1 DS-GVO; § 22 BDSG
169 § Art. 9 Abs. 2 lit. d DS-GVO
170 Art. 32 DS-GVO

Daher sind mit jeder und jedem ehrenamtlich Tätigen schriftliche Regelungsabsprachen zu treffen bzw. der jeweilige Auftrag ist insoweit zu präzisieren und zu konkretisieren, dass genau festgelegt ist, welche Daten wie, wo und in welchem Umfang verarbeitet werden dürfen. Dabei ist zu empfehlen, ähnliche Festlegungen wie bei der Tele-Heimarbeit zu treffen, um den Verantwortlichen die Möglichkeit der ordnungsgemäßen Kontrolle zu geben. Ebenso ist in dem Auftrag aber auch die Pflicht der Ehrenamtlichen zu fixieren, gegenüber den Verantwortlichen, hier der Gewerkschaft, Veränderungen hinsichtlich ihrer Leistungserbringung anzuzeigen, wenn diese relevant für den Inhalt und den Umfang der ehrenamtlichen Tätigkeit sind.

Außerdem sind klare Festlegungen zu technisch-organisatorischen Maßnahmen, insbesondere bei Gebrauch von privater Hardware bzw. privaten Endgeräten,[171] zu treffen.[172]

Unabhängig davon sollte die Gewerkschaft mindestens einmal im Jahr ehrenamtlich Tätige um Auskunft bitten, ob aus ihrer Sicht Statusänderungen vorliegen und ob Maß und Umfang der Tätigkeit für ein Ehrenamt noch angemessen sind.

Diese Anforderungen für die Beschäftigung von ehrenamtlich Tätigen haben wir der betreffenden Gewerkschaft mitgeteilt und die Umsetzung unserer Empfehlungen bzw. Forderungen zeitnah eingefordert.

Für die Tätigkeit von ehrenamtlich Beschäftigten von Gewerkschaften sind zusätzlich zu Datenschutzerklärungen und Belehrungen klare Arbeitsvorgaben und Verhaltensregeln festzulegen.

8.2 Umgang mit Migrationsdaten

Das Gesetz zur Regelung von Partizipation und Integration in Berlin (PartIntG) hat zum Ziel, Menschen mit Migrationshintergrund die Möglichkeit zur gleichberechtigten Teilhabe in allen Bereichen des gesellschaftlichen Lebens zu geben und

171 Bring Your Own Device (BYOD)
172 JB 2012, 2.3

gleichzeitig jede Benachteiligung auszuschließen. Angestrebt wird die Erhöhung des Anteils der Beschäftigten mit Migrationshintergrund in den Institutionen, die in den Geltungsbereich des PartIntG fallen, entsprechend ihrem Anteil an der Bevölkerung. Der Senat wird durch das Gesetz ermächtigt, Zielvorgaben festzulegen. Bestimmt wird darüber hinaus, dass in der regelmäßigen Berichterstattung über die Personalentwicklung des öffentlichen Dienstes und der juristischen Personen des Privatrechts, an denen das Land Berlin Mehrheitsbeteiligungen hält, die Entwicklung des Anteils von Menschen mit Migrationshintergrund separat ausgewiesen wird. Um entsprechend berichten zu können, möchte der Senat statistische Aussagen zum Migrationshintergrund der Beschäftigten auch mit anderen im Rahmen des Personalstrukturstatistikgesetzes (PSSG) erfassten Merkmalen zum beruflichen Werdegang der Betroffenen inklusive z. B. Einkommen und Beurlaubungen oder sonstigen Abwesenheiten[173] verknüpfen, um die berufliche Entwicklung der Betroffenen statistisch nachverfolgen zu können. Die Senatsverwaltung für Integration, Arbeit und Soziales fragte nach, ob hierfür die Einholung einer Einwilligung der Betroffenen notwendig ist.

Zu dieser Frage sind die Regelungen des Berliner Datenschutzgesetzes in Verbindung mit dem Bundesdatenschutzgesetz zu beachten. Grundsätzlich dürfen personenbezogene Daten von Beschäftigten nur für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.[174] Die Erfassung des Migrationshintergrundes und dessen Verknüpfung mit anderen Merkmalen bzw. Daten der Betroffenen ist nicht für die Durchführung des Beschäftigungsverhältnisses erforderlich. Insoweit kommt nur eine Einwilligung der Betroffenen als Rechtsgrundlage in Betracht, eine Erhebung dieser Daten ohne eine entsprechende Einwilligung ist unzulässig.[175]

173 § 6 PSSG

174 § 18 Abs. 1 BlnDSG i. V. m. § 26 Abs. 1 BDSG

175 § 18 Abs. 1 BlnDSG; §§ 26 Abs. 2 und 3, 22 BDSG

In diesem Zusammenhang ist auch festzustellen, dass im Berliner Datenschutzgesetz ein Verweis auf das Bundesdatenschutzgesetz, das die Verarbeitungen zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken ohne Einwilligung des Betroffenen zulässt, fehlt.[176]

Die Freiwilligkeit kann bei der Einwilligung in die Datenverarbeitung im Rahmen des PSSG unterstellt werden, weil die betroffene Person keinerlei rechtliche oder wirtschaftliche Nachteile befürchten muss, wenn sie die Einwilligung nicht erteilt.[177] Die Einwilligung bedarf grundsätzlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.[178] Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht in Textform aufzuklären.[179]

Die o. g. Ausführungen gelten auch für Einwilligungen in die Verarbeitung besonderer Kategorien personenbezogener Daten.[180] Dabei muss sich die Einwilligung jedoch ausdrücklich auch auf diese Daten beziehen. In diesem Zusammenhang sind zudem die besonderen gesetzlichen Vorgaben zum Ergreifen geeigneter Schutzmaßnahmen zu beachten.[181] Die Betroffenen sind bei der Einwilligung auf die vorgesehenen Verknüpfungen mit den vom PSSG erfassten Merkmalen hinzuweisen. Bei einem Widerspruch der Betroffenen gegen eine weitere Datenverarbeitung in pseudonymisierter Form wäre nur noch eine Verarbeitung in anonymisierter Form möglich.

Die Aufnahme von Daten zum Migrationshintergrund kann nur auf eine Einwilligung der Betroffenen gestützt werden. Diese können der erteilten Einwilligung jederzeit widersprechen.

176 § 18 BlnDSG; § 27 BDSG
177 § 26 Abs. 2 Satz 1 und 2 BDSG
178 § 26 Abs. 2 Satz 3 BDSG
179 § 26 Abs. 2 Satz 4 BDSG; Art. 7 Abs. 3 DS-GVO
180 § 26 Abs. 3 Satz 2 BDSG
181 § 22 Abs. 2 BDSG

8.3 Übermittlung der Arztrechnung eines Beschäftigten an Dritte

Aus der Praxis

Ein Polizist hatte im Rahmen eines Einsatzes Verletzungen erlitten und Ärzte aufgesucht. Die Arztrechnungen reichte er bei der Dienstunfallfürsorge der Polizei zur Erstattung ein. Sein Dienstherr forderte nun die entstandenen Arztkosten bei dem Verursacher ein.

Die vom Betroffenen an die Dienstunfallfürsorge eingereichten Arztrechnungen wurden von dort ungeschwärzt an das Justiziariat der Polizei und dann an einen externen Rechtsanwalt übermittelt, der wiederum die Unterlagen an das Gericht und die Gegenseite weiterleitete. Sowohl der Name als auch die private Wohnanschrift des Betroffenen waren auf diesen Unterlagen lesbar.

Bei der Adresse des Beschäftigten handelt es sich um ein Personalaktendatum.[182] Die Zulässigkeit der Übermittlung durch den Dienstherrn an einen externen Rechtsanwalt richtet sich nach dem Landesbeamtengesetz.[183] Danach ist die Übermittlung von Personalaktendaten an Dritte ohne Einwilligung der Beschäftigten zulässig, wenn dies aus Gründen des Gemeinwohls zwingend erforderlich ist. Zum Gemeinwohl gehört auch das Interesse des Dienstherrn, die gewährte Dienstunfallfürsorge gegenüber dem Schädiger gerichtlich geltend zu machen. Denn der dem Betroffenen zustehende Schadensersatzanspruch geht im Falle des Ersatzes durch den Dienstherrn auf diesen über.[184] Dem Justiziariat kommt dann die Aufgabe zu, die Dienstunfallfürsorge gegenüber dem Schädiger als Schadensersatz einzuklagen.

Die Übermittlung der Adresse muss dabei für die Schadensersatzklage zwingend erforderlich sein. Dies bedeutet, dass es hierzu keine Alternative geben darf, um dem Interesse des Dienstherrn Rechnung zu tragen. In diesem Sinne war die Angabe der Privatanschrift keinesfalls zwingend erforderlich. Grundsätzlich müssen Schriftsätze vor den Zivilgerichten die für die Darlegung des geltend zu machen-

182 § 84 Abs. 1 Landesbeamtengesetz (LBG)
183 § 88 Abs. 2 Satz 1 LBG
184 § 79 LBG

den Anspruches erforderlichen Beweismittel enthalten. Da der Beschwerdeführer im vorliegenden Fall maßgeblich als Zeuge in Betracht kam, musste er namentlich benannt werden, da es für die ordnungsgemäße Benennung eines Zeugen im Zivilprozess keine Alternative zur namentlichen Benennung gibt und der Beschwerdeführer in seiner Position als Geschädigter als Zeuge nicht ersetzbar war.[185] Als Anschrift dagegen war auch die Dienstanschrift ausreichend.

Unabhängig davon besteht eine Anonymisierungspflicht des Dienstherrn hinsichtlich der Wohnanschrift. Sie ergibt sich aus der allgemeinen Fürsorgepflicht des Dienstherrn, die wiederum als Strukturprinzip aus den hergebrachten Grundsätzen des Berufsbeamtentums im Grundgesetz (GG) anerkannt ist.[186]

Die Übermittlung der Privatanschrift an den Anwalt der Polizei war unzulässig. Die Angabe der Privatanschrift war keinesfalls zwingend erforderlich. Dagegen war die Übermittlung des Namens zur ordnungsgemäßen Benennung eines Zeugen zwingend notwendig.

8.4 Einsichtnahme in Beurteilungen von Mitbewerberinnen und Mitbewerbern

Aus der Praxis

Die Beschwerdeführerin hatte sich auf die Stelle einer Sekretärin bei der Senatsverwaltung für Bildung, Jugend und Familie beworben und wurde abgelehnt. Deshalb bat sie um Einsicht in ihre Beurteilungsunterlagen, um die Gründe der Ablehnung nachvollziehen zu können. Ihr wurden daraufhin nicht nur ihre, sondern sämtliche Beurteilungsunterlagen aller Bewerberinnen und Bewerber zur Durchsicht zur Verfügung gestellt. Sie beschwerte sich bei uns darüber, da sie befürchtete, dass auch ihre personenbezogenen Daten von Mitbewerberinnen und Mitbewerbern auf diesem Weg eingesehen werden könnten.

Die Vorgehensweise der Senatsverwaltung für Bildung, Jugend und Familie war rechtswidrig. Bewerbungs- bzw. Beurteilungsunterlagen enthalten sensible Da-

185 § 88 Abs. 2 Satz 1 LBG
186 Art. 33 Abs. 5 GG

ten und unterfallen im öffentlichen Bereich dem Personalaktenrecht nach dem Landesbeamtengesetz bzw. dem Tarifvertrag der Länder. Damit unterliegen sie einer gesteigerten Geheimhaltungspflicht des Dienstherrn.[187] Sie dürfen nur mit Einwilligung der Betroffenen oder aufgrund einer gesetzlichen Grundlage Dritten zur Kenntnis gegeben werden.[188]

Das Akteneinsichtsrecht unterlegener Bewerberinnen und Bewerber ergibt sich aus dem Grundgesetz. Danach hat jeder Deutsche nach seiner Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amt.[189]

Nach einer Entscheidung des Bundesverwaltungsgerichtes aus dem Jahr 2012 ist es für einen effektiven Rechtsschutz der unterlegenen Bewerberin bzw. des unterlegenen Bewerbers erforderlich, aber auch genügend, Einsicht in die für die konkret angegriffene Auswahlentscheidung tragenden Erwägungen zu erhalten. Diese sind in der Regel z. B. in einem Auswahlvermerk zusammengefasst und dokumentiert. Nur diese Gründe können die Rechtmäßigkeit der Auswahlentscheidung stützen und nur diese Gründe müssen den Betroffenen ggf. zur Nachprüfung in einem Rechtsbehelfsverfahren vorgelegt werden. Ausdrücklich verneint das Bundesverwaltungsgericht dagegen einen Anspruch, darüber hinausgehende Informationen und Unterlagen einzusehen, die nicht Bestandteil der Auswahldokumentationen sind, wie z. B. interne vorbereitende oder erläuternde Vermerke.

Damit stellt das Bundesverwaltungsgericht klar, dass eine restriktive Handhabung der Bewerbungsunterlagen im Zusammenhang mit Einsichtsrechten von Mitbewerberinnen und Mitbewerbern geboten ist. Im vorliegenden Fall hätte der Bewerberin daher zunächst nur der Auswahlvermerk vorgelegt werden dürfen; bei etwaigen Verweisen im Vermerk auf Beurteilungen der Mitbewerberinnen und Mitbewerber wäre ein weiterer Anspruch auf Kenntnisnahme der Beurteilungen bzw. auf weitere Auswahlkriterien gegeben gewesen.

Im vorliegenden Fall handelte es sich zudem um eine Angestelltenstelle im Sekretariat. Ein in Ausnahmefällen mögliches Einsichtsrecht in Personalakten-

187 § 84 Abs. 4 LBG, § 3 TV-L
188 § 88 LBG, § 3 TV-L
189 Art. 33 Abs. 2 GG, 19 Abs. 4 GG

daten ohne Einwilligung der Beamtin oder des Beamten findet sich für Angestellte nicht im Tarifvertrag der Länder.

Dem Recht auf Einsichtnahme in Bewerbungsunterlagen von Mitbewerberinnen und Mitbewerbern sind enge Grenzen gesetzt.

9 Wirtschaft

9.1 „Drücken Sie…“ – Aufzeichnung von Kundengesprächen nach der DS-GVO

Immer wieder erreichen uns Anfragen von Verbraucherinnen und Verbrauchern, die sich erkundigen, ob Aufzeichnungen von Telefongesprächen zulässig sind, wenn eine Aufzeichnung nur verhindert werden kann, wenn die betroffenen Personen zu Beginn aktiv widersprechen.

Beispielhaft hierfür war der Fall eines großen Elektronik-Konzerns. Bei einem Anruf auf der Service-Telefonnummer informierte eine automatische Ansage die Kundinnen und Kunden zu Beginn des Telefonats über die Aufzeichnung des Gesprächs. Im Anschluss mussten die Kundinnen und Kunden per Tastendruck die Kategorie ihres Anliegens auswählen. Erst als eine Mitarbeiterin oder ein Mitarbeiter das Gespräch entgegennahm, konnten die Betroffenen der Aufzeichnung des Gesprächs widersprechen. Wenn die Kundinnen und Kunden widersprachen, wurde das bis zu diesem Zeitpunkt bereits aufgezeichnete Gespräch gelöscht und die Aufzeichnung nicht fortgesetzt.

Die Vorgehensweise des Unternehmens war schon nach alter Rechtslage zu beanstanden, weil die Einwilligung in die Aufzeichnung von Kundengesprächen vor Beginn der Aufzeichnung eingeholt werden musste. Die Möglichkeit eines späteren Widerspruchs und eine damit verbundene Löschung reichten nicht aus. Daran hat sich auch durch die DS-GVO nichts geändert.

Auf unseren Hinweis und im Hinblick auf die DS-GVO stellte das betreffende Unternehmen sein Servicetelefon so um, dass die Kundinnen und Kunden unmittelbar nach der Begrüßung darauf hingewiesen wurden, dass das Gespräch aus Trainings- und Qualitätsgründen aufgezeichnet und überwacht werden kann. Danach hatten die Kundinnen und Kunden die Möglichkeit, der Aufzeichnung zu widersprechen, indem sie die Taste „1“ drückten. Wenn sie dies nicht taten, wurde das weitere Gespräch aufgezeichnet.

Auch diese Vorgehensweise mussten wir beanstanden. Nach der Datenschutz-Grundverordnung muss die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.[190] Ein Stillschweigen bzw. eine Widerspruchsmöglichkeit zu Beginn des Gesprächs reicht hierfür nicht aus.

Auf unseren erneuten Hinweis hat das Unternehmen sein Verfahren mittlerweile so umgestellt, dass die Kundinnen und Kunden sich durch Tastendruck aktiv entscheiden müssen, ob Sie einer Aufzeichnung zustimmen oder nicht. Damit ist gewährleistet, dass die Kundinnen und Kunden durch eine aktive Handlung in die Aufzeichnung ihrer Gespräche einwilligen.

Wenn Unternehmen ein Kundengespräch aufzeichnen möchten, müssen die Kundinnen und Kunden vor Beginn der konkreten Aufzeichnung durch eine eindeutige bestätigende Handlung, z. B. das freiwillige Drücken einer Telefontaste, in die Aufzeichnung einwilligen.

9.2 „Ihren Ausweis, bitte!“ – Identifizierung bei der Geltendmachung der Betroffenenrechte

Häufig werden Personen, die Unternehmen um eine Auskunft oder Löschung der über sie gespeicherten Daten bitten, zunächst gebeten, sich mit einer Personalausweiskopie zu identifizieren, obwohl keine Zweifel an ihrer Identität bestehen.

Das Anfordern einer Ausweiskopie stellt für die Betroffenen eine Hürde dar. Ein Auskunfts- oder Löschungsverlangen sollte aber möglichst einfach zu stellen sein.[191] Durch den zusätzlichen Aufwand können Personen davon abgehalten werden, ihre Betroffenenrechte auszuüben. Die verantwortlichen Unternehmen dürfen daher nur bei begründeten Zweifeln an der Identität einer Person zusätzliche

190 Art. 4 Nr. 2 DS-GVO

191 Art. 12 Abs. 1 Satz 1 DS-GVO

Informationen anfordern.[192] Wenn eine Person Auskunft über die zu ihr gespeicherten Daten verlangt und die Information an ihre dem Unternehmen bekannte Adresse gesendet werden soll, gibt es meist schon keine Zweifel an der Identität. Das Gleiche gilt für Anfragen, die von E-Mail Adressen aus gesendet werden, die dem Unternehmen bekannt sind, weil sie auch sonst über dieselbe Adresse kommunizieren.

Müsste der Personalausweis generell vorgelegt werden, hätten Unternehmen Zugriff auf mehr Daten, als sie benötigen. In einigen Fällen wurden die betroffenen Personen auch gebeten, ihre Ausweiskopie per unverschlüsselter E-Mail zu senden. Eine Information, wie lange die Ausweisdaten gespeichert werden sollten, wurde i. d. R. nicht gegeben.

Natürlich darf eine Auskunft nur den tatsächlich Betroffenen zur Verfügung gestellt werden. Auch soll ein Konto nur von den Berechtigten gelöscht oder gesperrt werden können. Gleichzeitig aber sollte es nicht schwieriger sein, Betroffenenrechte geltend zu machen, als beispielsweise mit einem Unternehmen in eine Vertragsbeziehung zu treten. Kann ein Konto ohne Ausweisdokument angelegt werden, sollte auch die Löschung ohne Dokument möglich sein. Schließlich stellt sich hier die Frage, welchen Sinn das Anfordern eines Ausweisdokuments hat, wenn es mit keiner früher über die Person gespeicherten Information abgeglichen werden kann.

Neben einem Ausweisdokument gibt es auch andere Möglichkeiten zum Nachweis der Berechtigung, die zu einem Konto gespeicherten Informationen zu erfahren und das Konto zu löschen. So ist ein Portal, in welchem Personen ihre Anfragen mit den schon angelegten Zugangsdaten zu ihren Konten bestätigen können, eine gute Möglichkeit, sich zu authentifizieren. Gleichzeitig können Portale, in denen Anfragen zumindest teilweise automatisiert oder gut strukturiert bearbeitet werden, das Ausüben von Betroffenenrechten erleichtern.

Wenn in begründeten Einzelfällen die Anforderung einer Ausweiskopie berechtigt ist, etwa weil sich mehrere Daten der Betroffenen geändert haben, sind die

192 Art. 12 Abs. 6 DS-GVO

Unternehmen verpflichtet, darauf hinzuweisen, dass für die Identifizierung nicht erforderliche Daten geschwärzt werden können.

Eine Personalausweiskopie sollte für die Geltendmachung von Betroffenenrechten nur in Ausnahmefällen angefordert werden.

9.3 Lange Speicherdauer bei Lieferdiensten

Viele Lieferdienste speichern die Daten Ihrer Kundinnen und Kunden auch noch Jahre, nachdem diese etwas bestellt haben. Mit dem Inkrafttreten der Datenschutz-Grundverordnung haben Personen, die seit vielen Jahren nichts mehr bei den betreffenden Diensten bestellt hatten, dennoch Datenschutzerklärungen von diesen Unternehmen zugeschickt bekommen.

Durch die Benachrichtigungen über aktualisierte Datenschutzerklärungen ist einigen ehemaligen Kundinnen und Kunden von Lieferdiensten erst aufgefallen, dass ihre Daten immer noch bei den betreffenden Diensten gespeichert sind. So stellte sich heraus, dass Datensätze von Bestellungen gespeichert waren, die bis zu zehn Jahre zurücklagen. Es zeigte sich, dass viele Unternehmen keine funktionierenden Löschkonzepte haben. Es mangelt auch an der technischen Umsetzung, inaktive Kundenkonten systematisch zu löschen und gleichzeitig den aktiven Datenbestand zu erhalten.

Daten dürfen grundsätzlich nur so lange gespeichert werden, wie dies für die ursprünglichen Zwecke erforderlich ist. Bei einem Kundenkonto kommt es letztlich darauf an, ob dieses regelmäßig genutzt wird. Eine unbegrenzte Speicherung ist nicht zulässig. Die Unternehmen müssen Konzepte erstellen, nach welcher Zeit der Inaktivität Kundenkonten gelöscht werden, und diese durch Löschroutinen technisch-organisatorisch implementieren. Dabei kommt es auch darauf an, um welche Dienstleistung es sich handelt und in welchen Zyklen Kundinnen und Kunden typischerweise wieder bestellen. Eine Speicherung von Kundenkonten über einen Zeitraum zweijähriger Inaktivität wird allerdings regelmäßig nicht erforderlich sein.

Viele Beschwerden im Zusammenhang mit den Lieferdiensten befinden sich derzeit im Sanktionsverfahren.

Daten von Kundinnen und Kunden sollten nur so lange gespeichert werden, solange diese das Angebot von Lieferdiensten auch regelmäßig in Anspruch nehmen.

9.4 Bericht aus der Start-up-Sprechstunde

Die zweimal im Monat stattfindende Sprechstunde geht mit Erfolg ins dritte Jahr. Die Start-up-Unternehmen in Berlin nehmen die spezifische Beratungsmöglichkeit sehr gut an: Im letzten Jahr waren die Beratungstermine in der Regel für drei Monate im Voraus ausgebucht. Zwar ist die Sprechstunde grundsätzlich nicht termingebunden. Aufgrund der hohen Nachfrage war es allerdings in der Regel erforderlich, vorab einen Termin zu reservieren.

Auch viele Start-up-Unternehmen erkennen mit der gesetzlichen Umstellung auf die DS-GVO einen Anpassungsbedarf bei ihren Datenverarbeitungsprozessen bzw. stellen fest, dass das Thema „Datenschutz" auch für sie relevant werden könnte. Die DS-GVO war damit das bestimmende Thema in vielen Beratungsgesprächen, die wir geführt haben. Dabei war für viele Start-ups von Bedeutung, ob sie Datenschutzbeauftragte zu bestellen haben, wie Verfahrensverzeichnisse zu erstellen sind und wie die Informationspflichten erfüllt werden können. In den Beratungen ging es häufig darum, Datenverarbeitungen des Start-ups systematisch zu erfassen, Zwecke und Rechtsgrundlagen zu identifizieren und so Hilfestellungen zu geben, wie und worüber die von der Datenverarbeitung betroffenen Personen zu informieren sind. Häufig konnten wir darüber aufklären, dass keine Einwilligungserklärungen erforderlich sind, wenn die Start-ups etwa auf vertraglicher Basis Daten verarbeiten. Es zeigte sich, dass vielfach irrtümlich angenommen wird, dass die DS-GVO Einwilligungen für sämtliche Datenverarbeitungen erforderlich mache.

Viele Gespräche drehten sich auch um die Gestaltung und den Inhalt von Datenschutzerklärungen auf Webseiten. Bestimmende Themen waren dabei die Einbin-

dung von Instrumenten zur Webseitenanalyse und zur Verfolgung von Nutzungsaktivitäten sowie zur Einbindung von Social Plugins.

Darüber hinaus lebt die Sprechstunde aber – wie auch schon in den Vorjahren – von spezifischen, die jeweiligen Geschäftsmodelle betreffenden Fragestellungen. Hier zeigt sich, dass der persönliche Austausch zielführend ist, da verschiedene Lösungsmöglichkeiten bzw. die Anpassung von Prozessen diskutiert werden können. Thematisch geht es immer häufiger um den Einsatz von automatisierten Entscheidungsalgorithmen und von „intelligenten" Systemen. Aus datenschutzrechtlicher Sicht sind dabei insbesondere die Aspekte der Transparenz, der Gestaltung von Einwilligungserklärungen und Interventionsmöglichkeiten sowie der Anforderungen an die Durchführung von Datenschutz-Folgenabschätzungen zu beachten.

Der Beratungsbedarf bei den Start-up-Unternehmen ist unverändert hoch. Die Erfahrungen aus der Sprechstunde zeigen, dass das Format einer Sprechstunde die Start-up-Unternehmen sehr gut anspricht und im Gespräch viele Anfragen schnell und unkompliziert beantwortet werden können.

9.5 Stilles Factoring im Zeitalter der DS-GVO

Gerade kleine und mittelständische Unternehmen haben ein Interesse daran, ausstehende, häufig noch nicht fällige Forderungen zu verkaufen, um über ausreichende Liquidität zu verfügen. Hierauf spezialisierte Unternehmen, aber auch Banken bieten sich als Forderungskäufer an. Wenn die Schuldnerinnen und Schuldner nicht über den Forderungsverkauf informiert werden, spricht man von stillem Factoring. Dieses ist diskret und verhindert, dass sich Kundinnen und Kunden über den Verkauf nicht fälliger Forderungen beschweren. An uns wurde die Frage gerichtet, ob stilles Factoring unter der DS-GVO noch möglich ist bzw. welche Beschränkungen zu beachten sind.

Zivilrechtlich ist ein Forderungsverkauf möglich, wenn kein Abtretungsverbot vereinbart wurde.[193] Das Bürgerliche Gesetzbuch (BGB) geht auch davon aus, dass

193 § 399 Bürgerliches Gesetzbuch (BGB)

ein Forderungsverkauf ohne Information der Schuldnerin oder des Schuldners möglich ist. So regelt § 407 Abs. 1 BGB die befreiende Wirkung der Leistung an bisherige Gläubiger, wenn die Schuldnerin oder der Schuldner keine Kenntnis von der Abtretung hat.

Soweit das die Forderung aufkaufende Unternehmen keine Schuldnerdaten erhält oder die Schuldnerin eine juristische Person ist, ist stilles Factoring weiter unproblematisch möglich. Werden aber personenbezogene Daten an neue Gläubiger übermittelt, sind die Transparenzpflichten von Forderungsverkäufern[194] und Forderungskäufern[195] zu beachten. Forderungsverkäufer werden zumindest bei Vertragsschluss allgemein darüber informieren müssen, dass eine Datenübermittlung im Zusammenhang mit einem Forderungsverkauf ggf. erfolgt.[196] Auch Forderungskäufer haben Informationspflichten. Dies ist zwar nicht der Fall, wenn nationales Recht die Erlangung oder Offenlegung durch Rechtsvorschrift regelt, denen die Verantwortlichen unterliegen und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Personen vorsehen.[197] Es ist aber nicht anzunehmen, dass die BGB-Normen als solche Rechtsvorschriften anzusehen sind. Insbesondere ist darauf hinzuweisen, dass ein Forderungskäufer nicht das Recht hat, eine Bonitätsprüfung der Schuldnerin oder des Schuldners durchzuführen, da diese bei Vertragsabschluss nicht damit rechnen mussten, dass Dritte, mit denen sie keinen Vertrag abschließen wollten, Abfragen bei Auskunfteien vornehmen würden, die zu einer Verschlechterung ihres Scoring-Werts führen können.

Stilles Factoring sollte nur ohne Übermittlung von Schuldnerdaten erfolgen.

194 Art. 13 DS-GVO
195 Art. 14 DS-GVO
196 Art. 13 Abs. 1 lit. e DS-GVO
197 Art. 14 Abs. 5 lit. c DS-GVO

9.6 Weitergabe von Kontodaten an Überweisungsempfänger

Einige Banken übermitteln den Überweisungsempfängerinnen und -empfängern per Kontoauszug die IBAN-Daten der Überweisenden. Hierüber beschwerte sich ein Mieter, der zuviel gezahltes Geld von seinem Vermieter zurückerhalten hatte. Die betroffene Bank trug vor, zur Übermittlung der IBAN gesetzlich verpflichtet zu sein.

Gegen die Annahme einer rechtlichen Verpflichtung spricht schon, dass die Mehrzahl der deutschen Banken die IBAN nicht mittels Kontoauszug übermittelt. Zu beachten ist auch, dass anders als im vorliegenden Fall die IBAN leicht missbräuchlich genutzt werden kann, wie etwa für rechtswidrige Abbuchungen. Für Verbraucherinnen und Verbraucher ist es zudem schwer möglich, nachzuverfolgen und konkrete Kenntnis darüber zu behalten, wer ihre Kontodaten kennt und ggf. gespeichert hat.

Wir haben der Bank empfohlen, zukünftig auf die Übermittlung der IBAN zu verzichten. Die Bank ist nach der von ihr genannten Geldtransferverordnung nicht zur Übermittlung der IBAN-Daten verpflichtet. Dieses Gesetz ist auf die Verhinderung von Geldwäsche und Terrorismusfinanzierung im Rahmen von Geldtransfers gerichtet; hierfür reicht es aus, wenn die Bank mit Zahlungseingang die IBAN-Daten erhält. Sie darf die Daten aber nicht an die Zahlungsempfängerin bzw. den Zahlungsempfänger übermitteln. Die nationalen Regelungen zur Erbringung von Zahlungsdienstleistungen[198] sind im Lichte des Erwägungsgrundes 54 der europäischen Zahlungsdiensterichtlinie (ZDRL) auszulegen. Danach soll die oder der Betroffene zu den Zahlungsvorgängen alle notwendigen, ausreichenden und verständlichen Informationen erhalten. Dies ist jedoch schon dann gewährleistet, wenn nicht die IBAN-Daten mit der eingehenden Überweisung an die Zahlungsempfängerin bzw. den Zahlungsempfänger übermittelt werden, sondern lediglich Name, Kennung, Betrag und der angegebene Verwendungszweck der Auftraggeberin oder des Auftraggebers.

198 Art. 248 § 8 EGBGB

Banken sollten den Zahlungsempfängerinnen und Zahlungsempfängern nicht die IBAN der Überweisenden mitteilen.

9.7 Rechtswidrige Einmeldung in die Warndatenbank der Versicherungswirtschaft

Eine Versicherungsnehmerin beschwerte sich darüber, dass ihre Versicherungsgesellschaft sie in das Hinweis- und Informationssystem der Deutschen Versicherer (HIS) eingemeldet hat, da sie ihrer Sachversicherung drei Schadensfälle innerhalb von 24 Monaten gemeldet hatte. Das von der Informa HIS GmbH betriebene Informationssystem informiert die Versicherer über erhöhte Risiken, dort eingemeldete Versicherte haben Schwierigkeiten, in der betroffenen Sparte mit einer anderen Versicherung noch einen Vertrag abzuschließen; zumindest ist mit Prämienaufschlägen zu rechnen. Die Beschwerdeführerin wurde in das HIS eingemeldet, obwohl zwei der drei gemeldeten Schadensfälle nicht versichert waren.

Bei der Einmeldung in das HIS muss eine Abwägung vorgenommen werden zwischen dem Interesse der Versicherungswirtschaft, sich vor erhöhten Risiken und Versicherungsbetrug zu schützen, und dem informationellen Selbstbestimmungsrecht der Betroffenen.[199] Auch wenn die DS-GVO bei der Einmeldung von Betroffenen in Auskunfteien grundsätzlich von Einzelfallprüfungen ausgeht, wird man bei Massenverfahren die Benutzung eines Kriterienkatalogs grundsätzlich akzeptieren müssen. Vorliegend hätte die Einmeldung aber nicht erfolgen dürfen, da zwar kriteriengemäß drei Schadensfälle gemeldet wurden, zwei dieser Fälle aber gar nicht versichert waren. Insbesondere sind Versicherungen nach der DS-GVO verpflichtet, bei Beschwerden von Betroffenen Einzelfallprüfungen vorzunehmen, auch wenn die Kriterien beachtet wurden.

Nach unserem Eingreifen hat die Versicherungsgesellschaft die Einmeldung löschen lassen.

199 Art. 6 Abs. 1 lit. f DS-GVO

Das HIS kann auch unter der DS-GVO weiter betrieben werden, es ist aber eine größere Berücksichtigung des Einzelfalls erforderlich.

9.8 Schwarze Liste einer Online-Bank

Ein ehemaliger Kunde einer Online-Bank wollte bei dieser erneut ein Konto eröffnen. Der Antrag wurde abgelehnt. Der Beschwerdeführer vermutete, dass die Online-Bank die Kontoeröffnung bei ehemaligen Kundinnen und Kunden generell ablehnt.

Die Bank hat eingeräumt, die Daten ehemaliger Kundinnen und Kunden weiter zu speichern, um eine schwarze Liste, eine Art Warndatei, zu führen, damit sie diesen Personen kein neues Konto zur Verfügung stellt. Die Bank begründet dies damit, dass sie nach dem Kreditwesengesetz (KWG)[200] verpflichtet sei, Sicherheitsmaßnahmen gegenüber geldwäscheverdächtigen Kundinnen und Kunden vorzunehmen. Derzeit seien sie leider nicht in der Lage, zwischen geldwäscheverdächtigen und nicht geldwäscheverdächtigen Betroffenen zu differenzieren, daher würden sie die erneute Kontoeröffnung von ehemaligen Kundinnen und Kunden durch die weitere Datenspeicherung und Durchführung eines Datenabgleichs verhindern.

Die Vorgehensweise der Bank ist rechtswidrig. Die Daten ehemaliger Kundinnen und Kunden sind zu löschen oder bei Vorliegen einer Aufbewahrungspflicht zu sperren. In eine Abgleichdatei zur Verhinderung einer neuen Bankverbindung dürfen nur Betroffene aufgenommen werden, die tatsächlich unter Geldwäscheverdacht stehen oder bei denen andere triftige Gründe vorliegen, eine erneute Bankverbindung abzulehnen.[201]

Die Bank hat ihren Fehler eingeräumt und will das Verfahren zeitnah umstellen. Wir haben trotzdem ein Ordnungswidrigkeitenverfahren eingeleitet.

Eine schwarze Liste für ehemalige Kundinnen und Kunden, gegen die keine Verdachtsmomente bestehen, ist rechtswidrig.

200 § 25 h KWG
201 Siehe Art. 6 lit. f DS-GVO

9.9 Datenübermittlung bei Videoidentifizierung

Aus der Praxis

Viele Neukundinnen und Neukunden von Banken möchten zur Kontoeröffnung nicht in eine möglicherweise weit entfernte Bankfiliale gehen; Online-Banken verfügen teilweise gar nicht mehr über Filialen. Um die Betroffenen nach den Vorgaben des Geldwäschegesetzes[202] zu identifizieren, arbeiten viele Banken mit Dienstleistern zusammen, die sich auf Videoidentifizierung mittels Smartphone spezialisiert haben. Eines dieser Unternehmen führt die Identifizierungen nur dann durch, wenn die Betroffenen darin eingewilligt haben, dass der Dienstleister die bei der Identifizierung angefallenen Daten auch für andere Vertragspartner (z. B. bei Abschluss eines Versicherungsvertrags) verwenden kann. Eine Bank hielt dies für problematisch und bat uns um Stellungnahme.

Verantwortlich für die Videoidentifizierung sind die geldwäschepflichtigen Banken, der Dienstleister ist demgegenüber Auftragsverarbeiter. Wenn dieser die bisherigen Fremddaten nunmehr für eigene Zwecke nutzen will, findet rechtstechnisch eine Datenübermittlung von der Bank an den Dienstleister statt. Da die weitergehende Nutzung der personenbezogenen Daten der Betroffenen (sog. Pooling) weder für den Bankvertrag noch für die Identifizierung erforderlich ist, ist die Einwilligung der Betroffenen unfreiwillig und damit rechtswidrig.[203] An dieser Wertung ändert sich auch nichts dadurch, dass Betroffene der Weiternutzung ihrer Daten schon während des Identifizierungsprozesses widersprechen können. Auch können Betroffene nicht darauf verwiesen werden, das Post-ident-Verfahren durchzuführen, da dieses gegenüber dem von den Betroffenen gewünschten Verfahren umständlicher und zeitaufwendiger ist.

Die Datenschutz-Grundverordnung hat die Anforderungen an die Freiwilligkeit von Einwilligungen erhöht. Eine Videoidentifizierung darf nicht davon abhängig gemacht werden, dass Betroffene in die Weiternutzung ihrer Daten einwilligen.

202 § 11 GwG
203 Art. 7 Abs. 4 DS-GVO

10 Politische Parteien und das Abgeordnetenhaus von Berlin

10.1 Daten von Flüchtlingshelfenden auf NPD-Webseite

Der Berliner Landesverband der NPD veröffentlichte im Februar 2018 auf seiner Internetseite[204] eine mit Google Maps erstellte Karte von Einrichtungen für Asylsuchende in Berlin. Titel: „Eine Übersicht der Überfremdungsschwerpunkte in unserer Stadt". Jedem Standort waren Namen, Telefon- und Handynummern sowie E-Mail-Adressen dort tätiger Personen beigefügt. Der Begleittext erläuterte, dass sich nunmehr jeder darüber informieren könne, „welche interessanten ungebetenen Gäste sich in Ihrer Nachbarschaft tummeln, wer für Überfremdung unserer Heimat verantwortlich ist, wer finanziell an den Hunderttausenden Migranten Profit erzielt und an wen Sie sich wenden können, wenn Sie eine Beschwerde direkt vor Ort entrichten wollen". Alle Daten stammten aus öffentlichen Quellen.

Das für den Kartendienst Google Maps verantwortliche Unternehmen Google gab an, die Karte aufgrund von Verletzungen der eigenen Richtlinien gesperrt zu haben.[205] Jedoch war es möglich, den Quellcode auszulesen und so die in der Karte hinterlegten personenbezogenen Daten weiterhin sichtbar zu machen.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit dies durch Gesetz erlaubt ist oder die Betroffenen eingewilligt haben.[206] Die Veröffentlichung der personenbezogenen Daten war hier rechtswidrig. Die betroffenen Personen haben keine Einwilligung erteilt. Die Verwendung war

204 https://www.npd-berlin.de/asylheimkarte-berlin2018/

205 https://www.welt.de/politik/deutschland/article173227076/NPD-veroeffentlicht-auf-Google-Maps-Karte-mit-Asylunterkuenften.html

206 § 4 Abs. 1 BDSG a. F.

auch nicht nach § 28 Abs. 1 Nr. 3 BDSG a. F. erlaubt. Danach war die Verarbeitung von allgemein zugänglichen Daten rechtmäßig, sofern die verantwortliche Stelle dadurch berechtigte Interessen verfolgte und eine Interessenabwägung ergab, dass keine schutzwürdigen Interessen der betroffenen Personen überwogen. Personen, die im Bereich der Flüchtlingshilfe tätig sind, haben jedoch ein erhebliches Interesse daran, dass ihre Daten nicht auf einer Webseite mit fremdenfeindlichen Inhalten veröffentlicht werden („ungebetenen Gäste", „Überfremdung unserer Heimat"). Die betroffenen Personen wurden gezielt für Flüchtlingsgegnerinnen und -gegner sichtbar gemacht. Diese schutzwürdigen Belange der betroffenen Personen überwiegen hier eindeutig gegenüber etwaigen Interessen der NPD an der Veröffentlichung dieser Daten.

Indem die Daten mittels Einsehen des Quellcodes weiterhin sichtbar gemacht werden können, dauert der rechtswidrige Zustand an. Wir haben die NPD Berlin aufgefordert, die o. g. personenbezogenen Daten endgültig von der Webseite zu löschen und den Vorgang an unsere Sanktionsstelle abgegeben.

10.2 Wahlkampf mithilfe der Deutschen Post

Die CDU und die FDP haben im zurückliegenden Bundestagswahlkampf das Produkt „Wähleransprachen mit Parteiaffinität" der Deutsche Post Direkt GmbH genutzt. Das Produkt ermöglicht die Anzeige wahlkreisbezogener sog. Cluster (Gruppen von Gebäuden), deren Bewohnerinnen und Bewohner über eine (auf einer Skala von 1–10 einstellbare) Mindestaffinität für die jeweilige Partei verfügen, sodass Straßenzüge, die einen hohen Wert aufweisen, für den Haustürwahlkampf herangezogen werden können. Eine weitere Funktion weist wahlkreisbezogen auch einzelne Gebäude aus, die über eine bestimmte Mindestaffinität für die jeweilige Partei verfügen.

Die Daten, die den Parteien bei der Nutzung des Produkts zugänglich gemacht werden, sind nicht personenbezogen. Zwar handelt es sich bei der Parteiaffinität auf einer Skala von 1-10 um einen Score-Wert, der auch Aussagen zu politischen Meinungen, d. h. zu besonderen Arten personenbezogener Daten,[207] ermöglicht.

207 § 3 Abs. 9 BDSG a. F.

Dieser Score-Wert ist jedoch vorliegend keiner konkreten Person zugeordnet, sondern Gebäuden. Diese Zuordnung ist daher vergleichbar mit regulären Geodaten, die in der Regel ebenfalls gebäude- bzw. grundstücksbezogen zugeordnet werden. Bei Geodaten gehen wir bei einer Aggregierung von mindestens vier Haushalten davon aus, dass die Daten so stark vergröbert sind, dass schutzwürdige Interessen bei der Verarbeitung nicht beeinträchtigt werden.[208] Im vorliegenden Fall werden mindestens fünf bis sechs Haushalte in einem Cluster zusammengezogen. Sowohl die Darstellung in der Kartenansicht als auch die Teiladressierung per Postwurf erfolgt nur gebäudebezogen, sodass die Daten nochmals vergröbert werden.

Die CDU und die FDP haben das Produkt „Wähleransprachen mit Parteiaffinität“ datenschutzkonform genutzt.

10.3 Initiative „Neutrale Schule“ der AfD-Fraktion

Mit der Initiative „Neutrale Schule Berlin“ machte die AfD-Fraktion in Berlin Schlagzeilen. Auf ihrer Internetseite schaltete die Fraktion das Online-Portal „Neutrale Schule in Berlin“ frei und veröffentlichte dort ein Meldeformular, mit welchem Berichte über mutmaßliche Verstöße gegen das Neutralitätsgebot an die Fraktion gesendet werden können. Die AfD-Fraktion bezeichnet ihre Initiative als Hilfsangebot und bietet an, die gemeldeten Vorgänge „unter Wahrung der Persönlichkeitsrechte“ an die Schulbehörde zur Überprüfung weiterzuleiten. Ähnliche Initiativen wurden auch von weiteren Fraktionen der AfD in verschiedenen Landesparlamenten ins Leben gerufen.

Seit Freischaltung der Initiative erreichen uns viele Anfragen der Presse, von Politikerinnen und Politikern sowie von Eltern, Lehrerinnen und Lehrern und anderen Bürgerinnen und Bürgern, die datenschutzrechtliche Bedenken gegen diese Initiative geltend machen. Teilweise handelt sich dabei um allgemeine Hinweise, teilweise schildern Personen, dass sie die AfD-Fraktion um Auskunft gebeten hätten,

208 Dies entspricht den Verhaltensregeln „GeoBusiness und Datenschutz“, die von den Datenschutzbehörden im Jahre 2015 gebilligt und vom damaligen BlnBDI genehmigt wurden.

ob diese im Rahmen der Initiative personenbezogene Daten von ihnen gespeichert habe, und darauf keine Reaktion erhalten hätten.

Nach dem neuen Berliner Datenschutzgesetz sind Fraktionen ebenso wie das Abgeordnetenhaus und dessen Mitglieder nicht dem Geltungsbereich des Gesetzes unterworfen, soweit sie zur Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten.[209] Damit ist unsere Zuständigkeit als Aufsichtsbehörde für diese Bereiche ausgeschlossen.

Hintergrund für diese Einschränkung ist, dass es die verfassungsrechtliche Gewaltenteilung nicht ohne Weiteres erlaubt, dass Datenschutzaufsichtsbehörden als Teil der ausführenden Gewalt (Exekutive) die Einhaltung datenschutzrechtlicher Bestimmungen der gesetzgebenden Gewalt (Legislative) kontrollieren. Parlamente einschließlich ihrer Organe und Abgeordnete unterliegen daher bei Ausübung parlamentarischer Aufgaben nur dann datenschutzrechtlichen Regelungen und der Aufsicht der Aufsichtsbehörde, wenn sich dies aus einer klaren gesetzlichen Regelung ergibt.

Der Begriff „Wahrnehmung parlamentarischer Aufgaben“ ist zudem weit zu verstehen. Lediglich Verwaltungstätigkeiten wie etwa das Anmieten von Büros, das Einstellen von Mitarbeiterinnen und Mitarbeitern, der Bezug von Büromaterial etc. fallen nicht darunter und bleiben damit im Anwendungsbereich des Berliner Datenschutzgesetzes.[210] Jegliche politisch-inhaltliche Arbeit einer Fraktion hingegen ist hiervon ausgenommen. Wir konnten das Online-Portal daher weder prüfen noch in den Fällen konkreter Beschwerden tätig werden.

Seit Längerem schon empfehlen wir dem Berliner Abgeordnetenhaus, sich für die parlamentarische Arbeit selbst eine Datenschutzordnung zu geben und darin auch Datenschutzrechte für betroffene Personen zu regeln. Eine solche Datenschutzordnung existiert bspw. bei der Hamburger Bürgerschaft schon seit dem Jahre 1999. Dort ist u. a. der Anspruch für betroffene Personen festgeschrieben, Auskunft über ihre personenbezogenen Daten verlangen zu können, die im Rah-

209 Siehe § 2 Abs. 3 BlnDSG

210 Begründung zu § 2 Abs. 3 BlnDSG, Drs. 18/1033 des Berliner Abgeordnetenhauses, S. 71

men der parlamentarischen Arbeit von Fraktionen in der Hamburger Bürgerschaft gespeichert werden.[211]

Das Berliner Abgeordnetenhaus hat sich bislang nicht durch die Schaffung einer Datenschutzordnung verpflichtet. Diese Lücke sollte das Abgeordnetenhaus, unabhängig von der Initiative „Neutrale Schule", unverzüglich schließen, um rechtsfreie Räume zu verhindern.

10.4 Übermittlung personenbezogener Daten bei Schriftlichen Anfragen

Für den Senat stellt sich immer wieder die Frage, ob und inwieweit im Rahmen der Beantwortung von Schriftlichen Anfragen einzelner Abgeordneter personenbezogene Daten weitergegeben werden dürfen. Die Voraussetzungen hierfür regelte in der Vergangenheit explizit das Berliner Datenschutzgesetz[212]. Diese Vorschrift ist in der Neufassung des Gesetzes ersatzlos weggefallen.

Das Recht eines jeden Abgeordneten, sich mit Schriftlichen Anfragen an den Senat zu wenden, ist als Mittel der parlamentarischen Kontrolle ein hohes Gut und entsprechend auch in der Berliner Verfassung[213] verankert.

In der Regel lassen sich Schriftliche Anfragen beantworten, ohne dass dabei datenschutzrechtliche Belange berührt werden. Anders sieht es aber z. B. aus, wenn Abgeordnete mit ihrer Anfrage gerade das Ziel verfolgen, Einzelpersonen betreffende Sachverhalte oder sogar konkrete Namen in Erfahrung zu bringen[214]. In diesen Fällen ist zu entscheiden, ob sich die Weitergabe von Informationen mit dem informationellen Selbstbestimmungsrecht der betroffenen Personen vereinbaren lässt.

211 § 9 der Datenschutzordnung der Hamburger Bürgerschaft vom 19. Oktober 1999, in der Fassung vom 18. Mai 2018; abrufbar unter https://www.hamburgische-buergerschaft.de/recht/

212 § 20 Abs. 1 BlnDSG a. F.

213 Art. 45 Abs. 1 Verfassung von Berlin

214 Drs. 18/15244, 18/14847

Nach der bisherigen Regelung im Berliner Datenschutzgesetz war die Übermittlung von personenbezogenen Daten dann möglich, wenn – vereinfacht gesagt – das schutzwürdige Interesse der betroffenen Person der Übermittlung nicht entgegenstand.[215] Nach der Novellierung des Gesetzes im Juni 2018 findet sich im neuen Gesetz keine entsprechende Vorschrift mehr.

Das heißt jedoch nicht, dass den Abgeordneten nunmehr gar keine personenbezogenen Daten mehr übermittelt werden dürfen. Vielmehr räumt die Verfassung den Abgeordneten sogar das Recht ein, sich unmittelbare Kenntnis von Akteninhalten der Verwaltung zu verschaffen.[216] Dieses Recht ist seiner Natur nach damit sogar weitgehender. Die Akteneinsicht kann nur verwehrt werden, soweit öffentliche oder private Interessen an der Geheimhaltung dies zwingend erfordern.

Die Übermittlungsbefugnis fortan direkt auf die Verfassung zu stützen, sollte trotzdem nur eine Übergangslösung sein. Denn nach den Regelungen der DS-GVO muss für natürliche Personen Transparenz bestehen, wie ihre Daten verarbeitet werden.[217] Dies ist derzeit nicht ohne Weiteres gewährleistet. Jedenfalls aber ist bei der im jeweiligen Einzelfall zu treffenden Abwägungsentscheidung maßgeblich zu berücksichtigen, dass die Antworten des Senats auf Schriftliche Anfragen auch veröffentlicht werden.[218] Das ist ein bedeutender Unterschied zur persönlichen Akteneinsicht der Abgeordneten und dürfte nicht selten zu dem Ergebnis führen, dass die Geheimhaltungsinteressen der betroffenen Personen hier überwiegen.

Der Gesetzgeber ist gefordert, eine klare Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten im Rahmen von Schriftlichen Anfragen zu schaffen, die sowohl den verfassungsmäßigen Rechten der Abgeordneten als auch dem Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen Rechnung trägt.

215 Siehe im Einzelnen § 20 Abs. 1 Satz 2 BlnDSG a. F. i. V. m. § 28 Abs. 1 Satz 1 Nr. 2, Nr. 3 BDSG a. F.

216 Art. 45 Abs. 2 Verfassung von Berlin

217 Siehe Art. 5 Abs. 1 lit. b DS-GVO und Erwägungsgrund 42 Satz 2 DS-GVO

218 § 50 Abs. 1 Geschäftsordnung des Abgeordnetenhauses von Berlin

11 Aus der Arbeit der Sanktionsstelle

11.1 Entwicklung der Ordnungswidrigkeitenverfahren

Durch die neuen datenschutzrechtlichen Regelungen haben sich einige Änderungen in der Sanktionspraxis ergeben. Insbesondere wurden der Bußgeldrahmen erweitert und die Anzahl der Bußgeldtatbestände erhöht.[219]

In einigen Fällen in unserer Sanktionspraxis waren schon die neuen Bußgeldvorschriften zugrunde zu legen, obwohl die Taten vor Inkrafttreten der neuen Bestimmungen begangen wurden. Zwar gilt nach dem Gesetzlichkeitsprinzip grundsätzlich, dass eine Tat nur dann sanktioniert werden kann, wenn die Strafbarkeit gesetzlich bestimmt war, bevor die Tat begangen wurde.[220] Eine Ausnahme von diesem Grundsatz bildet jedoch das sog. Prinzip der Meistbegünstigung im Ordnungswidrigkeitenrecht.[221] Ändert sich das Gesetz zwischen Beendigung der Tat und der Entscheidung, gilt gemäß dem Prinzip der Meistbegünstigung das mildeste Gesetz. Zwar bedeutet die Anwendbarkeit der DS-GVO, insbesondere vor dem Hintergrund des erweiterten Bußgeldrahmens, in den meisten Fällen für den Täter keine Milderung, sondern eine Verschärfung der Bußgeldandrohung. Eine Ausnahme findet sich jedoch im neuen Berliner Datenschutzgesetz. Die unbefugte Verarbeitung nicht offenkundiger personenbezogener Daten war nach dem alten Berliner Datenschutzgesetz eine Straftat. Nach dem neuen Berliner Datenschutzgesetz ist dieses Verhalten nunmehr eine Ordnungswidrigkeit und damit im Ergebnis die mildere Vorschrift. Strafbar ist ein solches Verhalten jedoch auch weiterhin dann, wenn der Täter gegen Entgelt oder in Schädigungs- oder Bereicherungsabsicht handelt.[222]

219 JB 2016, 1.2.4
220 Art. 103 Abs. 2 GG
221 § 4 Abs. 3 OWiG
222 § 32 BlnDSG a. F. - § 29 Abs. 1 und 2 BlnDSG; § 70 BlnDSG

11.2 Unbefugte Datenerhebungen aus der Polizeidatenbank POLIKS

Aufgrund der vorgenannten neuen Bußgeldbestimmungen im Berliner Datenschutzgesetz haben wir nunmehr auch Ordnungswidrigkeiten über unberechtigte Zugriffe auf die Polizeidatenbank POLIKS zu bearbeiten.[223] In dieser Datenbank werden sowohl Vorgangsdaten als auch Daten von Beschuldigten, Straftätern, Tatverdächtigen, Betroffenen sowie Daten von Opfern und Zeugen erfasst und gespeichert; darunter Namen, Geburtsdaten, Anschriften und Familienstand. Die Datenbank dient den Dienstkräften der Polizei als Informationssystem und soll Schnellauskünfte zu Personen, Sachen, Institutionen und Vorgängen durch gezielte Anfragen bzw. Recherchen ermöglichen.

Der Zugang zu POLIKS wird aber immer wieder auch dazu missbraucht, Freunde, Familie, Nachbarn oder Dritte und deren Lebensumstände auszuspionieren. In diesem Jahr stellten wir in solchen Fällen nach der alten Rechtslage 14 Strafanträge und leiteten nach den neuen Vorschriften bereits fünf Bußgeldverfahren ein. Die uns vorliegenden Fälle betrafen ausschließlich unbefugte Zugriffe auf die Datenbank von POLIKS durch Mitarbeiterinnen und Mitarbeiter der Polizei.

In technischer Hinsicht können alle Polizistinnen und Polizisten auf POLIKS zugreifen. In rechtlicher Hinsicht ist eine Datenabfrage jedoch nur zulässig, wenn sich diese auf einen Vorgang bezieht, für den die oder der Abfragende zuständig ist. Jede Abfrage ohne dienstlichen Bezug ist unzulässig. Bedienstete der Polizei werden in regelmäßigen Abständen über datenschutzrechtliche Vorschriften informiert. Es ist ihnen ausdrücklich untersagt, Daten aus POLIKS und anderen polizeilichen Informationssystemen für private Zwecke oder aus privatem Interesse abzurufen.

Unbefugte Zugriffe auf POLIKS werden von uns konsequent mit durchaus empfindlichen Bußgeldern geahndet.

223 Bisher wurden derartige Vorfälle zur Prüfung einer möglichen Strafbarkeit an die Staatsanwaltschaft abgegeben.

11.3 Polizeibeamter warnt vor Razzien der Polizei

Gegen einen Polizeibeamten haben wir Strafantrag gestellt, weil er ohne dienstliche Veranlassung Daten aus dem Informationssystem POLIKS über geplante polizeiliche Maßnahmen, darunter auch Razzien, abrief und diese Informationen gegen Entgelt an Mitglieder aus dem kriminellen Milieu verkaufte.

Die Polizei informierte uns über einen Vorfall, der durch die Anzeige von Vertrauenspersonen des Landeskriminalamtes bekannt geworden war. Ermittlungen im Bereich der Drogenkriminalität ergaben, dass Drogendealer zur Vermeidung von Strafverfolgungsmaßnahmen Geldbeträge an Polizeibedienstete zahlten, um Informationen über polizeiliche Maßnahmen zu erhalten. Im Zuge der polizeilichen Ermittlungen stellte sich heraus, dass der beschuldigte Polizeibeamte über einen längeren Zeitraum und ohne dienstliche Veranlassung eine Vielzahl von Abfragen in der POLIKS-Datenbank zu den Personalien der Drogendealer vornahm, um so den jeweiligen Stand der Ermittlungen zu erfahren. Die auf diese Weise gewonnenen Erkenntnisse übermittelte der beschuldigte Polizeibeamte daraufhin gegen Entgelt an die Drogendealer. Neben dem Verdacht des Verstoßes gegen datenschutzrechtliche Bestimmungen bestand der Verdacht der gewerbsmäßigen Bestechlichkeit, der Verletzung von Dienstgeheimnissen und der Beteiligung am Betäubungsmittelhandel.

Die unbefugte Verarbeitung nicht offenkundiger personenbezogener Daten gegen Entgelt ist strafbar[224] und wird regelmäßig von uns bei der Berliner Staatsanwaltschaft zur Anzeige gebracht.

11.4 Zahnarztmitarbeiterin veröffentlicht das Schulzeugnis einer Praktikantin im Internet

Aus der Praxis

Gegen eine Mitarbeiterin einer Zahnarztpraxis haben wir Strafantrag bei der Staatsanwaltschaft Berlin gestellt, weil sie das Zeugnis einer Praktikantin im Internet veröffentlicht hatte.

224 § 29 Abs. 1, 2 BlnDSG

Im Zuge einer berufsvorbereitenden Ausbildungsmaßnahme hatte sich die Betroffene für eine Praktikumsstelle bei einer Zahnarztpraxis beworben. Unter ihren Bewerbungsunterlagen befand sich auch ihr Schulzeugnis, das sie der Zahnarztpraxis übersandte. Schon am ersten Tag ihres Praktikums äußerte sich eine Mitarbeiterin der Zahnarztpraxis gegenüber der Praktikantin abfällig über deren schulische Leistungen. In der darauffolgenden Zeit teilten Unbekannte der Betroffenen über Facebook mit, dass ihr Schulzeugnis abfotografiert, auf diversen Internetplattformen eingestellt worden und für jeden einsehbar sei.

Bewerbungsunterlagen können eine Vielzahl detaillierter Informationen über die Bewerberinnen und Bewerber enthalten, darunter auch sensitive Daten. Eine Veröffentlichung gegenüber Dritten – insbesondere im Internet – ohne rechtliche Grundlage ist unzulässig und kann mit einem Bußgeld geahndet werden. Eine Veröffentlichung in der Absicht, die betroffene Person zu schädigen, ist darüber hinaus strafbar.[225]

Die rechtsgrundlose Veröffentlichung von Beschäftigtendaten im Internet kann eine Straftat darstellen.

11.5 Strafantrag gegen einen Ausschussvorsitzenden des Abgeordnetenhauses von Berlin

Aus der Praxis

Gegen einen Abgeordneten des Abgeordnetenhauses von Berlin und zugleich Vorsitzenden des für Datenschutz zuständigen Fachausschusses haben wir Strafantrag[226] wegen rechtswidriger Datenverarbeitung gestellt, weil dieser Auszüge eines zuvor illegal veröffentlichten Haftbefehls auf dem Kurznachrichtendienst Twitter weiterverbreitet hatte.

Nachdem in einem Strafverfahren wegen einer tödlichen Messerattacke in Chemnitz ein Haftbefehl ergangen war, wurde dieser kurze Zeit später im Internet ver-

225 §§ 43 Abs. 2, 44 Abs. 1 BDSG a. F.
226 §§ 42 Abs. 2 Nr. 1, 44 BDSG a. F.

öffentlicht. Wie sich herausstellte, hatte ein Mitarbeiter der Justizvollzugsanstalt Dresden das Dokument abfotografiert und ins Internet gestellt. Den so veröffentlichten Haftbefehl verbreitete der Ausschussvorsitzende auf seinem Twitter-Account. Der Fall war aufgrund der Stellung des Betroffenen als Abgeordneter und als Vorsitzender des für Datenschutz zuständigen Parlamentsausschusses von besonderer Brisanz.

Die Veröffentlichung von Gerichtsakten, darunter Anklageschriften und Haftbefehle, ist nicht nur datenschutzrechtlich, sondern außerdem nach dem StGB strafbar.[227] Die mit der Weiterverbreitung des Haftbefehls veröffentlichten personenbezogenen Daten sind in hohem Maße schutzbedürftig. Zwar wurde der Twitter-Beitrag mit dem veröffentlichten Haftbefehl nach kurzer Zeit entfernt. Es ist jedoch nicht unwahrscheinlich, dass der Beitrag von Dritten auf Twitter und auf anderen Internetseiten weiterverbreitet wurde. Aufgrund der hohen Anzahl von Abonnentinnen und Abonnenten der Twitter-Beiträge des Abgeordneten ist von einem großen Empfängerkreis und damit von einer schwerwiegenden Verletzung der Persönlichkeitsrechte des Betroffenen auszugehen.

Mit der Veröffentlichung des Haftbefehls werden neben den Persönlichkeitsrechten des Betroffenen auch insbesondere dessen Justizgrundrechte verletzt. Dabei handelt es sich um Grundrechte, die den Einzelnen in Gerichtsverfahren schützen sollen. Dadurch soll die Unbefangenheit von Verfahrensbeteiligten, insbesondere von Laienrichtern und Zeugen, ebenso gewährleistet werden wie der Schutz der betroffenen Person vor Diskriminierung. Hierzu zählt auch die Aufrechterhaltung der bis zu einem rechtskräftigen Abschluss des Verfahrens zugunsten des Betroffenen bestehenden Unschuldsvermutung, die nicht durch Vorabveröffentlichungen amtlicher Schriftstücke gefährdet werden soll. Die Veröffentlichung ist darüber hinaus dazu geeignet, das Vertrauen der Allgemeinheit in die Strafrechtspflege zu beeinträchtigen.

Die Veröffentlichung eines Haftbefehls stellt eine schwere Persönlichkeitsrechtsverletzung dar. Von dem Vorsitzenden des für Datenschutz zuständigen Fachausschusses hätten wir hier mehr Zurückhaltung erwartet.

227 § 353d StGB

12 Telekommunikation und Medien

12.1 Bericht aus der Berlin-Group

Auch im Jahr 2018 traf sich die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (IWGDPT oder kurz Berlin-Group) zweimal unter dem Vorsitz der Berliner Beauftragten für Datenschutz und Informationsfreiheit.

Auf der Frühjahrstagung in Budapest am 9. und 10. April beschäftigte sich die Gruppe unter anderem mit Fragen der Privatsphäre und des Datenschutzes bei grenzüberschreitenden Datenanforderungen zu Strafverfolgungszwecken, insbesondere im Zusammenhang mit dem Zugriff auf Daten in einer Cloud. Die grenzüberschreitenden Auskunftsersuchen werfen komplizierte datenschutzrechtliche Fragen auf. Traditionelle Regelungen zur internationalen Koordinierung durch die Strafverfolgungsbehörden gelten mit Blick auf die zunehmende Häufigkeit und Komplexität grenzüberschreitender Datenanfragen als zu schwerfällig. Alternative Mechanismen, wie etwa freiwillige Vereinbarungen zwischen Anbietern und ausländischen Behörden, können unterschiedlichen und intransparenten Standards unterworfen sein. In dem in Budapest verabschiedeten Arbeitspapier zu Standards für den Datenschutz und den Schutz der Privatsphäre bei grenzüberschreitenden Datenanforderungen zu Strafverfolgungszwecken skizziert die Berlin-Group die aktuellen Entwicklungen in diesem Bereich und fordert die beteiligten Akteure dazu auf, bei der Förderung einer schnellen Bearbeitung legitimer grenzüberschreitender Datenanfragen die Interessen des Datenschutzes und der Privatsphäre stets zu wahren. Das Arbeitspapier gibt zudem Empfehlungen zu verbindlichen Standards.

Ebenfalls in Budapest verabschiedete die Berlin-Group das Arbeitspapier „Vernetzte Fahrzeuge“. Darin werden die verschiedenen Datenarten analysiert, die im Zusammenhang mit vernetzten Fahrzeugen erhoben, generiert, übermittelt und gespeichert werden. Fahrzeuge sind immer häufiger mit dem Internet verbunden und sammeln dabei unterschiedlichste Informationen, z. B. zum Verhalten

der Fahrerin oder des Fahrers oder über die Personen, die sich inner- oder außerhalb des Fahrzeugs aufhalten. Solche Daten können sowohl vom fahrzeugeigenen IT-System oder durch andere technische Geräte erhoben werden, die mit dem Fahrzeug verbunden sind,. Besonders viele Daten benötigen autonome Fahrzeuge, weshalb ihre Weiterentwicklung künftig auch weitere datenschutzrechtliche Fragen mit sich bringen wird. Das Arbeitspapier zeigt die Risiken für die Privatsphäre auf, die mit den unterschiedlichen Prozessen verbunden sind. Zudem beinhaltet es für alle relevanten Akteure Empfehlungen, wie diesen Risiken effektiv entgegengewirkt werden kann.

Am 29. und 30. November traf sich die Berlin-Group in Queenstown, Neuseeland. Der Sitzungsort in der südlichen Hemisphäre ermöglichte es vielen Interessentinnen und Interessenten aus dem asiatisch-pazifischen Raum, auch einmal persönlich an der Sitzung teilzunehmen. Der Termin war zudem so gewählt worden, dass die Sitzung der Berlin-Group unmittelbar vor dem in Wellington tagenden 50. APPA Forum[228] und dem sich dort anschließenden „International Privacy Forum" stattfand, sodass eine gegenseitige Teilnahme der Mitglieder der Berlin-Group und der des APPA-Forums an der jeweils anderen Sitzung möglich war. Diese Planung stellte sich als ausgesprochen sinnvoll und produktiv heraus. Gerade im Bereich der Telekommunikation spielen asiatische Länder eine wichtige Rolle, ihre Einbindung in die Berlin-Group, die bisher nur unbefriedigend erfolgt war, ist daher von nicht zu unterschätzender Bedeutung. Andererseits stieß die aktive Teilnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit und anderer Teilnehmerinnen und Teilnehmer der Berlin-Group an den Vorträgen und Diskussionen des APPA-Forums und des International Privacy Forums auf äußerst positive Resonanz. Die dortigen Teilnehmerinnen und Teilnehmer hatten aufgrund der internationalen Auswirkungen der DS-GVO ein lebhaftes Interesse an den ersten Erfahrungen mit der neuen europäischen Rechtsordnung.

In Queenstown verabschiedete die Berlin-Group ein Arbeitspapier zu Fragen des Datenschutzes im Zusammenhang mit künstlicher Intelligenz. Das Papier definiert verschiedene Begrifflichkeiten, die bei der Diskussion um die künstliche Intelligenz immer wieder eine Rolle spielen. Es beschreibt praktische Beispiele sowie Anwendungsszenarien für den Einsatz von künstlicher Intelligenz und gibt

228 Asia Pacific Privacy Authorities (APPA) Forum

einen detaillierten Überblick über die Herausforderungen für den Datenschutz und die Privatsphäre. Es beinhaltet zudem Empfehlungen im Hinblick auf die Einhaltung der Grundsätze des Datenschutzes für relevante Akteure.

Darüber hinaus verabschiedete die Berlin-Group ein Arbeitspapier zur weiträumigen Erfassung der Standorte von Personen im öffentlichen Raum. Die Ortung, d. h. die Fähigkeit moderner Technologien, die Bewegungen Einzelner zu verfolgen und aufzuzeichnen, ist ein Bereich, in dem sich das reale und das virtuelle Leben der Menschen treffen. Das Papier zeigt einerseits das Potenzial der Technologien zum Nutzen von Menschen auf, etwa wenn die Effizienz der Straßenbenutzung verbessert und damit die CO_2-Emissionen reduziert werden können oder wenn „Smart City"-Dienste z. B. die Effektivität und Kosteneffizienz öffentlicher Dienste, wie etwa im öffentlichen Nahverkehr, steigern können. Es setzt sich andererseits aber mit den Risiken für den Datenschutz und die Privatsphäre auseinander, da das Wissen über die Standorte von Personen nicht nur die Möglichkeit eröffnet, typische Bewegungsverläufe zu erkennen, sondern auch, Menschen zu beeinflussen. Es enthält sowohl Empfehlungen, die sich an die Akteure richten, die solche Mechanismen zur Standortverfolgung einsetzen bzw. die Möglichkeiten der Standortverfolgung in ihre Geräte integrieren (wie etwa Smartphone-Hersteller), als auch Empfehlungen, die sich an die Aufsichtsbehörden richten.

Beide Arbeitspapiere aus der Novembersitzung stehen noch unter dem Vorbehalt der endgültigen Annahme und werden dazu, wie in der Berlin-Group üblich, noch in ein schriftliches Umlaufverfahren gegeben. Die Papiere werden voraussichtlich Anfang 2019 auf unserer Webseite veröffentlicht. Die Papiere aus der Frühjahrssitzung in Budapest stehen dort bereits zum Abruf bereit.

12.2 ePrivacy-Verordnung: Keine Einigung im Europäischen Rat!

Bereits im Januar 2017 hatte die EU-Kommission einen Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation, die sog. ePrivacy-Verordnung, veröffentlicht.[229] Die Verordnung soll Vorgaben zum Schutz der Grundrechte und Grundfreiheiten natürlicher und juristischer Personen bei der Bereitstellung und Nutzung elektronischer Kommunikationsdienste mit unmittelbarer Geltung in den europäischen Mitgliedstaaten festlegen und dabei insbesondere die Rechte auf Achtung des Privatlebens und der Kommunikation sowie den Datenschutz in diesem Bereich in Europa neu regeln und weiter harmonisieren. Das Europäische Parlament hatte daraufhin im Oktober 2017 eine Verhandlungsposition zu dem Entwurf festgelegt und die Aufnahme interinstitutioneller Verhandlungen beschlossen. Nun fehlte nur noch die Positionierung des Europäischen Rates, um den sog. Trilog zu starten, d. h. um den Verordnungsentwurf auf europäischer Ebene zwischen Kommission, Parlament und Rat zu verhandeln und schließlich zu verabschieden. Bis heute konnte im Rat jedoch keine Einigung unter den Mitgliedstaaten erzielt werden, so dass das Gesetzgebungsverfahren nicht vorangekommen ist.

Im Europäischen Rat wird der Text des Verordnungsentwurfs in der zuständigen Ratsarbeitsgruppe „Telekommunikation und Informationsgesellschaft" verhandelt. Wie aus dem aktuellen Fortschrittsbericht des Vorsitzes der Arbeitsgruppe hervorgeht,[230] besteht nach wie vor Diskussionsbedarf zu den gesetzlichen Befugnissen zur Verarbeitung von elektronischen Kommunikationsdaten, zum Schutz von auf Endeinrichtungen der Nutzerinnen und Nutzer gespeicherten Informationen, zu den Voreinstellungen zur Privatsphäre sowie zur Frage, wer die Datenschutzaufsicht führen soll. Offenbar ist eine Reihe von Mitgliedstaaten der Auffassung, dass die Vorschriften stärker an die DS-GVO angeglichen werden müssen, indem die Verarbeitungsbefugnisse für Abwägungen und für die Verarbeitung zu anderen Zwecken geöffnet werden. In diesem Zusammenhang wird es für erforderlich gehalten, eine weitreichendere Verarbeitung von Kommunikationsmeta-

229 Siehe ausführlich zu dem Entwurf JB 2017, 1.4

230 Ratsdokument 14491/18 vom 23. November 2018

daten zu erlauben. Dies ist fragwürdig, da der Vorschlag der EU-Kommission zur ePrivacy-Verordnung darauf angelegt war, die DS-GVO für bestimmte Datenverarbeitungen im Bereich der elektronischen Kommunikation zu ergänzen, zu präzisieren und konkrete sowie vorrangige Spezialregelungen zu schaffen. Dieses Vorhaben wird ins Gegenteil verkehrt, wenn nun unspezifische Erlaubnistatbestände sowie Möglichkeiten zur weitreichenden zweckändernden Datenverarbeitung geschaffen werden.

Darüber hinaus streiten die Mitgliedstaaten über die Regelungen zur Nutzung von Online-Diensten und über die Frage, ob die Anbieter dieser Dienste die Möglichkeit haben sollten, den Besuch ihrer werbefinanzierten Webseiten für die Nutzerinnen und Nutzer unter die Bedingung zu stellen, dass diese das Webtracking zulassen. Hierbei handelt es sich um eine der Kernfragen der Verarbeitung von Nutzungsdaten im Internet, denn Nutzerinnen und Nutzer könnten auf diese Weise gezwungen werden, die Kontrolle über ihre Daten abzugeben, um sich im Internet bewegen zu können. Wenn der Zugang zu Webseiten von der Möglichkeit abhängig gemacht wird, die Aktivitäten der Nutzerinnen und Nutzer auf der Webseite und webseitenübergreifend detailliert zu verfolgen und die erhobenen Informationen an Dritte weiterzuverbreiten, dann bleiben nur wenige bis gar keine Möglichkeiten, im Netz noch frei darüber zu entscheiden, wie personenbezogene Daten verwendet werden bzw. wie diese Daten effektiv geschützt werden sollen. – Die Hoffnung bleibt, dass der Rat hier zu einer ausgewogenen, die Interessen der Nutzerinnen und Nutzer ausreichend berücksichtigenden Position kommen wird.

Die Verzögerungen im Rat führen dazu, dass ein Eintritt in die Trilog-Verhandlungen und eine Verabschiedung der ePrivacy-Verordnung vor den Europawahlen 2019 mehr als fraglich ist. Diese Situation ist nicht nur für die Nutzerinnen und Nutzer von elektronischer Kommunikation äußerst unbefriedigend, sondern auch für die Unternehmen und Organisationen, für die das hängende Gesetzgebungsverfahren erhebliche Rechtsunsicherheiten bringt.

12.3 Positionsbestimmung der Deutschen Datenschutzkonferenz: Telemediengesetz und Nutzungsdatenverarbeitung in Zeiten der DS-GVO

Im April hat die Deutsche Datenschutzkonferenz (DSK) eine Positionsbestimmung zur Anwendbarkeit des 4. Abschnitts des Telemediengesetzes für nicht öffentliche Stellen veröffentlicht.[231] Auslöser für diese Positionsbestimmung war die Verlautbarung der Bundesregierung, dass eine Anpassung des Telemediengesetzes nicht geplant sei. Die DSK sah es daher als geboten an, auf die entstehende Rechtsunsicherheit zu reagieren und sich zum Anwendungsvorrang der DS-GVO gegenüber dem Telemediengesetz zu positionieren.

Die ePrivacy-Verordnung ist, anders als von der EU-Kommission vorgesehen, nicht rechtzeitig fertig geworden.[232] Damit bleibt die bisherige Datenschutzrichtlinie für elektronische Kommunikation,[233] die durch die ePrivacy-Verordnung ersetzt werden sollte, zunächst in Kraft. Im Verhältnis zur DS-GVO können daher Vorschriften, die die bisher geltende Datenschutzrichtlinie für elektronische Kommunikation durch nationales Recht umsetzten,[234] nach wie vor vorrangig anzuwenden sein. So bestimmt es die DS-GVO im Rahmen einer sog. Kollisionsregel.[235] Dies kommt etwa für weite Teile des Telekommunikationsgesetzes in Betracht, welches Regelungen der Datenschutzrichtlinie für elektronische Kommunikation in deutsches Recht umsetzt.

231 „Zur Anwendbarkeit des Telemediengesetzes für nicht-öffentliche Stellen ab dem 25. Mai 2018", Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2018/2018-DSK-Positionsbestimmung_TMG.pdf

232 Siehe zum Stand des Gesetzgebungsverfahrens 12.1

233 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

234 Eine europäische Richtlinie gilt im Gegensatz zu einer europäischen Verordnung nicht unmittelbar und muss durch nationales Recht umgesetzt werden.

235 Siehe Art. 95 DS-GVO

Anderes gilt hingegen beim Telemediengesetz. Hier hatten die Aufsichtsbehörden bereits seit langer Zeit darauf hingewiesen, dass insbesondere die Vorschrift zum Setzen von Cookies[236] in der Datenschutzrichtlinie für elektronische Kommunikation nicht bzw. nicht vollständig in deutsches Recht umgesetzt wurde. Dementsprechend kommt die Kollisionsregel in der DS-GVO für das Telemediengesetz nicht zum Tragen. Nationale Regelungen können zwar darüber hinaus auch dann neben der DS-GVO erhalten bleiben, wenn eine Öffnungsklausel der DS-GVO dies erlaubt. Eine solche ist für die Regelungen des Telemediengesetzes jedoch nicht ersichtlich. Vor diesem Hintergrund unterfallen die Regelungen des 4. Abschnitts des Telemediengesetzes für nichtöffentliche Stellen dem Anwendungsvorrang der DS-GVO.

In der Praxis bedeutet dies, dass für die Verarbeitung der Daten von Nutzerinnen und Nutzern einer Webseite die DS-GVO anzuwenden ist. Datenverarbeitungen, die für die Bereit- und Darstellung der Webseite und zur Sicherung der Integrität der Webseite erforderlich sind, sowie bestimmte Verfahren der Webanalyse bzw. Reichweitenmessung werden im Rahmen einer Interessenabwägung regelmäßig zulässig sein. Sofern allerdings das Surfverhalten der Nutzerinnen und Nutzer webseitenübergreifend auch unter Einbindung von Dritten detailliert dokumentiert und verfolgt wird, ist eine Einwilligung der betroffenen Person erforderlich.[237]

Bereits zusammen mit der Positionsbestimmung hatte die DSK beschlossen, im Nachgang zu der Veröffentlichung der Position eine Konsultation mit der Wirtschaft durchzuführen. Im Rahmen eines Konsultationsverfahrens haben wir unsere Position gegenüber der Wirtschaft verdeutlicht und werden diese weiter konkretisieren.

Viele Webseiten entsprechen (noch) nicht den Anforderungen der DS-GVO. Dies betrifft z. B. die nach wie vor eingesetzten Cookie-Banner, die mangels Wahlmöglichkeit keine Einwilligung i. S. d. DS-GVO darstellen. Hier besteht weiterhin Anpassungsbedarf.

236 Siehe Art. 5 Abs. 3 der Richtlinie 2002/58/EG

237 Wir haben zur weiteren Erläuterung Hinweise zur Verarbeitung von Nutzungsdaten durch Webseiten und Blogs auf unserer Internetseite veröffentlicht, abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/hinweise-zur-verarbeitung-von-nutzungsdaten-durch-blogs-bzw-webseiten/

12.4 Fotos in Gefahr? Kunst-Urhebergesetz und DS-GVO

In der Öffentlichkeit wurde mit der Einführung der DS-GVO intensiv diskutiert, unter welchen Voraussetzungen die Veröffentlichung von Fotos rechtmäßig ist. Hintergrund ist, dass das Recht am eigenen Bild, d. h. die Befugnis zur Verbreitung, durch das sog. Kunst-Urhebergesetz[238] einfachgesetzlich ausgestaltet ist. Da die Verbreitung von Fotos regelmäßig aber auch eine Verarbeitung personenbezogener Daten darstellt, kommt jedenfalls außerhalb des familiär persönlichen Bereichs auch die DS-GVO als anwendbares Gesetz in Betracht.

In der öffentlichen Debatte spielten die Befürchtungen von Fotografinnen und Fotografen und Journalistinnen und Journalisten eine besonders große Rolle, weil diese durch die DS-GVO Beschränkungen ihrer künstlerischen Freiheit oder freien Berichterstattung befürchteten. Für diese Bereiche ist die DS-GVO jedoch in weiten Teilen nicht anwendbar. Werden personenbezogene Daten, also auch Fotos, im Rahmen der Meinungsfreiheit zu journalistischen, literarischen oder künstlerischen Zwecken verarbeitet, gilt in Berlin § 19 BlnDSG, der die DS-GVO weitestgehend verdrängt und auf das KunstUrhG verweist.

Sofern außerhalb dieser Bereiche die DS-GVO anzuwenden ist, muss die Veröffentlichung von Fotos auf eine Rechtsgrundlage nach Art. 6 DS-GVO gestützt werden. Liegt eine Einwilligung der abgebildeten Personen nicht vor, ist zu prüfen, ob ein anderer gesetzlicher Tatbestand die Veröffentlichung rechtfertigen kann. In Betracht kommt in diesem Zusammenhang die Regelung zur Interessenabwägung,[239] die eine Abwägung zwischen den berechtigten Interessen der bzw. des Verantwortlichen (also der Person, die die Fotos verwenden möchte) und den schutzwürdigen Interessen der betroffenen Personen (also der Abgebildeten) vorsieht. Im Rahmen dieser Abwägung spielen ähnliche Erwägungen eine Rolle, die auch im Rahmen des KunstUrhG Berücksichtigung finden. Konkret bedeutet dies, dass die berechtigten Interessen der Person, die die Fotos verwenden möchte,

238 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie – KunstUrhG

239 Siehe Art. 6 Abs. 1 lit. f DS-GVO

vorbehaltlich besonderer Umstände im Einzelfall z. B. dann überwiegen könnten, wenn es sich um Bilder aus dem Bereich der Zeitgeschichte, um Bilder von Personen als „Beiwerk" neben einer Landschaft oder sonstigen Örtlichkeit oder um Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen handelt. Wenn es sich um Fotos von Kindern handelt, ist allerdings zu berücksichtigen, dass hier regelmäßig ein Einverständnis der Kinder bzw. der Eltern erforderlich ist, da Kinder nach der DS-GVO als besonders schutzbedürftig gelten.

Für journalistische, literarische bzw. künstlerische Aktivitäten, die sich im Rahmen der Meinungs- und Informationsfreiheit bewegen, hat sich durch die Einführung der DS-GVO nicht viel geändert. Wesentliche Teile der DS-GVO sind in diesen Bereichen von der Anwendung ausgenommen. Dies gilt auch für die Veröffentlichung von Fotos.

12.5 Ein Scoring für Richterinnen und Richter

Aus der Praxis

Wir haben eine Eingabe zum Anlass genommen, die Internetplattform www.richterscore.de einer Vor-Ort-Prüfung zu unterziehen. Die Plattform möchte Rechtsanwältinnen und Rechtsanwälten einen Austausch über Richterinnen und Richter, Spruchkörper und Gerichte ermöglichen.

Die Plattformbetreiber sammeln und speichern personenbezogene Daten über die an den erfassten Gerichten tätigen Richterinnen und Richter. Bei den in Rede stehenden Daten handelt es sich um Angaben zur Spruchkörperzugehörigkeit (Titel, Name, Gericht und Spruchkörper), die aus den Geschäftsverteilungsplänen der Gerichte und damit aus öffentlich zugänglichen Quellen stammen. Außerdem handelt es sich um Bewertungen der Richterinnen und Richter sowie um Kommentare in Freitextfeldern. Die Bewertungen der Richterinnen und Richter können anhand einer Skala von bis zu fünf Sternen in den Kategorien Schnelligkeit, Vorbereitung, Hinweisbereitschaft, Objektivität und Rechtskenntnis abgegeben werden.

Auf unsere Intervention hin ist nicht mehr nur die Abgabe einer Bewertung, sondern auch schon die bloße Einsichtnahme in die gesammelten Daten ausschließ-

lich den auf der Plattform registrierten Rechtsanwältinnen und Rechtsanwälten möglich. So wird verhindert, dass die Inhalte von einer unbegrenzten Öffentlichkeit zu beliebigen Zwecken verwendet werden können. Gleichzeitig wurde unsere Forderung, auch den bewerteten Richterinnen und Richtern Zugang zu den über sie gespeicherten Bewertungen zu verschaffen, durch die Einrichtung eines speziellen Richterzugangs umgesetzt. Darüber hinaus konnten wir erreichen, dass immer auch die konkrete Anzahl der Bewertungen in den einzelnen Kategorien angezeigt wird, sodass eingeschätzt werden kann, ob die abgegebene Bewertung repräsentativ ist. Schließlich werden aufgrund unserer Empfehlung mittlerweile Wortfilter für die Kommentare in den Freitextfeldern eingesetzt, um diese auf etwaige Rechtsverstöße zu überprüfen.

Durch die Auflistung personenbezogener Daten sind die Richterinnen und Richter in ihrem Recht auf informationelle Selbstbestimmung tangiert. Die auf www.richterscore.de möglichen Bewertungen berühren dabei die Sozialsphäre, also den Bereich, in dem der Mensch sich privat oder beruflich im Austausch mit anderen Menschen befindet. Äußerungen in der Sozialsphäre können grundsätzlich nur beschränkt werden, wenn durch sie schwerwiegende Auswirkungen auf das Persönlichkeitsrecht zu befürchten sind. Das ist z. B. dann der Fall, wenn die Äußerung eine Stigmatisierung, soziale Ausgrenzung oder Prangerwirkung bewirken kann,[240] nicht jedoch bei den auf www.richterscore.de möglichen Bewertungen. Die auf dieser Plattform vorgegebenen Bewertungskriterien sind vorrangig objektiver Natur; die vorgenommene Bewertung gibt die jeweilige subjektive Meinung der Rechtsanwältin bzw. des Rechtsanwalts wieder. Folglich stellen sie Meinungsäußerungen i. S. d. Art. 5 Abs. 1 Satz 1 Grundgesetz (GG) dar. Aufgrund der Ausgestaltung der Bewertungskriterien ist eine unsachliche Schmähkritik eher unwahrscheinlich. Einzig in den Kommentaren wäre eine solche theoretisch möglich; dem wird aber mithilfe des nunmehr eingerichteten Wortfilters entgegengewirkt.

Auch der Umstand, dass die Bewertungen anonym abgegeben werden, kann keine Unzulässigkeit der auf www.richterscore.de erfolgenden Datenerhebung und -speicherung begründen. Die anonyme Nutzung ist dem Internet innewohnend. Eine Beschränkung der Meinungsäußerungsfreiheit auf Äußerungen, die einem

240 BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, Rn. 41 (sog. Spickmich-Urteil)

bestimmten Individuum zugeordnet werden können, ist nach der Rechtsprechung des BGH mit Artikel 5 Abs. 1 Satz 1 GG nicht vereinbar.[241]

Nach Umsetzung unserer Forderungen arbeitet die Plattform www.richterscore.de nun datenschutzkonform.

241 BGH, Urteil vom 23. Juni 2009 – VI ZR 196/08, Rn. 38

13 Informationsfreiheit

13.1 Informationsfreiheit in Deutschland

Nach jahrelangen vergeblichen Initiativen ist nun auch in **Hessen** der allgemeine Informationszugang gesetzlich normiert. Beide Rechtsbereiche, der Datenschutz und die Informationsfreiheit, wurden in ein und demselben Gesetz geregelt,[242] ein bundesdeutsches Novum. Nach dem hessischen Neuzugang sind noch drei Bundesländer, nämlich Bayern, Niedersachsen und Sachsen, ohne Informationsfreiheitsgesetze.

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)** verabschiedete auf Initiative der Informationsfreiheitsbeauftragten von Berlin, Bremen und Schleswig-Holstein mit großer Mehrheit ein Positionspapier zur Frage der Transparenz der Verwaltung beim Einsatz von Algorithmen.[243] Auch die öffentlichen Verwaltungen treffen zunehmend automatisierte Entscheidungen unter Zuhilfenahme von Algorithmen und Künstlicher Intelligenz (KI). Hieraus ergeben sich auch unter dem Gesichtspunkt der Informationsfreiheit Probleme, weil diese Verfahren weitgehend intransparent arbeiten und damit fraglich ist, inwieweit diese grundrechtskonform eingesetzt werden können. Die öffentliche Verwaltung ist zu gesetzmäßigem Handeln verpflichtet, ihre Entscheidungen müssen vorhersehbar und nachvollziehbar sein. Dies ist nur zu erreichen, wenn sichergestellt werden kann, dass die Verfahren durch ausreichende Transparenz und durch die technisch-organisatorische Gestaltung überprüfbar und beherrschbar sind. Die Transparenzanforderungen müssen schon bei der Programmierung beachtet werden („Transparency by Design"). Das Positionspapier beschreibt konkret die Pflichten der öffentlichen Stellen, bereits vor der Entscheidung über den Einsatz dieser Verfahren zu prüfen, ob dies jeweils grundrechtskonform möglich ist, denn

242 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG), GVBl. S. 82 ff.

243 Positionspapier vom 16. Oktober 2018: „Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar", abrufbar in deutscher und englischer Fassung unter www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-ifk/

nicht jede Datenverarbeitung ist erlaubt. Betont wird zudem die Aufgabe der öffentlichen Verwaltungen, für hinreichende Transparenz zu sorgen.

Außerdem hat die IFK eine Entschließung gefasst, mit der die Sozialleistungsträger aufgefordert werden, Verwaltungsvorschriften antragsunabhängig, zeitnah und benutzerfreundlich zu veröffentlichen.[244]

13.2 Informationsfreiheit in Berlin

13.2.1 Allgemeine Entwicklungen

Das Berliner Informationsfreiheitsgesetz (IFG) musste – anders als das Berliner Datenschutzgesetz (BlnDSG)[245] – nicht an den neuen europäischen Rechtsrahmen angepasst werden, da das neue Datenschutzrecht keinen Einfluss auf die materiell-rechtlichen Bestimmungen des IFG zur Offenbarung personenbezogener Daten hat.[246] Denn die Datenschutz-Grundverordnung (DS-GVO) erlaubt ausdrücklich die Offenlegung personenbezogener Daten in amtlichen Dokumenten, die sich zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe im Besitz einer Behörde oder einer öffentlichen oder privaten Einrichtung befinden.[247] Auch haben die EU-Mitgliedstaaten ausdrücklich die Befugnis zum Erlass besonderer Regelungen zur Verarbeitung personenbezogener Daten für Aufgaben, die im öffentlichen Interesse liegen.[248] Der gesetzlich normierte Zugang zu amtlichen Informationen nach dem IFG ist eine Aufgabe im öffentlichen Interesse. Die Verarbeitung (Offenlegung durch Übermittlung)[249] von personenbezogenen Daten ist auch des-

244 Entschließung vom 16. Oktober 2018: „Soziale Teilhabe braucht konsequente Veröffentlichung von Verwaltungsvorschriften!", abrufbar unter www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-ifk/

245 Siehe 1.7

246 § 6 IFG

247 Art. 86 DS-GVO, Erwägungsgrund 154

248 Art. 6 Abs. 1 lit. e, Abs. 2 und 3 DS-GVO

249 Art. 4 Nr. 4 DS-GVO

halb zulässig,[250] weil sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt.[251]

Die DS-GVO hat die Informationsfreiheit in Berlin allerdings mittelbar beeinflusst. Bislang sind die Aufgaben und Befugnisse der Berliner Beauftragten für Informationsfreiheit im IFG durch Verweis auf die Regelungen im „alten" BlnDSG normiert. Da es diese Regelungen nicht mehr gibt, geht der Verweis nunmehr ins Leere. Wir haben deshalb gegenüber der federführenden Senatsverwaltung für Inneres und Sport die erforderliche Änderung des IFG vorgebracht und mit einem konkreten Vorschlag angeregt, die jeweils anwendbaren Regelungen aus dem „alten" BlnDSG unmittelbar in das IFG zu übernehmen. Hierzu gehören insbesondere das Recht zur Beanstandung[252] und die Unterstützungspflicht öffentlicher Stellen.[253]

Die Herauslösung der Befugnisse der Beauftragten für Informationsfreiheit aus dem BlnDSG ist nicht nur aus Gründen der Praktikabilität, sondern auch wegen der eigenständigen Bedeutung der Informationsfreiheit sachgerecht. Dafür spricht auch, dass die Informationsfreiheitsbeauftragten – anders als die Datenschutzbeauftragten – primär als Schlichtungsstellen sowie beratend gegenüber antragstellenden Personen und den informationspflichtigen Stellen tätig werden, sodass die neuen Aufgaben und Befugnisse als Datenschutzbeauftragte nach der DS-GVO nicht ohne Weiteres auf die Informationsfreiheitsbeauftragten übertragen werden können.

Es bleibt zu hoffen, dass die entsprechende Änderung des IFG wenn nicht kurzfristig, dann doch spätestens im Rahmen eines Transparenzgesetzes berücksichtigt wird. Denn laut Koalitionsvereinbarung soll das IFG in Richtung Transparenzgesetz weiterentwickelt werden; ein Entwurf – so die Planung der Senatsverwaltung für Inneres und Sport – soll im Laufe des Jahres 2019 ins Abgeordnetenhaus eingebracht werden. Hierfür und zum Austausch der bisherigen Erfahrungen mit

250 Art. 6 Abs. 1 lit. c DS-GVO
251 §§ 2, 6 IFG
252 § 26 BlnDSG a. F.
253 § 28 BlnDSG a. F.

dem IFG hat sie eine Arbeitsgruppe eingerichtet. Wir haben der Arbeitsgruppe unsere Mitarbeit angeboten.

13.2.2 Einzelfälle

Herausgabe von Richterdaten durch die Justizverwaltung?

Die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung hat uns um eine Einschätzung gebeten, wie mit dem Widerspruch gegen den zurückgewiesenen Auskunftsantrag der Betreiber des Bewertungsportals unter www.richterscore.de umzugehen sei. Die Plattform möchte Rechtsanwältinnen und Rechtsanwälten einen Austausch über Richterinnen und Richter, Spruchkörper und Gerichte ermöglichen. Zu den begehrten Daten gehörten der Name, die jeweilige Funktion sowie der jeweilige Tätigkeitsanteil beim Gericht. Wir haben der Senatsverwaltung empfohlen, dem Widerspruch abzuhelfen.[254]

Diesem Ergebnis lagen folgende Bewertungen zugrunde: Soweit keine Einwilligung der betroffenen Richterinnen und Richter vorliegt, ist Rechtsgrundlage für die Übermittlung der begehrten Daten § 3 Abs. 1 Satz 1 IFG. Der Anspruch ist nicht nach § 6 Abs. 1 IFG ausgeschlossen oder eingeschränkt. Denn der Offenbarung der personenbezogenen Daten stehen schutzwürdige Belange der Betroffenen nicht entgegen. Dies galt nicht nur für diejenigen Daten, für die nach den Regelbeispielen des § 6 Abs. 2 Satz 1 Nr. 1 lit. a und Nr. 2 IFG schutzwürdige Belange der Betroffenen in der Regel nicht entgegenstehen, sondern auch für weitergehende Daten wie z. B. die Angaben, zu welchem Anteil die Betroffenen bei welchem Gericht tätig sind. Der Rechtsgedanke der vorgenannten Regelungen sollte in die Entscheidung über den Widerspruch zumindest mit einfließen.

Das Informationsinteresse der Antragsteller war nachvollziehbar und als solches – angesichts von inzwischen gängigen und vergleichbaren Angeboten zu Ärzten – nicht per se zu verneinen. Dem Informationsinteresse stand auch nicht entgegen, dass die Antragsteller damit auch wirtschaftliche Interessen verfolgten. Denn das IFG bietet für eine solche Beschränkung keine Anhaltspunkte; vielmehr lässt es

254 Siehe auch 12.5 (datenschutzrechtliche Bewertung der Plattform)

gerade die freie Weiterverwendung der erlangten Informationen zu, wie sich nicht zuletzt aus der Aufhebung von § 13 Abs. 7 und § 22 IFG ergab, die im Jahr 2015 vor dem Hintergrund der Europäischen Richtlinie zur Weiterverwendung von Informationen des öffentlichen Sektors erfolgt war. Die aufgehobenen Bestimmungen hatten die Nutzung der erlangten Informationen zu gewerblichen Zwecken als bußgeldbewehrtes Verbot normiert.

Geheimhaltungsinteressen der betroffenen Richterinnen und Richter hatte die Senatsverwaltung nicht angeführt und waren auch für uns nicht ersichtlich. Die nach § 6 Abs. 1 IFG vorzunehmende, aber bislang unterbliebene Interessenabwägung konnte also nicht zulasten der Antragsteller ausfallen.

Die Senatsverwaltung hat den Widerspruch gleichwohl zurückgewiesen und den Informationszugang schließlich unter Berufung auf den „unverhältnismäßigen Verwaltungsaufwand" abgelehnt, der mit der erforderlichen Auswertung von ca. 1600 Personalvorgängen einherginge. Elektronisch seien die begehrten Daten nicht vorhanden.

Wir haben die Betreiber der Plattform darin bestärkt, die Angelegenheit verwaltungsgerichtlich klären zu lassen.

Elektronischer Antrag und Gebührenvorauszahlung beim AG Wedding

Ein Petent bat uns um Unterstützung, weil er auf seine beiden elektronischen IFG-Anträge beim AG Wedding keine zufriedenstellende Auskunft erhalten habe. Er hatte eine Liste mit allen im Amtsgericht vorhandenen Kunstwerken mit Künstler- und Werknamen, Anschaffungsjahr und Wert erbeten. Ein weiterer Antrag betraf Abschriften aller im Jahr 2018 beim Amtsgericht eingereichten schriftlichen Beschwerden und Dienstaufsichtsbeschwerden. Das AG Wedding habe beide Anträge unter Hinweis darauf zurückgewiesen, dass per E-Mail kein kostenauslösender Antrag gestellt werden könne. Auch habe das Amtsgericht mitgeteilt, dass es beabsichtige, die für die Auskunftserteilung anfallenden Kosten „im Vorschusswege zu erheben".

In beiden Fällen handelte es sich um nach dem IFG zulässige Auskunftsanträge. Denn der Anwendungsbereich des Gesetzes erstreckt sich auch auf die Gerichte,

jedoch nur soweit sie Verwaltungsaufgaben erledigen.[255] Das war hier unstreitig der Fall. Allerdings war die Auffassung, dass ein IFG-Antrag nicht per E-Mail gestellt werden könne, nicht korrekt. Denn mit der letzten Änderung des IFG wurde ausdrücklich die Möglichkeit normiert, einen Antrag nicht nur mündlich oder schriftlich, sondern auch elektronisch zu stellen.[256] Dagegen hatte der Petent die Aussage, die Kosten ggf. im Vorschusswege zu erheben, als unzulässige Vorkasse missverstanden. Denn diese Bitte des AG Wedding war nur für den Fall geäußert worden, dass der Petent keine Postanschrift für die Zustellung des Gebührenbescheides angeben wollte.

Die Fälle waren gleichwohl Anlass für uns, auf die Rechtsprechung des Oberverwaltungsgerichts Berlin-Brandenburg zur Vorauszahlung einer Gebühr für den Informationszugang hinzuweisen.[257] Das OVG hatte deutlich gemacht, dass im Bereich des Informationszugangs eine gebührenpflichtige Amtshandlung nur ausnahmsweise von der vorherigen Entrichtung der Verwaltungsgebühr abhängig gemacht werden darf. Voraussetzung sei, dass Anhaltspunkte dafür vorhanden sind, dass ohne die Vorauszahlung das Haushaltsinteresse gefährdet wäre. Solche Anhaltspunkte lägen nicht schon dann vor, wenn der Verwaltungsaufwand für die Gewährung des Informationszugangs hoch sei und möglicherweise die nach dem einschlägigen Gebührenrahmen vorgesehene Höchstgebühr übersteige. Ein Kostenvorschussbescheid sei rechtswidrig, wenn eine Gefährdung des Haushaltsinteresses objektiv nicht erkennbar und die Bemessung der Gebühr allein an dem mit der Informationsgewährung verbundenen Verwaltungsaufwand ausgerichtet ist.

Mit der nun ausdrücklichen Möglichkeit der elektronischen Antragstellung ist im IFG ein kleiner, eigentlich selbstverständlicher Schritt in Richtung Digitalisierung getan. IFG-Bescheide, die pauschal und ohne Prüfung des Einzelfalls einen Kostenvorschuss verlangen, sind rechtswidrig.

255 § 2 Abs. 1 Satz 2 IFG

256 § 13 Abs. 1 Satz 1 IFG, geändert durch Gesetz vom 2. Februar 2018, GVBl. S. 160

257 OVG 12 B 22.12, Beschluss vom 26. Mai 2014

Sieg in Etappen im Bezirksamt Neukölln

Eine Petentin beschwerte sich bei uns darüber, dass sie in der Denkmalschutzbehörde des Bezirksamts Neukölln keine Akteneinsicht erhalte. Sie wolle die Umgestaltung insbesondere der Innenhöfe der unter Denkmalschutz stehenden „IDEAL-Passage“ nachvollziehen. Die Einsichtnahme in die Unterlagen des abgeschlossenen Verfahrens sei von der Vorlage einer Vollmacht der Baugenossenschaft (Eigentümerin) abhängig gemacht worden, was sie als Mieterin des denkmalgeschützten Gebäudes nicht nachvollziehen könne. Später wurde für die Akteneinsicht vor Ort eine Gebühr in Höhe von 40 Euro zuzüglich der Kosten für Kopien erhoben. Auch wurde mitgeteilt, dass auf Wunsch der Baugenossenschaft alle personenbezogenen Daten, Firmen- und Preisangaben anlässlich der Akteneinsicht geschwärzt würden. Nach unserer ersten Intervention hat die Denkmalschutzbehörde der Petentin kopierte Unterlagen mit Schwärzungen vorgelegt, ohne dass noch eine Vollmacht der Genossenschaft gefordert wurde.

Nach dieser ersten Akteneinsicht hat uns die Petentin erneut um Unterstützung gebeten, weil sie meinte, dass ihre Informationszugangsrechte durch das Amt nicht vollständig beachtet wurden. Wir hielten deshalb eine Sichtung der in Rede stehenden Akten vor Ort für sachgerecht. Grundsätzlich ist uns bei Vor-Ort-Prüfungen vor dem Hintergrund des IFG zunächst daran gelegen nachzuvollziehen, woraus der Original-Vorgang im Einzelnen besteht und welche Informationen hieraus aus welchem rechtlichen Grund der antragstellenden Person vorenthalten werden. Deshalb baten wir um Vorlage sowohl der Original-Akten als auch der der Petentin im Akteneinsichtstermin vorgelegten Kopien. Zudem baten wir darum, rechtzeitig zum Ortstermin die in den Kopien erfolgten Schwärzungen rechtlich zu begründen. Denn nach dem IFG sind grundsätzlich alle in Akten enthaltenen Informationen offenzulegen, es sei denn, es liegt ein einschränkender Tatbestand nach dem IFG vor.[258] Nur in diesem Fall durften Schwärzungen vorgenommen und durfte der Aufwand hierfür der Petentin in Rechnung gestellt werden. Ob alle Schwärzungen rechtlich erforderlich waren, war zweifelhaft.

Beim Abgleich des Original-Vorgangs mit den geschwärzten Kopien stellten wir fest, dass gesetzliche Gründe für die Nichtoffenlegung der zurückgehaltenen In-

258 §§ 4 ff. IFG

formationen nicht angeführt werden konnten. Bereits die umfassende Beteiligung der Abteilung Umwelt und Natur des Bezirksamts sprach dafür, dass es sich bei dem in Rede stehenden Vorgang insgesamt um „Umweltinformationen" handelte. Dieser Begriff ist nach der Rechtsprechung des Bundesverwaltungsgerichts weit auszulegen; eines unmittelbaren Zusammenhangs der einzelnen Daten mit der Umwelt bedarf es nicht.[259] Das Bezirksamt hat unsere Empfehlungen geprüft und der Petentin schließlich nach vier Monaten den gesamten Vorgang – noch dazu gebührenfrei –[260] zur Akteneinsicht zur Verfügung gestellt.

Durch eine Vor-Ort-Prüfung gelang es uns, der Petentin zu einer umfassenden und gebührenfreien Akteneinsicht zu verhelfen.

259 BVerwG, Urteil vom 23. Februar 2017 – 7 C 31.15

260 Nach § 18a Abs. 4 Satz 3 Nr. 1 IFG ist die Akteneinsicht in Umweltinformationen vor Ort gebührenfrei.

14 Aus der Dienststelle

14.1 Entwicklungen

Die ersten Erfahrungen nach dem Wirksamwerden der DS-GVO am 25. Mai 2018 bestätigen, dass dieses Datum tatsächlich als Zeitenwende für den Datenschutz insgesamt und für die aufsichtsbehördliche Tätigkeit der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) im Besonderen anzusehen ist.

Die öffentliche Debatte um das neue Regelwerk haben sowohl Bürgerinnen und Bürger als auch Behörden, Unternehmen und sonstige Einrichtungen für das Thema Datenschutz sensibilisiert. Der Umgang mit personenbezogenen Daten erfolgt seitdem in vielen Teilen der Gesellschaft bewusster. Die von einer Datenverarbeitung Betroffenen fordern zunehmend ihre Datenschutzrechte ein und bei den verantwortlichen Stellen setzt sich immer mehr die Erkenntnis durch, dass der Datenschutz bei der Einführung von neuen Verfahren oder Produkten bereits von Anfang an berücksichtigt werden muss, um so einen späteren technischen, finanziellen und bürokratischen Mehraufwand zu vermeiden.

Diese Entwicklung hat natürlich erhebliche Auswirkungen auf die aufsichtsbehördliche Praxis. Durch die immens gestiegene Anzahl von Eingaben, Beschwerden und Beratungsersuchen, die seit dem Wirksamwerden der DS-GVO an die BlnBDI gerichtet werden, ist der Arbeitsanfall in der gesamten Behörde nicht mehr zu bewältigen. Es können bei Weitem nicht mehr alle Anfragen sachgerecht beantwortet werden, erforderliche Prüfungen sind kaum noch machbar.

Besonders problematisch ist die Situation bei der Bearbeitung von Bürgereingaben. Das Aufkommen von Beschwerden hat sich im Vergleich zum Jahr 2017 nahezu vervierfacht. Allein durch die Vielzahl der (neu) eingehenden Beschwerden ist deren zeitnahe Bearbeitung grundsätzlich gefährdet. Dies ist insofern kritisch, als die Aufklärung, Prüfung und Bewertung von Beschwerdesachverhalten nicht selten zu weiteren ordnungsbehördlichen Maßnahmen führt. Eine zeitnahe Bearbeitung dieser Vorgänge ist daher für die aufsichtsbehördliche Tätigkeit der BlnBDI von zentraler und übergeordneter Bedeutung.

Die Zunahme an Beschwerden ist vor allem auch darauf zurückzuführen, dass sich der Zuständigkeitsbereich der BlnBDI erheblich erweitert hat. War die Behörde zuvor nur für die Bearbeitung von Beschwerden gegen Berliner Behörden und Unternehmen zuständig, hat die DS-GVO mit dem sog. Marktortprinzip die Zuständigkeit auf alle (nationalen und europäischen) Stellen erweitert, die den Berliner Bürgerinnen und Bürgern Waren und Dienstleitungen anbieten oder ihr Verhalten beobachten. Die Einführung des One-Stop-Shop-Prinzips[261] erfordert, dass bei allen eingehenden Beschwerden zunächst zu prüfen ist, ob ein grenzüberschreitender Bezug besteht. Ist dies der Fall, hat die BlnBDI als federführende Behörde alle Aufsichtsbehörden in der EU über die Beschwerde zu informieren und alle betroffenen Aufsichtsbehörden an dem Verfahren zu beteiligen. Geht bei einer der anderen europäischen Aufsichtsbehörden eine Beschwerde mit grenzüberschreitendendem Bezug ein und sind dabei die Rechte von Berliner Bürgerinnen und Bürgern betroffen, wirkt die BlnBDI an dem (europäischen) Prüfverfahren als „betroffene Behörde" mit.

Dadurch kommt es zu komplizierten, arbeits- und zeitintensiven Abstimmungsverfahren mit den anderen Aufsichtsbehörden, die zudem in englischer Sprache und unter strengen Fristen geführt werden müssen. Um diese neue Aufgabe bewältigen zu können, wurde die Servicestelle Europaangelegenheiten neu geschaffen. Die Abstimmung bei grenzüberschreitenden Sachverhalten erfolgt über das elektronische Binneninformationssystem (IMI). Die Anzahl der abstimmungsbedürftigen Fälle hat alle Erwartungen übertroffen. Seit dem Wirksamwerden der DS-GVO wurden im Jahr 2018 ca. 500 Fälle in das IMI eingestellt. Sämtliche Fälle wurden in der Servicestelle Europaangelegenheiten auf eine mögliche Betroffenheit der BlnBDI geprüft. In über 150 Fällen wurde eine Betroffenheit festgestellt, sodass sich die Behörde inhaltlich mit den jeweiligen Sachverhalten befassen musste.

Nach der DS-GVO können verantwortliche Stellen ihre Produkte und Dienste (freiwillig) datenschutzrechtlich zertifizieren lassen.[262] Die Zertifizierung kann durch akkreditierte Zertifizierungsstellen oder auch durch die zuständigen Aufsichtsbehörden erfolgen. Die Akkreditierung der Stellen wird von der Deutschen Ak-

261 Art. 56 DS-GVO
262 Art. 42 DS-GVO

kreditierungsstelle GmbH (DAkkS) zusammen mit den Aufsichtsbehörden vorgenommen. Für die Aufsichtsbehörden handelt es sich um einen vollkommen neuen Aufgabenbereich. Die Tätigkeit als Begutachterin bzw. Begutachter im Akkreditierungsverfahren erfordert ein umfangreiches rechtliches und technisches Spezialwissen. Entsprechende Kenntnisse und Kompetenzen waren bei den Aufsichtsbehörden bisher nicht vorhanden. Um sie zu erwerben, haben einzelne Beschäftigte der BlnBDI an Schulungen der DAkkS zu den Anforderungen an Zertifizierungsstellen teilgenommen. Nach Mitteilung der DAkkS lagen bis Mitte Oktober für Berlin bereits neun Interessenbekundungen für die Akkreditierung von Zertifizierungsstellen vor. Nur in Nordrhein-Westfahlen gab es zu diesem Zeitpunkt mehr Interessenbekundungen (12).

In den ersten fünf Monaten gingen bei der BlnBDI ca. 5.000 allgemeine Anfragen von Bürgerinnen und Bürgern, Unternehmen, Behörden, freiberuflich tätigen Personen, Vereinen, Verbänden etc. im Zusammenhang mit der Umsetzung der DS-GVO ein. Ein großer Teil der Beratungsersuchen erfolgte telefonisch. Um die Anfragen zu bewältigen, wurde von Juni bis einschließlich August 2018 eine Telefon-Hotline speziell für Fragen zur DS-GVO geschaltet. Über diese Hotline konnten die Bürgerinnen und Bürger, Unternehmen, Vereine und freiberuflich tätigen Personen täglich in der Zeit von 10:00 bis 13:00 Uhr ihre Fragen zur DS-GVO klären. In den drei Monaten, in denen die Hotline geschaltet war, gingen dort 2.164 Anrufe ein.

Seit dem Jahr 2017 bietet die Berliner Beauftragte für Datenschutz und Informationsfreiheit Start-up-Unternehmen spezielle Sprechstunden an, um die Entwicklung von Start-up-Unternehmen am Standort Berlin zu unterstützen. Insgesamt wurden im Berichtszeitraum 55 Beratungen von interessierten Unternehmen durchgeführt. Die Sprechstunden sind immer weit im Vorhinein ausgebucht. Ob die Beratung für Start-up-Unternehmen im Jahr 2019 weiterhin angeboten werden kann, ist angesichts der starken Belastung der Mitarbeiterinnen und Mitarbeiter durch andere (Pflicht-)Aufgaben derzeit ungewiss.

Zur Gewinnung von Multiplikatoren bei der Umsetzung der DS-GVO haben die Dienstkräfte der BlnBDI in Kammern, Verbänden, Behörden und sonstigen Einrichtungen bis Ende Dezember 2018 in insgesamt 54 Fachvorträgen über die Anwendung der DS-GVO informiert. Nicht alle Vortragsanfragen konnten im Rahmen

der dienstlichen Aufgabenbewältigung berücksichtigt werden. Deshalb haben viele Mitarbeiterinnen und Mitarbeiter der Behörde weitere Vorträge außerhalb der Dienstzeit im Rahmen einer Nebentätigkeit in ihrer Freizeit gehalten.

Von den für den Haushalt 2018/2019 beantragten 15 Stellen wurden der BlnBDI fünf Stellen des höheren Dienstes, vier Stellen des gehobenen Dienstes sowie die Stelle einer (Fremdsprachen-)Sekretariatskraft bewilligt. Die bewilligten Stellen konnten, bis auf eine A 15-Stelle in der Abteilung III (Informatik), alle besetzt werden. Die Besetzung dieser Stelle gestaltete sich angesichts des allgemeinen Fachkräftemangels in diesem Bereich problematisch, sodass diese Stelle Ende 2018 erneut ausgeschrieben wurde. Die vier weiteren Stellen des höheren Dienstes wurden mit juristischen Fachkräften zur personellen Verstärkung der Servicestellen Bürgereingaben, der Servicestellen Europaangelegenheiten und Sanktionen sowie der Arbeitsbereiche Grundsatzfragen der DS-GVO, Wirtschaft und Zertifizierung/Akkreditierung besetzt. Die Stellen des gehobenen Dienstes wurden mit Dienstkräften für die Sachbearbeitung in den Servicestellen Bürgereingaben, Europaangelegenheiten, Sanktionen, in der allgemeinen Verwaltung und mit einem Medienpädagogen besetzt.

Die Erfahrungen aus den ersten Monaten nach dem Wirksamwerden der DS-GVO zeigen deutlich, dass die mit dem Haushalt 2018/2019 bewilligten Stellen den Mehrbedarf an Personal, der durch die Umsetzung der DS-GVO bei der BlnBDI entstanden ist, nicht annähernd abdecken. Die BlnBDI kann ihren Aufgaben als Aufsichtsbehörde für den Datenschutz zukünftig nur ordnungsgemäß und zeitnah nachkommen, wenn der Behörde weitere Personalmittel bewilligt werden.

14.2 Zusammenarbeit mit dem Abgeordnetenhaus von Berlin

Der Ausschuss für Kommunikationstechnologie und Datenschutz (KTDat) tagte in elf Sitzungen, in denen die Berliner Beauftragte für Datenschutz und Informationsfreiheit zu verschiedenen Themen Empfehlungen und Vorschläge abgeben konnte. Ein besonderer Fokus lag auf der Anpassung des Berliner Datenschutzge-

setzes an das neue europäische Datenschutzrecht.[263] Darüber hinaus waren das elektronische Klassenbuch,[264] das Gesetz zur Änderung des Schulgesetzes[265] sowie erneut die IT-Sicherheit und der Datenschutz bei der Charité[266] Gegenstand der Befassung im Ausschuss.

14.3 Zusammenarbeit mit anderen Stellen

Die **Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)** tagte am 25./26. April in Düsseldorf sowie am 7./8. November in Münster und fasste zahlreiche Entschließungen zu aktuellen Fragen des Datenschutzes.[267] Aufgrund des extrem hohen Abstimmungsbedarfs im Zusammenhang mit der Datenschutz-Grundverordnung fanden darüber hinaus insgesamt drei Sondersitzungen der DSK statt: am 30. Januar in Berlin sowie am 11. Juli und 5. September jeweils in Düsseldorf. Auch die Geschäftsordnung der DSK musste aufgrund der neuen Anforderungen durch die DS-GVO komplett überarbeitet und „europatauglich" gemacht werden. Dies war ein schwieriger Prozess, der rechtzeitig vor Wirksamwerden der DS-GVO erfolgreich zum Abschluss gebracht wurde. Die Herausforderung bestand insbesondere darin, Verfahren der Zusammenarbeit zu definieren, die die Abstimmung verbindlicher gemeinsamer Positionen innerhalb der engen Zeitvorgaben der DS-GVO ermöglichen. Um dies zu erreichen, wurde das Mehrheitsprinzip auf fast alle inhaltlichen Bereiche ausgedehnt, außerdem wurden die Vertreterinnen und Vertreter in den verschiedenen europäischen Gremien sowohl auf Leitungs- als auch auf Arbeitsebene mit größerer Selbstständigkeit ausgestattet und die Verteilung der Zuständigkeiten zwischen den deutschen Aufsichtsbehörden wurde stringenter definiert.

263 Wortprotokoll KTDat 18/11 vom 14. Mai 2018, S. 14 ff.; Wortprotokoll KTDat 18/12 vom 28. Mai 2018, S. 10 f.

264 Inhaltsprotokoll KTDat 18/15 vom 15. Oktober 2018, S. 7

265 Beschlussprotokoll KTDat 18/16 vom 12. November 2018, S. 4

266 Wortprotokoll KTDat 18/7 vom 22. Januar 2018, S. 6 ff.; Wortprotokoll KTDat 18/8 vom 19. Februar 2018, S. 7 ff.

267 https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse/

Im Zuge der Neufassung der Geschäftsordnung der DSK und der Überprüfung sämtlicher Zuständigkeiten wurde der Düsseldorfer Kreis, in dem die Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich bislang zusammengearbeitet hatten, nach seiner letzten Sitzung am 28. Februar/1. März in Düsseldorf aufgelöst. Mit der DS-GVO war diese Struktur nicht mehr darstellbar. Die inhaltliche Abstimmung für diesen Bereich erfolgt nunmehr im Arbeitskreis Wirtschaft der DSK, der der DSK zuarbeitet und zum ersten Mal am 19./20. September ebenfalls in Düsseldorf tagte.

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)** tagte am 20. März in Stuttgart sowie am 16. Oktober in Ulm. Sie fasste eine Entschließung zur Veröffentlichung von Verwaltungsvorschriften und beschloss ein Grundsatzpapier mit Vorschlägen zur Förderung eines Kulturwandels in der öffentlichen Verwaltung sowie ein Positionspapier zur Transparenz der Verwaltung beim Einsatz von Algorithmen.[268]

Die **Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre (ICDPPC)** fand vom 21. bis 25. Oktober in Brüssel statt und fasste Entschließungen zu E-Learning Plattformen, zu Fragen von Ethik und Datenschutz bei der Entwicklung und dem Einsatz künstlicher Intelligenz, zur Zusammenarbeit zwischen Datenschutz- und Verbraucherschutzbehörden sowie zu Regeln, Verfahren und der Zukunft der ICDPPC.[269]

Die **Berlin-Group (IWGDPT)** tagte unter unserem Vorsitz am 9./10. April in Budapest sowie am 29./30. November in Queensland.[270]

Das **Global Privacy Enforcement Network (GPEN)** beschäftigt sich mit praktischen Fragen der Durchsetzung des Datenschutzes. Auch im Bereich der praktischen Umsetzung des Datenschutzes hilft der internationale Austausch enorm, weil dadurch lokale Vorgehensweisen optimiert und grenzüberschreitend harmonisiert

268 Hierzu näher Kapitel 13. Die Papiere sind abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-ifk/

269 https://icdppc.org/document-archive/adopted-resolutions

270 Zu den Ergebnissen siehe 12.1

werden können. Die Sitzung fand am 13./14. Juni unter dem Vorsitz der israelischen Datenschutzaufsichtsbehörde in Tel Aviv statt.

14.4 Pressearbeit

Bereits im Jahr 2017 hat unsere Behörde ihre Pressearbeit neu strukturiert, um eine höhere Präsenz des Themas Datenschutz in der Öffentlichkeit zu erreichen und dessen Wichtigkeit für jede und jeden Einzelnen deutlich zu machen.

In diesem Jahr beantworteten wir insgesamt 202 Presseanfragen und konnten unsere Arbeit in diesem Bereich annähernd verdoppeln. Ein Schwerpunktthema war dabei natürlich die Umsetzung der DS-GVO. Journalistinnen und Journalisten interessierte in diesem Zusammenhang besonders, wie sich das Beschwerdeaufkommen zahlenmäßig durch die Rechtsreform entwickelt hat, wegen welcher Themen sich Bürgerinnen und Bürger bei uns beschwerten und in welchen Bereichen besondere Probleme der Umsetzung bestanden. Weitere Themen, die für die mediale Öffentlichkeit von großem Interesse waren, waren das Pilotprojekt „Sicherheitsbahnhof Berlin-Südkreuz", das Volksbegehren für mehr Videoüberwachung sowie bekannt gewordene Sicherheitsmängel beim Zugang zum polizeilichen Informationssystem POLIKS. Unser Presseteam stand Journalistinnen und Journalisten zu diesen und diversen anderen Themen zur Verfügung, damit die teils schwierigen datenschutzrechtlichen und datenschutztechnischen Fragen in der Medienberichterstattung verständlich und richtig dargestellt werden konnten.

Mit insgesamt 19 Pressemitteilungen wandte sich die Berliner Beauftragte für Datenschutz und Informationsfreiheit mit eigenen Themen an die Öffentlichkeit. So konnten wir in gesellschaftlichen Diskursen, wie z. B. im Zuge des Skandals um Cambridge Analytica und den Datenhandel der Deutschen Post oder bei der Debatte um ein mögliches Verbot von Namen auf Klingelschildern von Mietshäusern, wichtige Aufklärungsarbeit leisten.

Folgende Pressemitteilungen haben wir in diesem Jahr veröffentlicht:

- Datenschutz für Kinder: Neue Kinderwebseite www.data-kids.de online (8. Januar 2018)

- Empfehlungen für den Datenschutz im WHOIS-Verzeichnis bei ICANN (9. März 2018)
- Arbeitspapier „Aktualisierung der Firmware eingebetteter Systeme im Internet der Dinge“ (12. März 2018)
- Einladung zum Pressegespräch: Jahresbericht 2017 (16. März 2018)
- Jahresbericht 2017 (23. März 2018)
- Datenhandel durch die Deutsche Post – Wie Betroffene sich wehren können (6. April 2018)
- Tag der offenen Tür und Netzfest: Berliner Beauftragte für Datenschutz und Informationsfreiheit on the Road (2. Mai 2018)
- Zeitenwende im Datenschutz. Neues Datenschutzrecht: Vorsicht, aber keine Panik! (25. Mai 2018)
- Das neue Berliner Datenschutzgesetz – eine vertane Chance (31. Mai 2018)
- Presseinformation – datenschutzkonferenz-online.de – Homepage der Datenschutzkonferenz geht online (19. Juli 2018)
- Datenschutz bei grenzüberschreitenden Datenabfragen zu Strafverfolgungszwecken – Berlin-Group fordert Standards (14. August 2018)
- 100 Tage Datenschutz-Grundverordnung – Zeit für eine erste Bilanz (30. August 2018)
- Warnung vor Abo-Falle der sogenannten Datenschutzauskunft-Zentrale! (2. Oktober 2018)
- Berlin-Group veröffentlicht Arbeitspapier zu vernetzten Fahrzeugen (4. Oktober 2018)
- Positionspapier „Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar“ (17. Oktober 2018)
- Klingelschilder sind kein Datenschutzproblem (19. Oktober 2018)
- Berliner Datenschutzbeauftragte eröffnet umfassende Prüfung des Betriebs von Facebook-Fanpages (16. November 2018)
- Neue Datenschutz-Tipps für Jugendliche (26. November 2018)
- Prüfung einer elektronischen Gesundheitskarte (13. Dezember 2018)

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.

14.5 Öffentlichkeitsarbeit

14.5.1 Veranstaltungen

Am 29. Januar fand auf Einladung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eine zentrale Veranstaltung aus Anlass des 12. Europäischen Datenschutztages in der Vertretung des Landes Niedersachsen beim Bund in Berlin statt. Das Thema lautete „Souveränität in der digitalen Welt – eine Illusion?".

Am 5. Mai nahmen wir am gemeinsamen „Tag der offenen Tür" des Abgeordnetenhauses von Berlin und des Bundesrats teil. Die Veranstaltung im Abgeordnetenhaus von Berlin stand in Verbindung mit dem 25. Jahrestag des Einzugs des Berliner Landesparlaments in das Gebäude des ehemaligen Preußischen Landtags. Dort präsentierten wir einen Stand mit Informationsmaterialen zu verschiedenen Datenschutzthemen. Außerdem beantworteten unsere Fachreferentinnen und -referenten Fragen rund um den Datenschutz. Folgende Schwerpunkte wurden angeboten: Betroffenen-Datenschutzrechte, Was tun gegen unerwünschte Werbung? Melderegister – Wer hat wofür Zugriff auf ihre Daten? Die Europäische Datenschutz-Grundverordnung kommt! Was ist neu? Datenschutz und Schule – Was ist erlaubt, was nicht? Sowohl der Infostand als auch das Beratungsangebot stießen auf großes Interesse.

Am 5. Mai war meine Behörde erstmals auch mit einem breiten Informationsangebot beim Netzfest der Internetkonferenz re:publica vertreten. Neben einem eigenen Informationsstand wurden ein Vortrag sowie ein Workshop mit Themen rund um die Änderungen durch die neue europäische Datenschutz-Grundverordnung (DS-GVO) angeboten. Das Angebot fand lebhaftes Interesse beim Publikum, das zahlreich auch die Gelegenheit nutzte, eigene Datenschutzfragen zu klären. Mit deutlich über 2000 Besucherinnen und Besuchern im Laufe des Tages war das

Informationsangebot der Berliner Beauftragten für Datenschutz und Informationsfreiheit beim re:publica-Netzfest ein voller Erfolg.

Zur Einführung unserer Kinderwebseite www.data-kids.de wurden die Berliner Grundschulen aufgerufen, im Rahmen eines Wettbewerbs die Namen für die Kinder der Roboterfamilie zu vergeben.[271] Der Gewinnerin – der Klasse 3b der Grundschule am Tegelschen Ort – wurde am 25. Juni in der Aula der Grundschule im Rahmen einer feierlichen Zeremonie unter reger Beteiligung der Kinder die Namenspatenschaft verliehen.

14.5.2 Veröffentlichungen

Durch die veränderte Rechtslage nach Inkrafttreten der DS-GVO am 25. Mai war es notwendig, alle Informationsmaterialen auf ihre Aktualität zu überprüfen und ggf. zu überarbeiten. Wir haben im Mai damit begonnen und bereits eine Reihe von Broschüren in aktualisierter oder neu gefasster Auflage herausgegeben. Folgende Broschüren stehen nun allen Interessierten zur Verfügung:

Aktuelle Gesetzestexte:

- **Datenschutz-Grundverordnung:** Zuletzt am 23. Mai 2018 berichtigter Text der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (Datenschutz-Grundverordnung) mit Erwägungsgründen

- **Bundesdatenschutzgesetz:** Am 27. April 2017 mit Wirkung zum 25. Mai 2018 beschlossene Neufassung des Bundesdatenschutzgesetzes nach den Anforderungen der DS-GVO

- **Berliner Datenschutzgesetz:** Neufassung des Berliner Datenschutzgesetzes (BlnDSG) für den öffentlich-rechtlichen Bereich Berlins mit Wirkung vom 13. Juni 2018

271 Ausführlicher zur Kinderwebseite siehe 5.5

Broschüren:

- **Informationsfreiheit in Berlin:** Die Informationsrechte gegenüber den Behörden und sonstigen öffentlichen Stellen des Landes Berlin regelt das Berliner Informationsfreiheitsgesetz (IFG). Der aktualisierte Flyer erläutert die Informations- und andere Einsichtsrechte jedes Menschen sowie jeder juristischen Person und beschreibt das Verfahren und die Einschränkungen bei der Gewährung des Rechts auf Akteneinsicht und -auskunft.

- **Ich suche dich. Wer bist du?** Der bereits in der 12. Auflage erschienene Ratgeber zu sozialen Netzwerken & Datenschutz wurde auf den neuesten Stand gebracht. Die im Rahmen des Berliner Landesprogramms „jugendnetz-berlin" von uns und der Senatsverwaltung für Bildung, Jugend und Familie herausgegebene Broschüre gibt zehn wichtige Tipps, wie Jugendliche ihre persönlichen Daten bei WhatsApp, Instagram und Co. schützen können.

- **Meine Privatsphäre als Mieter/in:** Der Ratgeber informiert u. a. darüber, welche Daten im Mietbewerbungsverfahren abgefragt werden dürfen, wen man zu welchen Anlässen während der Mietzeit in die Wohnung lassen muss, unter welchen Voraussetzungen die Vermieter/innen Videokameras einsetzen dürfen und wann Datenübermittlungen an Dritte zulässig sind.

14.5.3 Vorträge

Seit Jahren leisten die Mitarbeiter/innen der Berliner Beauftragten für Datenschutz und Informationsfreiheit eine umfangreiche Vortragstätigkeit im Rahmen von Kongressen, Workshops und Schulungen. In diesem Jahr war der Bedarf an Fachvorträgen besonders groß. Uns erreichten zahlreiche Anfragen, denen aufgrund der begrenzten Kapazitäten leider nur zum Teil entsprochen werden konnte. Allein in den Arbeitsbereichen Gesundheit sowie Jugend und Familie mussten 15 Vortragsanfragen abgelehnt werden.

Um die eingeschränkte individuelle Beratung zu kompensieren, haben wir dennoch versucht, durch die übernommenen Fachvorträge möglichst viele Multiplikatoren (z. B. bei Veranstaltungen von Branchenverbänden, Kammern, Fachverlagen

oder Interessenvereinigungen) zu erreichen. So haben die Berliner Beauftragte für Datenschutz und Informationsfreiheit und die Referentinnen und Referenten ihrer Behörde in diesem Jahr insgesamt 54 Fachvorträge vor teilweise über hundert Teilnehmerinnen und Teilnehmern gehalten. Im Anschluss an die Vorträge wurden regelmäßig Fragen der Teilnehmerinnen und Teilnehmer diskutiert und beantwortet. Besonders gefragte Themen waren dabei:

- Änderungen durch die DS-GVO
- Neue Sanktionsregeln
- Die Prüf- und Aufsichtspraxis der BlnBDI
- Datenschutz und Medienkompetenz
- Datenschutz in Vereinen
- Die Datenschutz-Folgenabschätzung
- Anonymisierung/Pseudonymisierung
- Auswirkungen der DS-GVO auf die Kinder- und Jugendhilfe

Regelmäßig bieten wir auch an der KinderUni Lichtenberg (KUL) Vorträge an. In diesem Jahr war es eine Veranstaltung am 17. November für Eltern zum Thema „WhatsApp, Instagram & Co. – Von Risiken und Nebenwirkungen“.[272] Der Vortrag traf auf großes Interesse, der Vorlesungssaal war bis auf den letzten Platz besetzt. Anschließend wurden rund eine Stunde lang Fragen aus dem Publikum beantwortet. Die Vorträge zum Datenschutz bei sozialen Netzwerken werden wir auch in den kommenden Jahren weiter anbieten. Interessierte Schulen, Universitäten und sonstige Bildungseinrichtungen können sich bei Bedarf an Vorträgen zu diesem Thema gern an uns wenden.

Insgesamt konnte nur ein Teil der angefragten Vorträge geleistet werden. Der tatsächliche Bedarf war und ist deutlich höher.

272 Siehe https://kinderuni-lichtenberg.de/vorlesungen/noch-planung-6

Anhang

Rede der Berliner Beauftragten für Datenschutz und Informationsfreiheit am 13. September 2018 im Abgeordnetenhaus von Berlin zum Jahresbericht 2017

Sehr geehrter Herr Präsident,
meine sehr verehrten Damen und Herren,

auf der Tagesordnung steht heute die Stellungnahme des Senats zu meinem Jahresbericht 2017. Unsere Prüftätigkeit umfasste wieder unterschiedlichste Lebensbereiche.

Sehr wichtig war erneut der Bereich der Videotechnik und der Videoüberwachung. Wir haben den Einsatz von Bodycams für das Sicherheitspersonal der Deutschen Bahn sowie den Ausbau von Videoüberwachung im öffentlichen Nahverkehr kritisch begleitet. Zum Thema Videoaufnahmen in Berliner Kindergärten haben wir gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Familie einen Handlungsleitfaden für pädagogische Fachkräfte erarbeitet. Geprüft haben wir ein System für Außenwerbung, das biometrische Merkmale von Passanten analysiert, sowie auch den Gesetzesentwurf der Initiative für ein Volksbegehren für mehr Videoüberwachung, vor dem wir nach sorgfältiger Analyse aus verfassungsrechtlichen Gründen gewarnt haben.

Viele Prüfungen gab es auch im Bereich der Wohnungswirtschaft, was vor dem Hintergrund des angespannten Berliner Wohnungsmarkts nicht überrascht. Wir haben darauf hingewirkt, dass die Bezirksämter die Vorgaben des Zweckentfremdungsverbot-Gesetzes einhalten und nicht in unzulässiger Weise intime Informationen über das Privatleben von Wohnungsinhaberinnen und -inhabern sammeln. Im Rahmen einer großangelegten Kontrolle der Immobilienbranche haben wir die dort eingesetzten Formulare zur Selbstauskunft bei Mietbewerbungen geprüft und jede Menge rechtswidriger Formulare aus dem Verkehr gezogen.

Vor allem aber war das Jahr 2017 geprägt von den intensiven Vorbereitungen auf die Datenschutz-Grundverordnung, die seit dem 25. Mai diesen Jahres wirksam ist.

Wir haben Unternehmen und Behörden beraten und bei der Umstellung auf die Verordnung begleitet. Aber auch unsere eigene Arbeit hat tiefgreifende Veränderungen erfahren. Neue Verfahren der Zusammenarbeit der europäischen und deutschen Aufsichtsbehörden mussten entwickelt werden, um für den Tag des Wirksamwerdens der Datenschutz-Grundverordnung gerüstet zu sein. Innerhalb unserer Behörde mussten die Arbeitsabläufe neu strukturiert und durchorganisiert werden. Nebenbei musste noch die inhaltliche Vorbereitung auf die neuen rechtlichen Regelungen erfolgen, ebenfalls im engen Austausch mit den übrigen Aufsichtsbehörden.

Wie wir jetzt sehen, hat die Mühe sich gelohnt; unsere Vorbereitungen haben uns geholfen, den Übergang ins neue Rechtssystem zu meistern. Obwohl wir uns auf eine erhebliche Mehrarbeit eingestellt hatten, hat der Anstieg der Beratungsanfragen unsere Erwartungen allerdings noch einmal deutlich übertroffen. In den letzten vier Monaten haben mich rund 1.800 Beschwerden von Bürgerinnen und Bürgern erreicht und damit viermal so viele wie im Vorjahreszeitraum. Auch die Menge an Beratungsanfragen von Unternehmen und Behörden befindet sich auf einem unverändert hohen Niveau. Darüber hinaus erreichen mich derzeit pro Woche rund zehn Mal so viele Meldungen von Datenpannen wie noch im Vorjahr. Und es zeichnet sich bisher auch keine Entspannung dieser Situation ab. Meine Behörde arbeitet an der Grenze ihrer Belastbarkeit und kann ihre Aufgaben nur noch teilweise erfüllen. Ich bin sehr glücklich, dass ich hochmotivierte Mitarbeiterinnen und Mitarbeiter habe, die mit riesigem Engagement ihre Arbeit verrichten – anders könnten wir diese Herausforderungen nicht bestehen und dafür möchte ich mich an dieser Stelle sehr herzlich bedanken!

Ich werte diese Zahlen aber vor allem als Erfolg. Sie zeigen, dass das neue Regelwerk die Unternehmen, die Behörden, aber auch die Bürgerinnen und Bürger für den Datenschutz sensibilisiert hat. Das war ein wichtiges Anliegen des europäischen Gesetzgebers. Die Zahlen zeigen uns, dass das Mammutprojekt Datenschutz-Grundverordnung Wirkung entfaltet – trotz aller Kinderkrankheiten, die es in den kommenden Jahren noch zu heilen gilt.

Es erscheint mir an dieser Stelle wichtig, noch einmal darauf hinzuweisen, dass die Datenschutz-Grundverordnung ein notwendiger Schritt war, um Bürgerrechte in einer Zeit fortschreitender globaler Digitalisierung zu schützen.

Die aktuellen technischen Entwicklungen sind nichts weniger als eine Zeitenwende für unsere Gesellschaft. Die Digitalisierung hat mittlerweile Einzug in fast alle Lebensbereiche gehalten. Einiges davon hat das Potenzial, unser Leben zu erleichtern und zu verbessern. Gleichzeitig bergen diese Entwicklungen aber auch Gefahren für unsere freie, demokratische Gesellschaft.

Die Quasi-Monopolstellungen großer Datenkonzerne haben zur Folge, dass nicht nur Bürgerinnen und Bürger, sondern auch Unternehmen und staatliche Institutionen mehr und mehr in deren Abhängigkeit geraten und ein fairer Wettbewerb behindert wird. Immer häufiger bereiten darüber hinaus Algorithmen Entscheidungen über uns Menschen vor oder treffen sie gar selbst. Diese Algorithmen sind zumeist vollkommen intransparent, obwohl sie erhebliche Auswirkungen auf das Leben von uns allen haben können. Sehr ernst zu nehmen ist auch die steigende Gefahr manipulierter Meinungsbildungsprozesse oder politischer Wahlen.

Die Datenschutz-Grundverordnung stellt einen ersten wichtigen Schritt dar, zur weltweiten Wahrung unserer Freiheitsrechte beizutragen. Dabei darf es angesichts der genannten Herausforderungen allerdings nicht bleiben. Damit alle Menschen von den Vorteilen der Digitalisierung profitieren und diese sorgenfrei genießen können, müssen wir Fehlentwicklungen entgegensteuern. Dies ist zum einen die Aufgabe der Aufsichtsbehörden, die jedoch dringend eine bessere Ausstattung benötigen, um diese Aufgaben auch erfüllen zu können. Zum anderen ist aber auch die Politik mehr denn je gefragt, mutige Antworten auf die großen Fragen unserer Zeit zu finden; es gibt erheblichen Regulierungsbedarf.

Meine Damen und Herren, ich möchte daher an dieser Stelle sehr herzlich an Sie appellieren, Ihre Möglichkeiten als gewählte Parlamentarierinnen und Parlamentarier zu nutzen und sich dafür einzusetzen, dass notwendige Regulierungsschritte unternommen werden.

Die Tatsache, dass heute eine Bundesratsinitiative zur Bekämpfung des Identitätsdiebstahls auf der Tagesordnung steht, ist ein guter Schritt in diese Richtung.

Aber es gibt viele weitere Punkte, bei denen etwas geschehen muss. So ist es dringend erforderlich, dass die europäische E-privacy-Verordnung endlich verabschiedet wird, die den Schutz der Menschen auch auf digitale Messenger-Dienste ausweiten soll. Diskutiert werden müssen Änderungen des Wettbewerbsrechts und die Besteuerung von Digitalunternehmen. Und es müssen dringend Lösungen für die Transparenz von Algorithmen gefunden werden. – Dies ist übrigens nicht nur ein Thema des Datenschutzes, sondern auch der Informationsfreiheit. Nur informierte Bürgerinnen und Bürger können souverän Entscheidungen fällen. Und ausreichende Informationen sind auch eine grundlegende Voraussetzung für das so elementar wichtige Vertrauen der Bürgerinnen und Bürger in den Staat.

Der Staat sollte in einer immer komplexeren digitalisierten Welt, in einer Zeit der Verunsicherung im Übrigen auch dafür sorgen, dass Alternativen zu den Angeboten der globalen Digitalunternehmen angeboten werden. Das schafft Vertrauen, das schafft Unabhängigkeit und das schafft Freiräume für die Entwicklung der einheimischen Wirtschaft.

Wir alle sollten den Datenschutz und die Informationsfreiheit als Chance begreifen, unsere demokratischen und freiheitlichen Werte sicher in die Zukunft zu bringen. Lassen Sie uns gemeinsam mit der Zivilgesellschaft und den Unternehmen aktiv und konstruktiv an neuen Lösungen arbeiten!

Vielen Dank!

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.

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.

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 Datenverarbeitern innerhalb der Europäischen Union.

Car-to-X-Kommunikation

Oberbegriff für die Vernetzung von Fahrzeug zu Fahrzeug bzw. von einem Fahrzeug mit der Infrastruktur.

Chief Information Security Officer (CISO)

Verantwortlicher 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.

Cluster

Leitet sich ab von engl. „cluster“ = „Bündel“, „Menge“ und steht für verdichtete Ansammlung von Häusern, Bebauung in Gruppen, Pulks von Hochhäusern.

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.
CRO	CRO steht für Clinical Research Organisation (Auftragsforschungsinstitut). Dabei handelt es sich um ein Dienstleistungsunternehmen für die Arzneimittel und Medizinprodukte produzierende Industrie, welches die Forschung und Entwicklung von Arzneimitteln bzw. Medizinprodukten im Zuge der Planung und Durchführung klinischer Studien unterstützt.
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 (DSGVO) 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 Datenver-

kehr innerhalb des Europäischen Binnenmarktes gewärleistet werden. Die Verordnung er setzt 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 Mitgliedstaaten der Europäischen Union unmittelbar anwendbar.

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 der vom Sender festgelegte Empfänger die Daten entschlüsseln, d. h. wieder lesbar machen kann. Zwischenstationen wie z. B. E-Mail-Anbieter 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 mit Hilfe der vom Netzwerk zur Verfügung gestellten Kommunikationsmittel zu vermarkten, z. B. indem die Seite von Facebook-Nutzerinnen und -Nutzern weiterempfohlen bzw. im „Freundeskreis" der Nutzerinnen und Nutzer 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, mit Hilfe der Seite z. B. direkt mit Kunden 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.
Gamification	Von engl. „game" für „Spiel"; bezeichnet den Einsatz von spieletypischen Elementen zur Motivationssteigerung und Verhaltensänderung bei Anwenderinnen und Anwendern.
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; deutsch: Globales Positionsbestimmungssystem.
Hashfunktion	Bei einer kryptografischen Hashfunktion handelt es sich um eine mathematische Berechnungsvorschrift, die aus beliebigen Ausgangsdaten wie beispielsweise 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 Ausgangs daten wie beispielsweise einem Dokument oder auch

	nur einem Wort bzw. einer Telefonnummer einen eindeutigen Hashwert mit fester Länge berechnet.
Integrität	Unter der Wahrung der Integrität von Daten versteht man ihren Schutz vor unbeabsichtigtem Verlust oder unbeabsichtigter Verfälschung bzw. die korrekte Funktionsweise von Systemen.
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 im Rahmen des Kohärenzverfahrens verbindliche Beschlüsse. Darüber hinaus werden im Kohärenzverfahren mit dem Ziel der einheitlichen Anwendung der DS-GVO auch Stellungnahmen des Europäischen Datenschutzausschusses – 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.

Metadaten	Die bei einer Datenübermittlung anfallenden Daten unterteilt man in Inhaltsdaten – beispielsweise 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 Kurz-nachrichtendienst 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.
One-Stop-Shop	Das One-Stop-Shop-Prinzip bedeutet, dass sich sowohl jede Bürgerin und jeder Bürger als auch jedes Unternehmen an die Aufsichtsbehörde vor Ort wenden kann. Dies gilt insbesondere auch dann, wenn personenbezogene Daten grenzüberschreitend verarbeitet werden, z. B. durch soziale Netzwerke oder andere international tätige Unternehmen. Die Aufsichtsbehörde, bei der eine Beschwerde eingereicht wurde, unterrichtet die Beschwerdeführer über den Stand und das Ergebnis des Verfahrens. Für Unternehmen mit Niederlassungen in verschiedenen Mitgliedstaaten ist die Aufsichtsbehörde am Sitz der Hauptverwaltung der zentrale Ansprechpartner. Alle diese Aufsichtsbehörden sind am aufsichtsbehördlichen Verfahren beteiligt und achten gemeinsam darauf, dass die Rechte der Bürgerinnen und Bürger gewahrt werden.
Open Data	Datenbestände, die den Bürgerinnen und Bürgern sowie der Wirtschaft ohne Beschränkung zur freien Weiterverwendung frei zugänglich gemacht werden.
Open Government	Öffnung von Staat und Verwaltung gegenüber den Bürgerinnen und Bürgern sowie der Wirtschaft.
OWASP10-Kriterien	Kriterien, die durch das Open Web Application Security Project, eine global tätige Stiftung zur Förderung der Netzsicherheit, veröffentlicht wurden.

Pixel	Kleine Grafiken auf Webseiten, die meist nur 1x1 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.
PNR-Daten	PNR steht für Passenger Name Record. Das sind Fluggastdatensätze, zu denen neben Kontakt-, Reise- und Zahlungsinformationen auch Informationen zu Ernährungsgewohnheiten und zum Gesundheitszustand der Reisenden zählen können.
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.
Prüfwert	Der Prüfwert wird mittels einer unumkehrbaren kryptografischen Hashfunktion aus der Telefonnummer berechnet.

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 möglicht ist.
Quellcode	Der Programmcode (technische Grundlage) einer Software.
Registrant	Person, die eine Webseiten-Registrierung bei einer Organisation durchführt, die Internet-Domains registriert (bei dem sog. Registrar).
Ringspeicherverfahren	Speichert Daten kontinuierlich in einem gewissen Zeitraum und überschreibt diese nach dem Ablaufen einer vorgegebenen Zeit wieder, um den Speicherplatz für neue Daten wieder freizugeben.
Score-Wert	Nummerischer Wert, der die Kreditwürdigkeit einer Person beschreibt. Der Score-Wert wird von Unternehmen und Auskunfteien mithilfe eines mathematisch-statistischen Verfahrens berechnet und dient als Grundlage für Vertragsentscheidungen.
sensitive Daten	Besondere Arten personenbezogener Daten. Dazu gehören Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.
Social Plugins	Ein Programmcode, der in die Webseite eingebunden wird und den Browser der Benutzerin bzw. des Benutzers der Webseite dazu veranlasst, Inhalte von einem Dritten anzufordern und dazu Daten an diesen Dritten übermittelt, z. B. „Gefällt mir"-Button von Facebook oder „Twitter"-Button.

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.
Telematiktarife	Versicherungstarif, dessen Beitrag abhängig von der Fahrzeugnutzung berechnet wird. Einbezogen werden z. B. die Anzahl der Nachtfahrten, Fahrten in riskanten Gegenden oder auf unfallträchtigen Straßen sowie die Einhaltung von Höchstgeschwindigkeiten und das Beschleunigungsverhalten. Hierzu erfolgt eine intensive elektronische Überwachung der Fahrzeugaktivitäten und Übermittlung der Daten an die Versicherung. Diese Tarife werden auch als „Pay as you Drive"-Tarife bezeichnet.
Tracking / Cookie Walls	Verhinderung der Nutzung einer Webseite bei Nichtakzeptieren von Cookies.
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.
Webtracking	Die Beobachtung und Analyse der Nutzerinnen und Nutzer zu Geschäfts- und Marketingzwecken.
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

E

F

G

H / I

J

K / L

M

N

O

P

Q / R

S

T

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, Orientierungshilfen 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 in aktualisierter bzw. neu gefasster Ausgabe.

Standpunkt: Datenschutzrechtliche bzw. datenschutzpolitische Positionierung der Beauftragten für Datenschutz und Informationsfreiheit zu einem konkreten Sachverhalt.

Kurzpapiere: Die Europäische Datenschutz-Grundverordnung (DS-GVO) wird am 25. Mai 2018 wirksam. Die Aufsichtsbehörden befassen sich zurzeit intensiv mit den neuen Rechtsgrundlagen und deren Anforderungen und stimmen eine einheitliche Sichtweise ab. Erste Ergebnisse dieses Prozesses sind gemeinsame Kurzpapiere zur DS-GVO, die die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) veröffentlicht.

Alle Informationsmaterialien sind auf unserer Webseite abrufbar und einige auch in gedruckter Form erhältlich. Eine Übersicht und Hinweise zur Bestellung finden Sie unter **www.datenschutz-berlin.de**.

Der Jahresbericht 2018 umfasst folgende Schwerpunkte:

Bearbeitung grenzüberschreitender Fälle und Beschwerden nach der DS-GVO; Informationspflicht bei Datenpannen; Datenschutz-Zertifizierung; Werbung nach der DS-GVO; das neue Datenschutzgesetz; Facebook-Fanpages und die gemeinsame Verantwortlichkeit für Datenverarbeitungen; Berliner Landesgesetze

www.datenschutz-berlin.de

Berlin