Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Datenschutz und Informationsfreiheit

Jahresbericht 2019

Jahresbericht

der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2019

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 28. März 2019 vorgelegten Jahresbericht 2018 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2019 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.

Abkürzungsverzeichnis

Abghs.-Drs.	Abgeordnetenhausdrucksache
ADM	Arbeitskreis Deutscher Markt- und Meinungsforschungsinstitute
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGG	Allgemeines Gleichbehandlungsgesetz
AGGVG	Gesetz zur Ausführung des Gerichtsverfassungsgesetzes
AO	Abgabenordnung
ASOG	Allgemeines Sicherheits- und Ordnungsgesetz
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BEM	Betriebliches Eingliederungsmanagement
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKartA	Bundeskartellamt
BlnAGBMG	Berliner Ausführungsgesetz zum Bundesmeldegesetz
BlnDSG	Berliner Datenschutzgesetz
BMI	Bundesministerium des Innern, für Bau und Heimat
BMG	Bundesmeldegesetz
BMGVwV	Allgemeine Verwaltungsvorschrift zur Durchführung des Bundesmeldegesetzes
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVG	Berliner Verkehrsbetriebe
BVR	Bundesverband der Deutschen Volksbanken und Raiffeisenbanken
CV	Curriculum Vitae
DSGV	Deutscher Sparkassen- und Giroverband
DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

DVG	Digitale-Versorgung-Gesetz
EDSA	Europäischer Datenschutzausschuss
EG	Erwägungsgrund
EGovG Bln	E-Government-Gesetz Berlin
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FITKO	Föderale IT-Kooperation
GBA	Gemeinsamer Bundesausschuss
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GG	Grundgesetz
GRCh	Charta der Grundrechte der Europäischen Union
GwG	Geldwäschegesetz
HTW	Hochschule für Technik und Wirtschaft
ICIC	Internationale Konferenz der Informationsfreiheitsbeauftragten
IFG	Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
IMI	Binnenmarkt-Informationssystem
ISBJ	Integrierte Software Berliner Jugendhilfe
IT	Informationstechnik
ITDZ	IT-Dienstleistungszentrum
IWGDPT	Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation (sog. Berlin-Group)
JB	Jahresbericht
KEF	Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten
KI	Künstliche Intelligenz
KMU	kleine und mittlere Unternehmen
KTDat	Ausschuss für Kommunikationstechnologie und Datenschutz
KUL	KinderUni Lichtenberg
KV	Kassenärztliche Vereinigung
LABO	Landesamt für Bürger- und Ordnungsangelegenheiten
LAF	Landesamt für Flüchtlingsangelegenheiten
LAGeSo	Landesamt für Gesundheit und Soziales
OZG	Onlinezugangsgesetz
PKI	Public Key Infrastructure

POLIKS	Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung
PStG	Personenstandsgesetz
RBStV	Rundfunkbeitragsstaatsvertrag
RL	Richtlinie
RSD	Regionaler Sozialpädagogischer Dienst
SenIAS	Senatsverwaltung für Integration, Arbeit und Soziales
SGB	Sozialgesetzbuch
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TMG	Telemediengesetz
TSG	Transsexuellengesetz
TU	Technische Universität
UWG	Gesetz gegen den unlauteren Wettbewerb
VBB	Verkehrsverbund Berlin-Brandenburg
VG	Verwaltungsgericht
VIG	Verbraucherinformationsgesetz
VK	Vereinigtes Königreich
VvB	Berliner Verfassung
WJH	Wirtschaftliche Jugendhilfe

Vorwort

Die Datenschutz-Grundverordnung (DS-GVO) wirkt. Der wegweisende Charakter dieses europäischen Gesetzes für den Datenschutz in Europa und auch darüber hinaus wird immer spürbarer.

So blicken wir in Berlin auf ein spannendes und erfolgreiches Jahr im Zeichen der DS-GVO zurück. Es war das erste vollständige Jahr mit der neuen Gesetzeslage und wir konnten in unserer Arbeit beobachten, dass die datenschutzrechtliche Sensibilität in fast allen Bereichen deutlich zugenommen hat. Verantwortliche Stellen wenden sich viel häufiger bei Fragen und Problemen aktiv an uns und legen verstärkt Wert auf ein gutes Datenschutzmanagement.

Vor allem bei den Bürgerinnen und Bürgern ist ein starkes und nicht nachlassendes Interesse am Schutz ihrer personenbezogenen Daten festzustellen. Dieses Interesse war mit der Einführung der DS-GVO und den in diesem Zusammenhang intensiv geführten öffentlichen Diskussionen über das Thema stark angestiegen und hat sich seither auf sehr hohem Niveau eingependelt. Meine Behörde hat im vergangenen Jahr mehrere tausend Beschwerden von Bürgerinnen und Bürgern bearbeitet, über tausend gemeldete Datenpannen gesichtet und ausgewertet, intensiv mit anderen Fachleuten auf nationaler und europäischer Ebene zusammengearbeitet und nicht zuletzt vielfältige Beratungen und Prüfungen von Unternehmen und Behörden sowie eine beachtliche Anzahl an Sanktionsverfahren durchgeführt.

Zunehmend rücken hierbei auch große Bußgeldverfahren gegen supranational tätige Unternehmen in den Mittelpunkt. Naturgemäß sind für Überprüfungen in diesen Bereichen angesichts der dort anzutreffenden komplexen Datenverarbeitungssysteme regelmäßig ein hoher Arbeitsaufwand und viel Zeit erforderlich, be-

vor Ergebnisse erzielt werden können. Aber mehr als ein Jahr nach Wirksamwerden der DS-GVO sind wir so weit, auch in ersten größeren Fällen Maßnahmen zur Sicherung des Datenschutzes zu ergreifen und uns dabei der neuen Kompetenzen zu bedienen, die die DS-GVO uns zur Verfügung stellt. Ergebnis dieser Entwicklung war unter anderem das deutschlandweit erste Bußgeld in zweistelliger Millionenhöhe.

Maßnahmen werden dabei immer vor dem Hintergrund der Grundidee der DS-GVO erlassen, dass in einer immer umfassender digitalisierten Gesellschaft dem Datenschutz nur dann zum Durchbruch verholfen werden kann, wenn Verstöße gegen dessen Prinzipien in spürbarer Weise geahndet werden. Dabei geschieht dies immer nach dem Grundsatz der Verhältnismäßigkeit und vor dem Hintergrund der wirtschaftlichen Leistungsfähigkeit des jeweiligen Unternehmens oder der jeweiligen Organisation. Über die Einzelverfahren hinaus muss es letztlich Ziel der datenschutzrechtlichen Sanktionierung sein, Stellen, die personenbezogene Daten verarbeiten, zu zeigen, dass es sich einerseits lohnt, Datenschutz aktiv zu betreiben, und dass es andererseits empfindlich weh tun kann, wenn man die gesetzlichen Vorgaben nicht einhält.

Bedeutsam war im letzten Jahr auch das Urteil des Europäischen Gerichtshofs zum Facebook-Like-Button. Das Gericht stellte fest, dass nicht nur Facebook, sondern auch Webseitenbetreibende, die den Facebook-Like-Button oder andere Social Plugins verwenden, für die damit zusammenhängende Datenverarbeitung mit verantwortlich sind. Bereits im Jahr 2018 hatte der Europäische Gerichtshof für Facebook-Fanpages die gemeinsame Verantwortlichkeit von Facebook und den Betreiberinnen und Betreibern der Fanpages festgestellt. Wir hatten daraufhin Prüfungen gegen Berliner Fanpage-Betreibende eingeleitet, die noch andauern. Verantwortliche müssen sich klarmachen, dass die Pflichten, die mit einer solchen gemeinsamen Verantwortlichkeit einhergehen, nicht ohne Weiteres erfüllbar sind. Entsprechendes gilt auch für die datenschutzrechtlichen Verpflichtungen, die man durch die Einbindung von Google Analytics und ähnlichen Dritt-Diensten in die eigene Webseite hat. Webseitenbetreibende sollten sich deshalb genau überlegen, ob sie überhaupt auf solche Angebote zurückgreifen möchten.

Im digitalen Bereich ist auch die datenschutzgerechte Gestaltung und Nutzung von mobilen Apps ein immer wichtigeres Thema. Besonders relevant ist neben der

Verwendung von Messengerdiensten wie WhatsApp durch öffentliche Stellen die zunehmende Verbreitung von Gesundheits-Apps, die oft sehr sensitive Daten der Nutzenden verarbeiten. In beiden Fällen ist die Durchführung geeigneter technischer und organisatorischer Maßnahmen sowie eine transparente Informationspolitik hinsichtlich des Zwecks und des Umfangs der Datenverarbeitung für einen rechtskonformen Einsatz unabdingbar. Hier herrscht noch großer Nachholbedarf bei den Verantwortlichen.

Je mehr unser Leben durch digitale Anwendungen geprägt wird, desto wichtiger ist die frühzeitige Aufklärung der Menschen von Kindheit an über Risiken und Rechte im Zusammenhang mit der Verarbeitung ihrer Daten. Nur wer um die Gefahren und die eigenen Handlungsmöglichkeiten weiß, kann den Schutz seiner Daten selbst in die Hand nehmen. Dabei kann man mit der Sensibilisierung gar nicht früh genug anfangen. Wir haben deswegen im vergangenen Jahr unsere Arbeit im Bereich der Medienpädagogik noch intensiviert, um bereits Grundschulkindern ein Bewusstsein dafür zu vermitteln, dass bei der Verwendung digitaler Medien vielfältige Informationen im Hintergrund über sie gesammelt werden und in vielfältiger Weise missbraucht werden können. Dafür haben wir u. a. weiter an unserer Kinderwebseite gefeilt und waren hocherfreut, als wir erfuhren, dass sie für den deutschen Kindersoftwarepreis TOMMI nominiert wurde.

Auch wenn der Schwerpunkt unserer Tätigkeit im vergangenen Jahr zwangsläufig die Umsetzung der DS-GVO war, tut sich doch auch im Bereich der Informationsfreiheit einiges: In Berlin sind erste Zeichen für die Schaffung eines Transparenzgesetzes sichtbar, nachdem bereits einige Bundesländer solche Gesetze verabschiedet haben, die staatliche Stellen verpflichten, der Öffentlichkeit eigeninitiativ Informationen über ihre Arbeit zur Verfügung zu stellen. Wir begrüßen diesen Weg ausdrücklich und werden Parlament und Regierung bei der Umsetzung eines solchen Gesetzes in Berlin mit Rat und Tat zur Seite stehen.

Etwa eineinhalb Jahre sind seit Einführung der DS-GVO vergangen; sie waren anstrengend, aber sehr lehrreich und insgesamt auch sehr erfolgreich. Alle, die mit Datenverarbeitung und Datenschutz befasst sind, mussten den Umgang mit dem neuen Regelwerk lernen. Unsere Erfahrungen zeigen jedoch, dass nicht nur die Bürgerinnen und Bürger, deren Rechte durch die DS-GVO nachhaltig erweitert wurden, gewonnen haben. Auch Unternehmen können von den neuen Regelungen

profitieren, wenn sie den Datenschutz ernst nehmen. In einer globalisierten und digitalisierten Welt hat die DS-GVO das Potenzial, das Grundrecht auf informationelle Selbstbestimmung zukunftsfähig zu machen. Es bleibt spannend!

Berlin, den 3. April 2020

Maja Smoltczyk
Berliner Beauftragte für Datenschutz und Informationsfreiheit

1 Schwerpunkte

1.1 Status unentbehrlich – Messenger-Dienste in Unternehmen und öffentlichen Einrichtungen

Messenger-Dienste auf privaten Smartphones werden vielfach auch für dienstliche oder geschäftliche Zwecke verwendet. Insbesondere in sensiblen Bereichen – z.B. dem Gesundheits- und dem Schulwesen – hat dies hohe Risiken zur Folge. Wir haben uns an der Erarbeitung einer Handreichung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zu dem Thema beteiligt, eine Krankenhauskette dazu beraten und Hinweise an die Berliner Schulverwaltung gegeben.

Der Reiz der schnellen Nachricht

Was tun, wenn die kompetente ärztliche Kollegin sich in Bereitschaft, doch weit vom Krankenbett befindet und eine Entscheidung so schnell wie möglich zu treffen ist? Ein, zwei Schnappschüsse der relevanten Ergebnisse der Diagnostik und eine Anfrage geht per WhatsApp ab an die Kollegin, die schon auf dem Weg telefonisch erste Hinweise für die weitere Behandlung geben kann. Dies ist ein Szenario, über das kaum gesprochen wird und das doch so oder so ähnlich mittlerweile durchaus in vielen Krankenhäusern anzutreffen ist. Die Vorteile für die Behandlung (schnellere Reaktionszeiten) und für das Krankenhaus (Vereinfachung des Bereitschaftsdiensts und geringere Belastung der Beschäftigten) sind offensichtlich. Ein zusätzlicher Reiz: Auf den ersten Blick entstehen keine Kosten.

Ambulante Pflegekräfte sind viel unterwegs. Auch für sie sind Messenger-Dienste ein günstiges und vielseitiges Hilfsmittel. Sie erhalten Änderungen an der Einsatzplanung, können Nachfragen bei dem Kollegen stellen, der am Vortag bei der gleichen Patientin tätig war. Die Nachrichten kommen zeitgerecht. Anders als bei einem Telefonat muss die aktuelle Tätigkeit nicht unterbrochen werden, um sie entgegenzunehmen. Auch später noch lässt sich nachlesen, was man bei mündlicher Kommunikation viel eher vergisst.

Auch in der Schule sind über einen Klassenchat sowohl die Schülerinnen und Schüler als auch die Eltern selbst über kurzfristige Änderungen im Schulablauf schnell informiert. Er stellt eine zeitsparende Alternative zur Information der Betroffenen dar und alle Teilnehmerinnen und Teilnehmer verfügen über die gleichen Informationen. Diejenigen, die Messenger-Dienste nicht verwenden möchten, sind jedoch zunächst hiervon ausgeschlossen.

Die versteckten Risiken

Die Verwendung von Messenger-Diensten in Fällen wie den oben beschriebenen bringt eine Reihe von datenschutzrechtlichen Problemen mit sich. Verstärkt wird dies, wenn die Kommunikation mit Privatgeräten der Beschäftigten erfolgt und die versandten Daten damit der unmittelbaren Kontrolle der jeweiligen Institution entzogen sind.

Viele der bekannten, öffentlich zugänglichen Messenger-Dienste sind problematisch, weil die Dienste-Anbieter, allen voran die zu Facebook gehörende WhatsApp Ireland Ltd. mit ihrem kostenlosen Angebot WhatsApp, nicht nur die Nachrichten übermitteln, sondern gleichzeitig eigene monetäre Ziele verfolgen. Für sie ist es gewinnbringend, die Kommunikationsmuster der Personen zu kennen, die ihre Dienste nutzen, um ihnen Werbenachrichten zuspielen zu können.

In diesem Zusammenhang ist deutlich auf die mit dem Einsatz von Messenger-Diensten im beruflichen Umfeld verbundenen Verantwortlichkeiten hinzuweisen: Wenn Unternehmen und Behörden ihre Beschäftigten oder Kommunikationspartnerinnen und -partner dazu auffordern, einen Messenger-Dienst zu nutzen, bei dem eine unzulässige Datennutzung zum Geschäft des Messenger-Dienstes gehört, dann tragen sie einen Teil der Verantwortung für diese Rechtsverletzung.

Das beginnt damit, dass die meisten Dienste-Anbieter ungefragt die Adressbücher der Smartphones auslesen. Auch einige nichtkommerzielle Angebote wie Signal gehen so vor.

Doch Unternehmen oder öffentliche Stellen brauchen eine Rechtsgrundlage, wenn sie ihre Beschäftigten zur Nutzung eines Messenger-Dienstes auffordern und dadurch veranlassen, dass Daten privater Dritter, die in den Adressbüchern der Smartphones der Beschäftigten enthalten sind, an den jeweiligen Dienste-An-

bieter weitergegeben werden. Da hierfür keine gesetzliche Erlaubnis besteht, müssten sämtliche im jeweiligen Adressbuch enthaltenen privaten Kommunikationspartnerinnen und -partner um Einwilligung in diese Übermittlung gebeten werden. Das ließe sich jedoch kaum praktikabel umsetzen. Daher sollte eine im beruflichen Umfeld genutzte Messenger-App nur diejenigen Daten an Dienste-Anbieter übergeben, die diese benötigen, um die jeweiligen Nachrichten an die korrekten Empfängerinnen und Empfänger zu übermitteln. In der Praxis werden dies ausschließlich die eindeutigen Kennungen von absendenden und empfangenden Personen sein (oft deren Telefonnummern).

Die Masse der kritischen Daten aus der Nutzung von Messenger-Diensten fällt beim Austausch der Nachrichten unter den Teilnehmenden an. Auch wenn die Inhalte der Nachrichten verschlüsselt sind, erfahren die Anbieter dabei, wer mit wem kommuniziert. Bei diesen Informationen handelt es sich um sog. Verkehrsdaten. Mögen diese zuweilen auch banal sein, so kann man vielen dieser Verkehrsdaten durchaus relevante Informationen entnehmen, die keineswegs banal sind. Beispielsweise stellt es eine schützenswerte Information dar, wer mit welcher Ärztin oder welchem Arzt kommuniziert, da hieraus relevante Rückschlüsse auf den jeweiligen Gesundheitszustand gezogen werden können.

Mehrere Faktoren können darüber hinaus das Risiko vergrößern, dass die Anbieter der Messenger-Dienste die anfallenden Verkehrsdaten unrechtmäßig selbst nutzen oder Dritten offenlegen. Erstens unterliegen Messenger-Dienste derzeit (noch) nicht dem Telekommunikationsrecht und damit der Verpflichtung zum besonderen Schutz der Verkehrsdaten. Zum Zweiten sind einige der größten Dienste-Anbieter oder die sie beherrschenden Konzerne in Drittstaaten angesiedelt, deren Rechtsordnungen einen Zugriff auf die Verkehrsdaten durch staatliche Behörden auch unter Voraussetzungen erlauben, die durch europäisches Recht nicht gedeckt sind. Die letztgenannten Umstände können sich auch kurzfristig durch die Verlagerung von Unternehmenssitzen oder den Wechsel von Gesellschaftern oder beherrschenden Unternehmen ergeben. Im Jahr 2019 geschah dies z.B. bei der Wire Swiss GmbH, der Anbieterin des Messenger-Dienstes Wire. Und zum Dritten kann sich auch der Ort der Datenverarbeitung in ein rechtlich unsichereres Umfeld verlagern, weil der Dienste-Anbieter sich bewusst dafür entscheidet oder einem Clouddienstleister, der für ihn tätig ist, erlaubt, dies zu tun.

All diese Umstände haben auch Auswirkungen auf den Schutz der Vertraulichkeit der übermittelten Daten. Zwar kommen mittlerweile regelmäßig Verschlüsselungsverfahren zur Anwendung, die bei korrekter Ausführung die übermittelten Daten auch gegenüber dem Dienste-Anbieter schützen. In einigen Fällen erfüllen diese Verfahren sogar ausgesprochen hohe Anforderungen. Doch liegt es völlig in der Hand der Dienste-Anbieter, zu kontrollieren, ob, wie und mit welchen Schlüsseln die Daten gesichert werden. Institutionen, die einen öffentlichen Messenger-Dienst einsetzen wollen, müssen daher sorgfältig die Zuverlässigkeit der jeweiligen Dienste-Anbieter sowie die rechtliche und technische Gestaltung der angebotenen Produkte mit den Folgen abwägen, die eine eventuelle Offenlegung der übertragenen Daten für die betroffenen Personen hätte.

Wenn eine Institution sich über einen Messenger-Dienst an Privatpersonen wendet, bspw. eine Bank an ihre Kundinnen und Kunden, ergeben sich zusätzliche Vertraulichkeitsrisiken daraus, dass die Sicherheitseigenschaften der Geräte, die die datenempfangenden Personen benutzen, oft weit hinter denen der dienstlichen Geräte zurückfallen. Dabei ist es weder zulässig, Personen von einem Kommunikationskanal auszuschließen, weil sie kein geeignetes Gerät besitzen oder einsetzen wollen, noch diese Personen zu einer Form der Kommunikation zu drängen, die ihre eigenen Daten gefährdet. Daher müsste in jedem Fall sichergestellt werden, dass der Zugang zu den Mitteilungen auch auf einem anderen Wege als über die Messenger-Dienste ermöglicht wird.

Über die Gewährleistung der Vertraulichkeit hinaus sind bei jedem beruflich begründeten Versand personenbezogener Daten mit einem Messenger-Dienst und bei der nachfolgenden Speicherung der Nachrichten auf den Geräten der Kommunikationspartner bzw. -partnerinnen auch die anderen Datenschutzgrundsätze einzuhalten und die Betroffenenrechte zu gewähren. Dies wird oft vergessen: Die Institution bleibt verantwortlich für die Datenverarbeitung. Auch über Daten, die zunächst nur auf den Geräten der beteiligten Beschäftigten gespeichert sind, muss auf Verlangen der Betroffenen Auskunft erteilt werden können. Es muss die Möglichkeit bestehen, dass die Daten berichtigt und in ihrer Verarbeitung eingeschränkt oder gelöscht werden können. Werden sie nicht mehr benötigt, so sind sie unaufgefordert und unverzüglich zu löschen. Für andere Zwecke dürfen die Daten nur eingesetzt werden, wenn dies verhältnismäßig und mit dem ursprünglichen Kontext, in dem die Übermittlung stattfand, vereinbar ist.

So geht es richtig

Ein gesetzeskonformer Einsatz von Messenger-Diensten erzielt nicht nur den gewünschten Effekt einer schnellen und einfachen Kommunikation zum Nutzen der betroffenen Personen, sondern schützt gleichzeitig auch deren Rechte. Dazu müssen die verwendete App, der Übermittlungsdienst und die eingesetzten Geräte grundlegenden Anforderungen genügen. Vielfach ist zudem eine Einbindung des Messenger-Dienstes in die übrige Datenverarbeitung der oder des Verantwortlichen notwendig, um die Einhaltung von Datenschutzgrundsätzen und die Gewährung von Betroffenenrechten zu gewährleisten sowie ggf. bestehende Dokumentationspflichten zu erfüllen. Letzteres lässt sich in der Regel nur umsetzen, wenn der Dienst durch das Unternehmen selbst oder spezifisch für dieses durch einen Auftragsverarbeiter bereitgestellt wird.

Die Messenger-Applikation muss zunächst verständlich darstellen, was mit den übermittelten Daten, den Verkehrs- und ggf. den Nutzungsdaten, geschieht. Wenn die App dazu genutzt wird, sensitive Daten zu speichern, dann darf sie erst nach Eingabe eines besonderen Passworts und, je nach Risiko, eines zweiten Sicherheitsmerkmals Zugriff auf die gespeicherten Daten gewähren. Speicherung und Übertragung der Daten müssen nach dem Stand der Technik verschlüsselt erfolgen. Soll die App für verschiedene Zwecke zum Einsatz kommen, so sollte sie es ermöglichen, Nachrichten nach ihrem jeweiligen Zweck zu sortieren. Sie benötigt zudem zumindest Funktionen für den Export der gespeicherten Nachrichten und für ihre Löschung.

Der Übermittlungsdienst muss die Nachrichten unverfälscht und von Ende zu Ende verschlüsselt übertragen. Angaben über die Nutzung der App durch Privatnutzende dürfen nur mit Einverständnis der jeweiligen Nutzerinnen und Nutzer durch den Dienste-Anbieter verwendet und an Dritte übermittelt werden. Daten über die Nutzung der App durch Beschäftigte dürfen Unternehmen nur dann durch Auftragnehmer auswerten lassen, wenn hierfür durch z.B. eine Betriebsvereinbarung o. Ä. eine Rechtsgrundlage besteht und die Beschäftigten informiert sind. Die Unternehmen dürfen dann Verkehrsdaten insoweit erheben, speichern und auswerten, wie dies erforderlich ist, um die Übermittlung personenbezogener Daten unter ihrer Verantwortung für legitime Zwecke, darunter insbesondere die Datenschutzkontrolle, nachvollziehen zu können.

Werden sensitive Daten verarbeitet, ist sicherzustellen, dass nur Befugte an dem Nachrichtenaustausch teilnehmen können und die Herkunft der Nachrichten eindeutig erkennbar ist. Die Nachrichten selbst gehören in einen Speicher, aus dem sie für die Weiterverwendung und ggf. Dokumentation durch die jeweilige Stelle entnommen werden können. Soweit keine Übernahme in andere Systeme erfolgt, dienen diese Speicher auch als Datenbestand für Auskünfte an Betroffene, die selbst nicht an der Kommunikation beteiligt waren. Selbstverständlich dürfen die Nachrichten nicht auf Dauer gespeichert bleiben. Vielfach werden die Nachrichteninhalte schon kurze Zeit nach dem Versand nicht mehr benötigt. Dann sind sie auf den genutzten Geräten und, solange keine Aufbewahrungspflichten gelten, auch in dem zentralen Speicher zu löschen.

Die Geräte, meistens Smartphones, die für die Kommunikation verwendet werden, müssen adäquate Sicherheit bieten. Das fängt bei einem aktuell gehaltenen Betriebssystem an. Bekannte Sicherheitslücken müssen zügig geschlossen werden. Damit Schadsoftware auf den Geräten kein Unheil anrichten kann, müssen die Geräte zusätzlich eine sichere Konfiguration erhalten. Die sichere Konfiguration muss sich in Abhängigkeit von den Risiken u. a. auf den Zugriffsschutz der Geräte, die Verschlüsselung der Gerätespeicher, die Kontrolle der Installation von Apps, deren zeitgerechte Aktualisierung und den Schutz der Schnittstellen erstrecken. Zur Steuerung der Konfiguration bedarf es eines zentralen Werkzeugs für das sog. Mobile Device Management. Von der Sensitivität der versandten Nachrichten hängt ab, wie streng diese Konfiguration gehalten werden muss. Sollen z. B. Patientendaten zwischen Beschäftigten in einem Krankenhaus versandt werden, dann müssen über einen zentral gesteuerten Dienst alle Zugangswege für Schadsoftware zu den Geräten geschlossen werden.

Da eine derartige Kontrolle ihrer Privatgeräte den Beschäftigten nicht zugemutet werden kann, muss ein Unternehmen, das von der schnellen Kommunikation unter seinen Beschäftigten profitieren will, in diesen Fällen Smartphones oder Tablets für den Dienstgebrauch zur Verfügung stellen.

Sind öffentliche Messenger im Schulbereich immer tabu?

Sofern ein öffentlicher Messenger-Dienst durch seinen Anbieter datenschutzgerecht erbracht wird (derzeit ist dies für WhatsApp nicht der Fall), kann dieser für

die Kommunikation im Schulbereich eingesetzt werden, wenn die folgenden zusätzlichen Bedingungen erfüllt sind:

- Erstens kann das Angebot, Informationen zum Schulbetrieb über einen Messenger zur Verfügung zu stellen, nur ein für die Betroffenen freiwilliges Angebot darstellen. Es muss gewährleistet sein, dass die Informationen die Schülerinnen und Schüler sowie deren Eltern erreichen, auch ohne dass diese einen Messenger-Dienst nutzen müssen.

- Zweitens bedarf es nach dem Berliner Schulgesetz einer Genehmigung durch die Schulleitung sowie einer Verpflichtung der Lehrkräfte zur Beachtung datenschutzrechtlicher Vorschriften,[1] soweit Lehrkräfte nicht über dienstliche Endgeräte verfügen. Nur in solch engen Ausnahmefällen wäre auch die Nutzung privater Smartphones, Tablets oder Laptops gesetzlich zulässig.

- Drittens ist durch organisatorische Vorgaben sicherzustellen, dass auf den privaten Endgeräten nur Daten mit geringem Schutzbedarf verarbeitet werden. Es dürfen also insbesondere keine Leistungsdaten der Schülerinnen und Schüler oder Gesundheitsdaten über die Messenger-Dienste ausgetauscht werden.

Dies ist in der Praxis jedoch schwer zu gewährleisten. Wir haben deshalb der Senatsverwaltung für Bildung, Jugend und Familie mitgeteilt, dass wir die Notwendigkeit sehen, für das Land Berlin perspektivisch einen eigenen Messenger-Dienst zur Verfügung zu stellen. Dies wäre technisch mit überschaubarem Aufwand auf der Grundlage verfügbarer Software zu realisieren, wie ähnlich gelagerte Projekte in anderen Bundesländern zeigen.

Nichtstun ist keine Option

Ähnliches gilt für andere Bereiche, in denen sensitive Daten verarbeitet werden. Wie bereits dargestellt, werden durchaus bereits Messenger-Dienste für die dienstliche oder betriebliche Kommunikation genutzt, ohne dass dabei die datenschutzrechtlichen Rahmenbedingungen eingehalten werden. Hier gibt es drin-

1 Siehe § 64 Abs. 2 Schulgesetz Berlin

genden Handlungsbedarf. Wie also können und müssen die Verantwortlichen der unzulässigen Nutzung von Messenger-Diensten entgegenwirken?

Ein bloßes Verbot ist keine ausreichende Option. Setzen die Beschäftigten ihre Privatgeräte ein, dann ist eine Kontrolle des Verbots durch Einblick in die Geräte nicht zulässig. Daher muss die jeweilige Institution hinreichend attraktive, aber gleichzeitig rechtskonforme Alternativen anbieten. Sie kann zunächst einen eigenen oder, wo datenschutzrechtlich akzeptabel, einen geeigneten öffentlichen Messenger-Dienst für die allgemeine organisatorische Kommunikation etablieren, bei der keine sensitiven Daten verarbeitet werden. Um die Attraktivität eines solchen betriebsinternen Messenger-Dienstes zu erhöhen und damit die Nutzung ausschließlich dieses Dienstes für dienstliche Zwecke zu erreichen, bietet sich dessen Verknüpfung mit spezifischen betriebsinternen Informationsangeboten an, die z. B. interne Sozialangebote o. Ä. betreffen können. Das Angebot geeigneter dienstlicher Geräte und deren Konfiguration entsprechend den Sicherheitsanforderungen wären die nächsten Schritte, die in eine Freigabe des Messenger-Dienstes auch für die Übermittlung sensitiver Daten innerhalb des jeweiligen Arbeitsbereichs münden können, sobald gesichert ist, dass nur ausreichend geschützte Geräte an der Kommunikation teilnehmen können.

Messenger-Dienste bieten eine willkommene Erleichterung der Kommunikation in den verschiedensten Institutionen. Doch viele gängige Dienste gehen mit datenschutzrechtlich nicht akzeptablen Risiken einher. Um diese zu vermeiden, müssen die jeweiligen Institutionen einen geeigneten Dienst sorgfältig auswählen und auf Risiken prüfen oder selbst betreiben. Nichtstun ist keine Option mehr.

1.2 Künstliche Intelligenz

Aus der Praxis

Künstliche Intelligenz (KI) wird derzeit als Oberbegriff für verschiedene Algorithmen verwendet, die auf automatischem Lernen – zumeist anhand von vielen Beispielen – basieren. Die immer stärkere Nutzung derartiger Algorithmen wird erhebliche Auswirkungen auf die Gesellschaft haben. Besonders relevant sind die Auswirkungen auf die Privatsphäre, da „intelligente" Algorithmen die bereits jetzt angehäuften Datenberge effizient analysieren und nutzen können. Die Frage

ist, zu welchen Zwecken dies geschieht, zu wessen Vorteil und ob betroffene Personen tatsächlich die Möglichkeit erhalten, die Verarbeitung ihrer personenbezogenen Daten zu verstehen und zu kontrollieren.

Ein Haupteinsatzgebiet für Algorithmen der KI sind Entscheidungen unterstützende Systeme, also z.B. Systeme bei Banken, die entscheiden, ob und zu welchen Konditionen Kundinnen und Kunden Kredite gewährt werden oder ob eine bestimmte Nutzung einer Kreditkarte möglicherweise ein Betrugsfall sein könnte.

Dabei kann es zu Fehlentscheidungen kommen, die die Betroffenen oft nur schwer korrigieren können. Werden hierbei Algorithmen eingesetzt, die auf automatischem Lernen basieren (der Fachbegriff lautet Deep Learning), können oft selbst deren Hersteller bzw. Programmierende nicht mehr sagen, weswegen und aufgrund welcher Daten im Einzelfall eine Entscheidung getroffen wurde.

Befürwortende algorithmischer Entscheidungssysteme führen ins Feld, dass Menschen dazu tendieren, voreingenommene Entscheidungen zu treffen. Durch Unterstützung von Algorithmen – eine sorgsame Entwicklung und Prüfung vorausgesetzt – könne erreicht werden, dass weniger falsche bzw. diskriminierende Entscheidungen getroffen würden. So würden autonome Fahrzeuge Unfälle zwar nicht absolut verhindern können. Die Hoffnung sei jedoch, dass die Algorithmen u.a. durch ihre höhere Reaktionsschnelligkeit wesentlich mehr Unfälle verhindern, als dies Menschen in vergleichbaren Situationen möglich wäre.

Dem ist entgegenzuhalten, dass auch derartige Entscheidungssysteme keineswegs unfehlbar sind, es ihnen aber im Vergleich zum Menschen nicht möglich ist, individuell auf Besonderheiten des Einzelfalls einzugehen. Daher kann der unbedachte Einsatz solcher Entscheidungssysteme zu genau gegenteiligen Ergebnissen führen, die keineswegs objektiver als die menschlicher Entscheidungen sind.

Dass es z.B. zur systematischen Diskriminierung von Bevölkerungsgruppen aufgrund unvorhergesehener Interpretationen personenbezogener Daten durch Algorithmen kommen kann, ist bereits bekannt. So wurde bei einem großen Online-Versandhändler eine zur Bewerbungsauswahl eingesetzte Software abgeschaltet, nachdem sich herausgestellt hatte, dass sie auf Grundlage der bisherigen Einstellungspraxis ausschließlich männliche Personen zur Einstellung

auswählte. Die Ursache für derartige Fehlentscheidungen liegt häufig darin, dass bereits die Ausgangsdaten für das Anlernen der Algorithmen, die sog. Trainingsdaten, Vorurteile oder Diskriminierungen abbilden. Die Intransparenz der Algorithmen führt dann dazu, dass Bevorzugung und Benachteiligung von Personengruppen dem System nicht angesehen werden können und erst bei der Anwendung zutage treten.

Der Mangel an Transparenz hat weitere Auswirkungen. Wenn Menschen eine Datenverarbeitung und die mit ihr verbundenen Risiken nicht verstehen, kann eine Entscheidung nicht mehr hinterfragt und begründet werden, eine wirksame Einwilligung in eine solche Datenverarbeitung ist ebenfalls kaum noch möglich. Ein wesentliches Instrument, mit dem Bürgerinnen und Bürger Kontrolle über die Verarbeitung sie betreffender Daten ausüben können, wird damit ausgehöhlt. Besonders deutlich wird dies immer dann, wenn scheinbar harmlose Daten zur Ausführung einer automatisierten Auswertung übergeben werden und sich herausstellt, dass der eingesetzte Algorithmus aus diesen Daten Feststellungen hinsichtlich sensitiver Eigenschaften der jeweiligen Person trifft, zum Beispiel zu ihrer sexuellen Orientierung oder zu psychischen Persönlichkeitsmerkmalen.

Forderungen an automatisierte Entscheidungssysteme

Es wird nicht zu verhindern sein, dass Techniken wie Maschinelles Lernen und KI im Zuge ihrer Weiterentwicklung zukünftig immer mehr eingesetzt werden. Denn natürlich können die genannten Techniken prinzipiell durchaus viele positive Auswirkungen haben, wie z. B. eine höhere Genauigkeit bei medizinischen Diagnosen. Dennoch muss in vielerlei Hinsicht steuernd eingegriffen werden. Die Datenschutzaufsichtsbehörden haben dies erkannt und im Frühjahr eine „Taskforce KI“ ins Leben gerufen, um die auf der 97. Datenschutzkonferenz (DSK) verabschiedete Hambacher Erklärung vorzubereiten, die datenschutzrechtliche Anforderungen an Systeme künstlicher Intelligenz enthält. Diese Hambacher Erklärung wurde auf der 98. DSK im November ergänzt durch ein Positionspapier zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen verbunden mit grundsätzlichen Empfehlungen für eine datenschutzkonforme Ausgestaltung solcher Systeme.

Die von den Aufsichtsbehörden formulierte Erklärung[2] geht auf die von der Bundesregierung veröffentlichte KI-Strategie ein und gibt datenschutzrechtliche Handlungsempfehlungen. Sie geht davon aus, dass für KI-Systeme die Grundsätze zur Verarbeitung personenbezogener Daten[3] gelten und deren Durchsetzung demzufolge auch in diesem Zusammenhang durch technische und organisatorische Maßnahmen sicherzustellen ist[4].

Die in der Erklärung niedergelegten Anforderungen beziehen sich auf sechs verschiedene Bereiche. Im Einklang mit dem Verbot einer ausschließlich automatisierten Entscheidungsfindung[5] dürfen Menschen durch den Einsatz von KI nicht zu Objekten herabwürdigt werden. Der jeweilige Zweck für den Einsatz muss vorab klar definiert werden und sich im verfassungsrechtlich legitimierten Bereich bewegen. Diese Zweckbindung darf auch nicht in Anschlussverwendungen der für das Training der Algorithmen erhobenen Datensätze aufgehoben werden. Weiterhin soll der Einsatz von KI stets transparent, nachvollziehbar und erklärbar gemacht werden, was die Voraussetzung für eine diskriminierungsfreie Anwendung von KI-Systemen ist. Insbesondere die sorgfältige und dem jeweiligen Risiko der Datenverarbeitung angemessene Auswahl der Trainingsdaten ist hier von Bedeutung. Sie müssen korrekt, relevant, repräsentativ und aktuell sein. Auch wenn bei KI-Systemen regelmäßig Daten in großer Menge benötigt werden, um ein hinreichendes Training der Software zu gewährleisten, ist der Grundsatz der Datenminimierung zu beachten. Das sollte vorzugsweise dadurch erfolgen, dass von vornherein anonymisierte Daten verwendet werden. Ist dies nicht möglich, muss der Umfang der verarbeiteten personenbezogenen Daten in angemessenem Verhältnis zu dem mit ihnen erzielten Trainingserfolg stehen. Um die Einhaltung derartiger Grundsätze und die Sicherheit der verarbeiteten Daten zu gewährleisten, ist eine klare Verantwortlichkeit beim Einsatz von KI-Systemen unabdingbar, nicht zuletzt damit die Betroffenen genau wissen, an wen sie sich zur Durchsetzung ihrer Rechte wenden können.

2 https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf
3 Art. 5 Datenschutz-Grundverordnung (DS-GVO)
4 Siehe Art. 25 DS-GVO
5 Art. 22 DS-GVO

Abschließend betonen die Aufsichtsbehörden, wie wichtig die Vornahme technischer und organisatorischer Maßnahmen zur Sicherstellung eines datenschutzkonformen Einsatzes von KI-Systemen ist. Mangels bestehender Standards wird dies im o. g. Positionspapier der DSK konkretisiert. Dabei wird nicht nur der Versuch einer möglichst trennscharfen Definition des Begriffs „KI" anhand des typischen Lebenszyklus eines KI-Systems unternommen. Die Anforderungen der Hambacher Erklärung werden nunmehr näher erläutert und um eine Übersicht zu möglichen technischen und organisatorischen Maßnahmen erweitert. Die Maßnahmen orientieren sich am jeweils aus datenschutzrechtlicher Sicht zu gewährleistenden Ergebnis, also bspw. an der Transparenz über die Herkunft der Daten oder der Minimierung des Personenbezugs der verwendeten Trainingsdaten.

Im Folgenden sollen zwei Schlüsselparameter des Einsatzes von Künstlicher Intelligenz besonders betrachtet werden: Die Frage der Transparenz und der Verzicht auf ausschließlich automatisierte Entscheidungen.

Transparenz

Algorithmische Entscheidungssysteme arbeiten oft intransparent. Anbieterinnen und Anbieter betrachten die interne Logik als Geschäftsgeheimnisse und stellen daher keine ausreichenden Informationen zur Verfügung. Diese Intransparenz ist vor allem dann inakzeptabel, wenn die betreffenden Systeme Entscheidungen treffen, die kritische oder nachteilige Auswirkungen auf betroffene Menschen haben können.

Zum Ausgleich der Interessen der betroffenen Personen und der Anbieterinnen und Anbieter der Entscheidungssysteme ist daher die Offenlegung der eingesetzten Verfahren gegenüber unabhängigen Kontrollinstanzen zu fordern. Neben den Trainingsdaten selbst ist deren Herkunft und die Gewichtung offenzulegen, mit dem sie in den Lernprozess des jeweiligen Algorithmus einfließen; auch sind praktische Tests der Algorithmen zu ermöglichen. Zudem muss dokumentiert werden, wie die Trainingsdaten überprüft wurden, insbesondere auf in ihnen enthaltene systematische Fehler. Der oben erwähnte Algorithmus zur Beurteilung von Bewerbungen z.B. lernte anhand früherer menschlicher Einstellungsentscheidungen.

Ein anderer Grund für begrenzte Transparenz sind die eingesetzten Verfahren. Bei einem sog. neuronalen Netz kann man das Zustandekommen eines Ergebnisses normalerweise nicht ohne Weiteres nachvollziehen oder gar logisch in einer Weise begründen, wie dies eine menschliche Entscheiderin oder ein menschlicher Entscheider tun könnte – es entsteht eine „Black Box". Vor dem Einsatz in kritischen Bereichen wäre daher zu fragen, ob nicht andere Verfahren vorzuziehen sind, deren Funktionsweise leichter nachvollzogen werden kann. Immerhin werden auch bei neuronalen Netzen oder Systemen, die verschiedene Techniken kombinieren, Methoden erforscht, welche die Nachvollziehbarkeit verbessern.

Eine Möglichkeit besteht z.B. darin, einen Entscheidungsprozess mehrfach mit jeweils teilweise veränderten Eingabewerten durchlaufen zu lassen. Auf diese Weise erfährt man, welche Eingabewerte wirklich relevant für ein bestimmtes Ergebnis waren und kann diese Informationen gegenüber den Betroffenen offenlegen.

Auf vollautomatische Entscheidungen verzichten

Wann immer möglich, sollte darauf verzichtet werden, Algorithmen vollautomatische Entscheidungen treffen zu lassen. Art. 22 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) sagt hierzu: „Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt." Vielmehr sollten Algorithmen die Beschäftigten allenfalls bei der Entscheidung durch begründete Empfehlungen unterstützen, sodass Sachbearbeitende nachvollziehbare Entscheidungen treffen können.

Ist dem eingesetzten Algorithmus eine Begründung nicht möglich, darf dieser auch keine Empfehlung aussprechen, sondern allenfalls eine Vorauswahl nachzuprüfender Daten treffen.

Ein Beispiel aus unserer Prüfpraxis: Im Landesverwaltungsamt Berlin erfolgt eine KI-unterstützte Untersuchung von Beihilfe-Rechnungen, um mögliche Betrugsfälle zu identifizieren. Ein Dienstleister untersucht dafür pseudonymisierte Rechnungsverläufe. Die KI markiert lediglich Rechnungsverläufe, die sich signifikant von der Norm unterscheiden. Dies stellt keinen Verdacht oder gar eine Vorverurteilung dar. Denn in jedem Fall erfolgt eine interne manuelle Prüfung der Daten,

aus der sich entweder ergibt, dass die Abweichungen erklärbar sind oder aber ein Verdacht gerechtfertigt ist, dem nachgegangen werden muss.

In zeitkritischen Bereichen, wie z.B. bei der Steuerung autonomer Fahrzeuge, ist die Einbindung eines Menschen in die Entscheidungsprozesse kaum möglich. Hier muss stattdessen noch mehr Wert auf die eingehende Vorprüfung der Algorithmen und eine klare Zuweisung der Verantwortung für mögliche Fehler gelegt werden.

Es gibt Bereiche wie z.B. das Militär, in denen besonders auf der Beschränkung vollautomatischer Entscheidungen bestanden werden muss: Niemals darf ein Algorithmus durch Auslösen einer Waffe darüber entscheiden, ob Menschen sterben. Gegen den Einsatz autonomer Waffen sprechen aber nicht nur ethische Aspekte. Eine derartige Entwicklung würde auch zu einem neuen Rüstungswettlauf und letztlich zur Unkontrollierbarkeit künftiger militärischer Konflikte führen, wenn verschiedene Seiten autonome Systeme einsetzen und menschliche Kommandoketten viel zu langsam sind, um Eskalationen zu verhindern bzw. zu begrenzen.

Ein im ersten Schritt vollautomatisiertes Entscheidungssystem kann jedoch immer dann hingenommen werden, wenn die Auswirkungen für Betroffene gering sind und die getroffenen Entscheidungen revidiert werden können. In diesem Fall wäre es lediglich erforderlich, Einspruchsmöglichkeiten zur Verfügung zu stellen.

Der Einsatz von Algorithmen der KI zur Verarbeitung von personenbezogenen Daten bedarf einer Ausgestaltung, die Datenschutz und ethische Aspekte von vornherein mit einbezieht. Transparenz muss hergestellt, die Auswirkungen für Einzelne und die Gesellschaft müssen betrachtet, Diskriminierungen vermieden und Menschen in ihrer Kontrolle über die Algorithmen und deren Anwendung gestärkt werden. Entwickler und Anwender stehen in der Pflicht, den mit KI erzielbaren Nutzen in einer fairen und die Rechte der betroffenen Personen achtenden Weise zu realisieren.

1.3 Adressvermietung für Werbung

Eine Vielzahl der bei uns eingehenden Beschwerden betrifft die Verarbeitung von Kontaktdaten durch Organisationen[6] für Werbezwecke. Dabei kontaktieren Unternehmen und Organisationen nicht nur Personen, die ihnen ihre Kontaktdaten selbst zur Verfügung gestellt haben. Häufig „mieten" sie Datensätze von anderen Unternehmen, die sie dann für ihre Werbeansprache nutzen. Bei dieser Adressvermietung werden die Datensätze nicht an die werbende Organisation weitergegeben: Die werbende Organisation gibt ein Musterwerbeschreiben an das vermietende Unternehmen. Dieses (oder ein Dienstleistungsunternehmen) fügt dann die vermieteten Adressen in das Schreiben ein und versendet sie. Die mietende Organisation hat in diesem Fall keine Kenntnis, an welche Personen die Werbung im Einzelnen versendet wurde, solange sie nicht über Post-Rückläufer oder Kontaktaufnahmen der Empfängerinnen und Empfänger deren Daten erfahren.

Ist das erlaubt?

Die Frage, inwieweit diese Praxis zulässig ist, war Gegenstand mehrerer Beschwerden, über die wir zu entscheiden hatten. Konkret lagen uns zum Beispiel Beschwerden gegen ein Versandhandelsunternehmen vor. Das Unternehmen hatte zur Abwicklung der Bestellungen die Adressen seiner Kundinnen und Kunden abgefragt und gespeichert. Diese Adressen hat das Unternehmen anschließend ohne Einwilligung der Kundinnen und Kunden an Organisationen vermietet, die für sich werben wollten. Die Beschwerdeführerinnen und Beschwerdeführer erhielten dann insbesondere in der Vorweihnachtszeit Werbeschreiben von einer Reihe von Organisationen, mit denen sie ansonsten nichts zu tun hatten.

Die Verwendung von Postadressen zu Werbezwecken ist gesetzlich nicht (mehr) ausdrücklich geregelt. Die Rechtslage hat sich mit der Einführung der DS-GVO geändert. Bis zum 25. Mai 2018 war im Bundesdatenschutzgesetz (BDSG) geregelt, dass Unternehmen Listen von Adressen, die sie selbst erhoben hatten, zu bestimmten Zwecken grundsätzlich vermieten durften (sog. Listenprivileg). Beruf-

6 Gemeint sind mit diesem Begriff im Folgenden sowohl Unternehmen als auch gemeinnützige Organisationen.

liche Anschriften durften danach für Werbung im beruflichen Kontext vermietet werden, im Übrigen durften Anschriften für Werbung gemeinnütziger Organisationen vermietet werden.[7] Diese Vorschrift ist mit Einführung der DS-GVO weggefallen. Die Vermietung von (Kunden-)Adressen für Werbebriefe unterliegt (nur noch) den allgemeinen Vorschriften der DS-GVO.

Danach können Adressen ohne Einwilligung nur zu Werbezwecken verwendet werden, wenn ein berechtigtes Interesse besteht und soweit schutzwürdige Interessen der Betroffenen nicht entgegenstehen.[8] Bei der Bewertung müssen die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, berücksichtigt werden. Entscheidend ist, ob die Versendung von Werbebriefen in der jeweiligen Sozialsphäre typischerweise akzeptiert oder abgelehnt wird.[9]

In einem konkreten Fall hatte das Unternehmen argumentiert, es liege in seinem berechtigten Interesse, seine Kundendaten zu Werbezwecken zu vermieten. Es hat darauf verwiesen, dass dies auch in seiner allgemeinen Datenschutzerklärung angegeben sei.

Wir sind bei der Interessenabwägung jedoch zu dem Ergebnis gekommen, dass der Vermietung von Kundenadressen zu Werbezwecken in der Regel die schutzwürdigen Interessen der Kundinnen und Kunden entgegenstehen. Denn es entspricht nicht den allgemeinen Erwartungen einer Person, die im Versandhandel etwas bestellt, dass sie in der Folge von diversen Organisationen Werbesendungen erhält.

Kundinnen und Kunden im Versandhandel stellen ihre Adressdaten typischerweise zum Zwecke der Vertragsabwicklung, insbesondere zur Versendung der bestellten Ware, zur Verfügung. Sie erwarten dabei regelmäßig nicht, dass ihre Adresse darüber hinaus einer unbekannten Anzahl dritter Organisationen für Werbezwecke zur Verfügung gestellt wird. Denn zu diesen Organisationen stehen

7 § 28 Abs. 3 Nr. 2 und 3 BDSG a. F.
8 Art. 6 Abs. 1 lit. f DS-GVO
9 EG 47 DS-GVO

sie in keinerlei Beziehung. Dass dies so ist, zeigt sich insbesondere auch an den häufigen Beschwerden gegen diese Praktiken des Adresshandels.

Allein die Tatsache, dass ein Unternehmen über die Vermietung seiner Kundenadressen in der Datenschutzerklärung informiert, führt noch nicht dazu, dass die Kundinnen und Kunden bei Abschluss des Vertrages damit rechnen müssen, unbegrenzt Werbepost zu erhalten. Die Datenschutzerklärung dient nicht dazu, eine Rechtfertigung für Datenverarbeitungen zu schaffen. Verantwortliche müssen erst prüfen, ob eine beabsichtigte Datenverarbeitung erlaubt ist. Erst wenn sie die Zulässigkeit der Verarbeitung feststellen und diese dann vornehmen wollen, müssen sie die betroffene Person informieren.[10] Dagegen wird eine Datenverarbeitung, für die die Rechtsgrundlage fehlt, nicht dadurch zulässig, dass über die Verarbeitung informiert wird.

Im Ergebnis ist eine Vermietung von Kundenadressen zu Werbezwecken ohne Einwilligung im Regelfall unzulässig. Unternehmen, die die Adressen ihrer Kundinnen und Kunden zu Werbezwecken vermieten möchten, müssen sich dafür von diesen regelmäßig eine gesonderte Einwilligung einholen.

Wer ist verantwortlich?

Eine weitere Frage, die wir in diesem Zusammenhang geprüft haben, ist die Frage, wer für diese Form der Datenverarbeitung verantwortlich ist, d.h. gegen wen wir ggf. aufsichtsrechtliche Maßnahmen ergreifen müssen.

Wir erhielten mehrere Beschwerden wegen unerwünschter Werbung von Organisationen, die Adressen für ihre Werbung von anderen Unternehmen gemietet hatten. Die Werbeschreiben wurden im Namen dieser Organisationen versandt und wirkten damit, als kämen sie direkt von dort. Auf unsere Nachfrage beriefen sich diese Organisationen häufig darauf, dass sie für die Datenverarbeitung nicht verantwortlich seien. Schließlich hätten sie selbst die Daten ja nie besessen oder verarbeitet. Dies mag zwar sein, entbindet die betreffenden Organisationen jedoch nicht in jedem Fall von ihrer Verantwortlichkeit. Nach Art. 4 Nr. 7 DS-GVO ist für eine konkrete Datenverarbeitung verantwortlich, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet. Über die

10 Art. 13 DS-GVO

Zwecke und Mittel der Datenverarbeitung kann aber auch entscheiden, wer die Daten nicht selbst verarbeitet, also selbst keinen Zugriff auf sie hat.[11]

Im Fall der Adressvermietung zu Werbezwecken entscheidet die werbende (mietende) Organisation maßgeblich mit über den Zweck der Nutzung der Adressen: Sie ist es, die durch die Adressanmietung die damit verbundene Datenverarbeitung erst initiiert und möglich macht. Sie ist damit auch gemeinsam mit dem vermietenden Unternehmen datenschutzrechtlich verantwortlich für die Verarbeitung. Es ist dementsprechend auch zu aufsichtsrechtlichen Verfahren unserer Behörde gegen Organisationen gekommen, die Adressen zu Werbezwecken angemietet hatten.

Welche Auskunft muss das werbende Unternehmen erteilen?

Häufig wenden sich Empfängerinnen und Empfänger von Werbepost zunächst an die werbende Organisation und fragen dort an, welche Daten von ihnen gespeichert sind und woher diese stammen. Auf diese Auskunft haben sie ein Recht.[12] Regelmäßig erhalten sie dann die schlichte Antwort, es seien keine Daten von ihnen gespeichert. Dies ist im Prinzip auch zutreffend (siehe oben).

Diese Auskunft ist jedoch nicht ausreichend. Denn als gemeinsam für die Verarbeitung Verantwortliche[13] muss auch die werbende Organisation sicherstellen, dass die Betroffenen alle Informationen erhalten, die ihnen zustehen. Dies gilt auch, wenn sie selbst nicht über diese Angaben verfügt. Die werbende Organisation muss dann zumindest identifizieren, von wem sie die entsprechenden Daten gemietet hat, und sicherstellen, dass die Betroffenenrechte durch die vermietende Organisation erfüllt werden.[14]

Unternehmen müssen in der Regel eine Einwilligung der betroffenen Personen einholen, wenn sie deren Adressen zu Werbezwecken an andere Unternehmen oder Organisationen vermieten möchten. Wenn Adressen zu Werbezwecken vermietet werden, sind für diese Datenverarbeitung sowohl die vermietende

11 EuGH, Urteil vom 5. Juni 2018 – C210/16 – Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388, Rn. 38

12 Art. 15 Abs. 1 DS-GVO

13 Siehe Art. 26 DS-GVO

14 Art. 26 Abs. 3 DS-GVO

als auch die werbende Organisation gemeinsam verantwortlich gemäß Art. 26 DS-GVO. Das bedeutet u. a., dass die werbende Organisation dafür mitverantwortlich ist, dass betroffene Personen auf Anfrage alle Informationen erhalten, die ihnen nach Art. 15 DS-GVO zustehen.

1.4 Bußgeldkonzept

Die DSK hat ein Konzept zur Zumessung von Geldbußen bei Verstößen gegen die DS-GVO durch Unternehmen verabschiedet. Ziel des Konzepts ist eine einheitliche, transparente und nachvollziehbare Anwendung der gesetzlichen Vorgaben der DS-GVO zur Bußgeldzumessung[15] durch die deutschen Aufsichtsbehörden. Die Veröffentlichung des Konzepts erfolgte, nachdem erste Verhandlungen auf europäischer Ebene zur konkreten Bußgeldzumessung stattgefunden hatten, in denen die Entwurfsfassung des Konzepts durch die deutsche Vertretung eingebracht worden war.

Erklärtes Ziel der DS-GVO ist die Vereinheitlichung der Bußgeldpraxis.[16] Es gibt eine ausdrückliche Regelung, nach der eine Harmonisierung der Festsetzung von Geldbußen durch Leitlinien zu fördern ist.[17] Bereits am 25. Mai 2018 hat daher der Europäische Datenschutzausschuss (EDSA) in seiner ersten Plenarsitzung Leitlinien für die Anwendung und Festsetzung von Geldbußen angenommen.[18] Diese Leitlinien umreißen ein einheitliches Konzept zu den Grundsätzen bei der Festsetzung von Geldbußen, enthalten jedoch noch keine Konkretisierung der Festsetzungsmethodik. Sie bleibt späteren Leitlinien des EDSA vorbehalten, deren Inhalt derzeit auf europäischer Ebene diskutiert wird.

Bis der EDSA endgültige Leitlinien erstellt hat, soll das Bußgeldkonzept der deutschen Aufsichtsbehörden Grundlage für die Sanktionspraxis in Deutschland sein, um die Anwendung einheitlicher Maßstäbe bei der Zumessung der Bußgelder sicherzustellen. Aufgrund der noch fehlenden praktischen Erfahrungen sind Ver-

15 Art. 83 DS-GVO
16 EG 150 DS-GVO
17 Art. 70 Abs. 1 lit. k DS-GVO
18 Bestätigung des WP 253 der Artikel-29-Datenschutzgruppe vom 3. Oktober 2017

änderungen und Ergänzungen sowohl des Konzepts als auch der Praxis der Aufsichtsbehörden durch neue Erkenntnisse aus den europaweiten Abstimmungen in der Zukunft möglich.

Das Bußgeldkonzept wurde vom Arbeitskreis Sanktionen der DSK unter Vorsitz unserer Aufsichtsbehörde entwickelt. Es findet bei der Bußgeldzumessung in Verfahren gegen Unternehmen im Anwendungsbereich der DS-GVO, nicht jedoch bei Geldbußen gegen Vereine oder natürliche Personen außerhalb ihrer wirtschaftlichen Tätigkeit Anwendung. Das Konzept entfaltet auch keine Bindung hinsichtlich der Festlegung von Geldbußen durch Gerichte.

Bei der Entwicklung des Bußgeldkonzepts haben sich die Beteiligten zunächst an den Verfahren zur Bußgeldzumessung durch die Bundesanstalt für Finanzdienstleistungsaufsicht und durch das Bundeskartellamt orientiert. Beide Institutionen bemessen das konkrete Bußgeld auf der Grundlage der Größe der zu sanktionierenden Stelle, die mithilfe deren Jahresumsatzes einer bestimmten Größengruppe zugeordnet wird, sowie der Schwere des Einzelfalls.

Im Hinblick auf die Ermittlung eines Grundbetrags, der Basis für die Berechnung des konkreten Bußgeldbetrags ist, haben sich die Beteiligten darüber hinaus an den im deutschen Strafrecht der Berechnung von Geldstrafen zugrundeliegenden sog. Tagessätzen orientiert. Tagessätze sind eine Berechnungseinheit für Geldstrafen, die mittels des durchschnittlichen Tageseinkommens der Beschuldigten gebildet wird.

Die konkrete Bußgeldzumessung erfolgt laut Bußgeldkonzept in fünf Schritten: Zunächst wird das betroffene Unternehmen einer Größenklasse zugeordnet (1.), danach wird der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt (2.), dann ein wirtschaftlicher Grundwert ermittelt (3.), dieser Grundwert mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert (4.) und abschließend der unter 4. ermittelte Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst (5.).

1. Kategorisierung der Unternehmen nach Größenklassen

Das betroffene Unternehmen wird anhand seiner Größe einer von vier Größenklassen (A bis D) zugeordnet (Tabelle 1).

Die Größenklassen richten sich nach dem gesamten weltweit erzielten Vorjahresumsatz der Unternehmen[19] und sind unterteilt in Kleinstunternehmen, kleine und mittlere Unternehmen (KMU) sowie Großunternehmen. Es gilt gemäß EG 150 DS-GVO der Begriff „Unternehmen" i.S.d. Artikel 101 und 102 AEUV[20] (sog. funktionaler Unternehmensbegriff).

Die Größeneinordnung der KMU orientiert sich hinsichtlich des Vorjahresumsatzes grundsätzlich an der Empfehlung der Kommission vom 6. Mai 2003 (2003/361/EG).

Die Größenklassen werden zur konkreteren Einordnung der Unternehmen nochmals in Untergruppen unterteilt (A.I bis A.III, B.I bis B.III, C.I bis C.VII, D.I bis D.VII).

Tabelle 1

Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU)				Großunternehmen	
Unterscheidung nach Jahresumsätzen in Millionen €					
A		B		C		D	
Kleinstunternehmen: ⩽2		Kleine Unternehmen: ⩾2–10		Mittlere Unternehmen: ⩾10–50		Großunternehmen: ⩾50	
A.I	⩽0,7	B.I	⩾2–5	C.I	⩾10–12,5	D.I	⩾50–75
A.II	⩾0,7–1,4	B.II	⩾5–7,5	C.II	⩾12,5–15	D.II	⩾75–100
A.III	⩾1,4–2	B.III	⩾7,5–10	C.III	⩾15–20	D.III	⩾100–200
				C.IV	⩾20–25	D.IV	⩾200–300
				C.V	⩾25–30	D.V	⩾300–400
				C.VI	⩾30–40	D.VI	⩾400–500
				C.VII	⩾40–50	D.VII	⩾500

19 Siehe Art. 83 Abs. 4 bis 6 DS-GVO

20 Vertrag über die Arbeitsweise der Europäischen Union

2. Bestimmung des mittleren Jahresumsatzes der jeweiligen Untergruppe der Größenklasse

Dann wird der mittlere Jahresumsatz der Untergruppe, in die das Unternehmen eingeordnet wurde, bestimmt (Tabelle 2). Dieser Schritt dient der Veranschaulichung der darauf aufbauenden Ermittlung des wirtschaftlichen Grundwertes (3.).

Tabelle 2

Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU)						Großunternehmen	
Unterscheidung nach Jahresumsätzen in Millionen €							
A		B		C		D	
A.I	0,35	B.I	3,50	C.I	11,25	D.I	62,50
A.II	1,05	B.II	6,25	C.II	13,75	D.II	87,50
A.III	1,70	B.III	8,75	C.III	17,50	D.III	150,00
				C.IV	22,50	D.IV	250,00
				C.V	27,50	D.V	350,00
				C.VI	35,00	D.VI	450,00
				C.VII	45,00	D.VII	konkreter Jahresumsatz*

** Ab einem jährlichen Umsatz von über 500 Mio. Euro ist der prozentuale Bußgeldrahmen von 2 % bzw. 4 % des jährlichen Umsatzes als Höchstgrenze zugrunde zu legen, sodass beim jeweiligen Unternehmen eine Berechnung anhand des konkreten Umsatzes erfolgt.*

3. Ermittlung des wirtschaftlichen Grundwertes

Für die Festsetzung des wirtschaftlichen Grundwertes wird der mittlere Jahresumsatz der Untergruppe, in die das Unternehmen eingeordnet wurde, durch 360 (Tage) geteilt und so ein durchschnittlicher, auf die Vorkommastelle aufgerundeter Tagessatz errechnet (Tabelle 3).

Tabelle 3

Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU)				Großunternehmen			
Unterscheidung nach Jahresumsätzen in €							
A		B		C		D	
A.I	972	B.I	9.722	C.I	31.250	D.I	173.611
A.II	2.917	B.II	17.361	C.II	38.194	D.II	243.056
A.III	4.722	B.III	24.306	C.III	48.611	D.III	416.667
				C.IV	62.500	D.IV	694.444
				C.V	76.389	D.V	972.222
				C.VI	97.222	D.VI	1.250.000
				C.VII	125.000	D.VII	konkreter Tagessatz*

** Ab einem jährlichen Umsatz von über 500 Mio. Euro ist der prozentuale Bußgeldrahmen von 2 % bzw. 4 % des jährlichen Umsatzes als Höchstgrenze zugrunde zu legen, sodass beim jeweiligen Unternehmen eine Berechnung anhand des konkreten Umsatzes erfolgt.*

4. Multiplikation des Grunwertes nach Schweregrad der Tat

Danach erfolgt anhand der konkreten tatbezogenen Umstände des Einzelfalls (vgl. Art. 83 Abs. 2 Satz 2 DS-GVO) eine Einordnung des Schweregrads der Tat in leicht, mittel, schwer oder sehr schwer.

Hierfür werden gemäß der nachstehenden Tabelle 4 unter Berücksichtigung der Umstände des Einzelfalls anhand des Kriterienkatalogs des Art. 83 Abs. 2 DS-GVO der Schweregrad des Tatvorwurfs und der jeweilige Faktor ermittelt, mit dem der Grundwert multipliziert wird. Im Hinblick auf die unterschiedlichen Bußgeldrahmen sind dabei für formelle (Art. 83 Abs. 4 DS-GVO) und materielle (Art. 83 Abs. 5, 6 DS-GVO) Verstöße jeweils unterschiedliche Faktoren zu wählen. Bei der Wahl des Multiplikationsfaktors einer sehr schweren Tat ist zu beachten, dass der einzelfallbezogene Bußgeldrahmen nicht überschritten wird.

Tabelle 4

Schweregrad der Tat	Faktor für formelle Verstöße gemäß Art. 83 Abs. 4 DS-GVO	Faktor für materielle Verstöße gemäß § 83 Abs. 5, 6 DS-GVO
leicht	1–2	1–4
mittel	2–4	4–8
schwer	4–6	8–12
sehr schwer	>6	>12

5. Anpassung des Grundwertes anhand aller sonstigen für und gegen die Betroffenen sprechenden Umstände

Der unter 4. errechnete Betrag wird anhand aller für und gegen die Betroffene oder den Betroffenen sprechenden Umstände angepasst, soweit diese noch nicht unter 4. berücksichtigt wurden. Hierzu zählen insbesondere sämtliche täterbezogenen Umstände (vgl. Kriterienkatalog des Art. 83 Abs. 2 DS-GVO) sowie sonstige Umstände, wie z.B. eine lange Verfahrensdauer oder eine drohende Zahlungsunfähigkeit des Unternehmens.

Das Bußgeldkonzept garantiert eine nachvollziehbare, transparente und einzelfallgerechte Form der Bußgeldzumessung. Gleichzeitig wird es durch die Berücksichtigung aller Umstände im konkreten Verfahren dem Einzelfall gerecht. Hierdurch wird eine umfassende gerichtliche Überprüfbarkeit und Nachvollziehbarkeit der Bußgeldzumessung möglich.

1.5 Die Kooperation der Datenschutzaufsichtsbehörden der EU nimmt Fahrt auf! – Die Servicestelle Europaangelegenheiten

Die DS-GVO verpflichtet die Datenschutzaufsichtsbehörden der EU-Mitgliedsstaaten, bei grenzüberschreitenden Datenverarbeitungen eng zu kooperieren. Um dieser neuen Aufgabe gerecht zu werden, hat unsere Behörde die Servicestelle Europaangelegenheiten eingerichtet.

Eingehende Beschwerden – aber auch alle Fälle, die wir von Amts wegen aufgreifen sowie von Unternehmen gemeldete Datenpannen – werden zunächst daraufhin geprüft, ob die beanstandete Verarbeitung personenbezogener Daten eine grenzüberschreitende Datenverarbeitung betrifft.[21] Dies ist vor allem dann der Fall, wenn die oder der Verantwortliche in mehr als einem Mitgliedsstaat der EU niedergelassen ist und die Verarbeitung in mehreren dieser Niederlassungen erfolgt. Selbst in Fällen nur einer einzigen Niederlassung in der EU kann jedoch ebenfalls eine grenzüberschreitende Verarbeitung vorliegen, wenn die Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedsstaat hat oder haben kann.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit erhält dementsprechend nicht nur Beschwerden gegen Berliner Unternehmen und Behörden, sondern auch Beschwerden, die Unternehmen mit Hauptsitz in anderen EU-Mitgliedsstaaten betreffen. Nach dem sog. One-Stop-Shop-Prinzip ist bei einer grenzüberschreitenden Datenverarbeitung die Aufsichtsbehörde am Hauptsitz des Unternehmens als federführende Aufsichtsbehörde die alleinige Ansprechpartnerin für die Verantwortlichen.

Die DS-GVO sieht vor, dass zwischen den europäischen Aufsichtsbehörden ein Kooperationsverfahren durchgeführt wird und beabsichtigte Maßnahmen zwischen diesen abzustimmen sind.[22] Aus diesem Grund erfolgt bei grenzüberschreitenden Fällen eine Prüfung, ob in die Fallbearbeitung neben der federführenden Aufsichtsbehörde auch andere betroffene Aufsichtsbehörden einzubeziehen sind.

Die Abstimmung bei derartigen Sachverhalten erfolgt über das mit Inkrafttreten der DS-GVO eingerichtete elektronische Binnenmarkt-Informationssystem (IMI). Über IMI findet die komplette Kommunikation zwischen allen europäischen Aufsichtsbehörden statt. Eingehende Beschwerden mit grenzüberschreitendem Bezug meldet unsere Servicestelle Europaangelegenheiten in einem ersten Schritt im IMI zur Bestimmung der federführenden und der betroffenen Aufsichtsbehörden ein.[23] Hierfür eröffnet sie einen neuen Vorgang im System, fasst den Inhalt

21 Art. 4 Nr. 23 DS-GVO
22 Art. 56, 60 ff. DS-GVO
23 Art. 56 DS-GVO

der Beschwerde zusammen und nennt die mutmaßlich federführende sowie die mutmaßlich betroffenen Aufsichtsbehörden. Daraufhin haben die verschiedenen Behörden einen Monat Zeit, um den Vorgang zu überprüfen und sich als betroffene bzw. federführende Behörde zu melden. Auch wenn von einer Federführung der Berliner Beauftragten für Datenschutz und Informationsfreiheit auszugehen ist, meldet die Servicestelle die Beschwerde im IMI ein, um andere betroffene Behörden zu informieren.

Die Feststellung der federführenden Aufsichtsbehörde verläuft allerdings nicht in allen Fällen problemlos. In einem Fall beschwerte sich eine Beschwerdeführerin z.B. über ein Unternehmen, welches seine Dienstleistungen an deutschsprachige Kunden richtet, aber gemäß Datenschutzerklärung den Hauptsitz in einem anderen Mitgliedsstaat hat. Die Aufsichtsbehörde dieses Mitgliedsstaates teilte jedoch mit, dass das Unternehmen dort nicht registriert und auch kein Standort zu ermitteln sei. Nachdem unsere Behörde die Zweigniederlassung in Berlin kontaktiert hatte, setzte uns diese in Kenntnis, dass die Zweigniederlassung zwischenzeitlich aufgegeben worden sei und sich die Hauptniederlassung in einem weiteren Mitgliedsstaat befinde.

Wenn in dem beschriebenen Verfahren bestätigt wird, dass die Federführung bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit liegt, bearbeiten wir die Beschwerde weiter und kontaktieren die oder den Verantwortlichen. Für den Fall, dass die Federführung bei einer anderen europäischen Aufsichtsbehörde liegt, übermittelt die Servicestelle Europaangelegenheiten die Beschwerde zur Bearbeitung an die betreffende Behörde. Hierzu muss die Beschwerde ins Englische übersetzt werden, da die Kommunikation zwischen den verschiedenen Aufsichtsbehörden auf Englisch stattfindet.

Die federführende Aufsichtsbehörde übernimmt die weitere Ermittlung des Sachverhalts und entwirft nach Abschluss der Prüfung einen Beschluss, den sie allen betroffenen Aufsichtsbehörden mitteilt. Diese haben dann vier Wochen Zeit, um den Entwurf zu prüfen. Innerhalb dieser Frist können sie Einspruch gegen den Entwurf einlegen.[24] So wird sichergestellt, dass ein Konsens zwischen den euro-

24 Art. 60 Abs. 4 DS-GVO

päischen Aufsichtsbehörden über die rechtliche Bewertung des jeweiligen Falls besteht.

Im IMI wurden 2019 rund 822 Fälle zur Bestimmung der federführenden und der betroffenen Aufsichtsbehörden gemeldet. Sämtliche Fälle wurden in der Servicestelle Europaangelegenheiten auf eine mögliche Betroffenheit bzw. Federführung der Berliner Beauftragten für Datenschutz und Informationsfreiheit geprüft. In über 390 Fällen, also knapp der Hälfte der Fälle, wurde eine Betroffenheit unserer Behörde festgestellt, sodass wir uns inhaltlich mit den jeweiligen Sachverhalten befassen mussten.

Unsere Behörde bearbeitet aktuell 35 Beschwerden, die uns von anderen Aufsichtsbehörden zur federführenden Bearbeitung übermittelt wurden. Zudem haben wir unsererseits bereits eine Vielzahl von Beschwerden von Betroffenen erhalten, die wir zur weiteren Bearbeitung an andere Aufsichtsbehörden übermitteln mussten, weil die Federführung nicht bei uns lag. Auch in diesen Fällen bleiben wir jedoch Ansprechpartnerin für die Beschwerdeführerinnen und Beschwerdeführer und informieren diese regelmäßig über den Stand der Bearbeitung.

Die Anzahl der im IMI gemeldeten Beschwerden, Amtsermittlungsverfahren und Datenpannen ist stetig gestiegen. Allerdings fällt auf, dass die Aufsichtsbehörden in der Zwischenzeit für viele Unternehmen bereits abschließend geprüft haben, wer federführende Aufsichtsbehörde ist, sodass viele eingehende Beschwerden direkt übermittelt werden können und die Verfahren sich dadurch bereits beschleunigen. Dies führt auch zu einer Zunahme von Beschlussentwürfen, die zur Abstimmung zwischen den europäischen Aufsichtsbehörden im IMI veröffentlicht werden.

Unsere Behörde hat bereits in mehreren Fällen Einsprüche gegen Beschlussentwürfe anderer Aufsichtsbehörden eingelegt, sodass diese von der federführenden Behörde erneut überarbeitet werden mussten. Dies betraf z.B. einen Fall, in dem die federführende Aufsichtsbehörde inhaltlich überhaupt nicht auf einen in der Beschwerde gerügten Datenschutzverstoß eingegangen war. Sie plante trotz eines klar vorliegenden Datenschutzverstoßes darüber hinaus, das Verfahren einzustellen. Mithilfe des Einspruchs will unsere Behörde in diesem noch nicht abgeschlossenen Fall erreichen, dass der Datenschutzverstoß festgestellt

und entsprechende aufsichtsrechtliche Maßnahmen durch die federführende Aufsichtsbehörde getroffen werden.

Dass gegen Beschlussentwürfe in Fällen mit grenzüberschreitendem Bezug mithilfe von Einsprüchen vorgegangen werden kann, sieht das Kooperationsverfahren zwischen den Aufsichtsbehörden ausdrücklich vor. Auf diese Weise können die Entscheidungen der Behörden gegenseitig überprüft werden, bis eine Einigung erzielt wird oder ein Streitverfahren zwischen den Aufsichtsbehörden vor dem EDSA landet, der mit Inkrafttreten der DS-GVO eingerichtet wurde, um auf Arbeitsebene nicht lösbare Fälle abschließend und verbindlich für alle EU-Aufsichtsbehörden zu entscheiden.

Ein besonderes Problem verursacht die Anwendung von unterschiedlichen nationalen Verfahrensvorschriften. In einigen Mitgliedsstaaten[25] ist bspw. eine sog. gütliche Einigung als verfahrensbeendende Maßnahme vorgesehen. Durch diese Maßnahme werden zahlreiche Beschwerden von einigen Aufsichtsbehörden zwischen dem verantwortlichen Unternehmen und der Beschwerdeführerin bzw. dem Beschwerdeführer beigelegt. Die Beschwerde gilt dann als zurückgezogen und der Datenschutzverstoß wird weder festgestellt noch einer aufsichtsrechtlichen Maßnahme unterworfen.[26] In der DS-GVO ist eine gütliche Einigung als verfahrensbeendende Maßnahme allerdings nicht vorgesehen, mit Ausnahme der Nennung in einem Erwägungsgrund, der jedoch nur für einen spezifischen eingeschränkten Anwendungsbereich gilt.[27] Dies führte zu Konflikten zwischen den beteiligten Aufsichtsbehörden. Nach unserer Auffassung ist die Anwendung von gütlichen Einigungen als verfahrensbeendende Maßnahme äußerst problematisch. Denn mit der gütlichen Einigung könnte das in der DS-GVO vorgesehene Abstimmungsverfahren zwischen den Aufsichtsbehörden umgangen werden, wenn die Beschwerdeführerin oder der Beschwerdeführer auf die Geltendmachung von Betroffenenrechten verzichtet und der Datenschutzverstoß nicht sanktioniert wird. Die Anwendung eines solchen nationalen rechtlichen Instrumentariums kann

25 So in Österreich, Belgien, Tschechien, Finnland, Griechenland, Ungarn, Irland, Italien, Litauen, Lettland, Niederlande, Polen, Schweden, Slowakei, Großbritannien, Estland. In Deutschland ist eine gütliche Einigung im Datenschutzrecht nicht geregelt.

26 Art. 58 Abs. 2 DS-GVO

27 EG 131 DS-GVO

europarechtlich nicht gewollt sein, weil dadurch die angestrebte europäische Einigung im Bereich des Datenschutzes behindert wird.

Wie bereits erwähnt, entscheidet der EDSA in Fällen, in denen sich die Aufsichtsbehörden nicht über die Federführung oder über die rechtliche Bewertung eines Sachverhalts einigen. Das in der DS-GVO für solche Fälle vorgesehene sog. Kohärenzverfahren[28] soll für ein einheitliches Datenschutzniveau in den Mitgliedsstaaten sorgen. Bei Streitfällen zwischen den Aufsichtsbehörden erlässt der EDSA einen verbindlichen Beschluss zur Klärung der Streitfrage in Fällen, in denen die betroffene Aufsichtsbehörde einen Einspruch gegen einen Beschlussentwurf der federführenden Aufsichtsbehörde eingelegt hat.[29]

Einem Beispiel aus unserer Fallpraxis liegt eine Beschwerde zugrunde, die in unserer Behörde eingegangen ist und von der Aufsichtsbehörde eines anderen Mitgliedsstaates als federführende Behörde bearbeitet wurde. Der Beschwerdeführer rügt eine fehlerhafte Datenschutzerklärung auf der Webseite eines Möbelunternehmens. Außerdem beschwert sich der Betroffene über einen unzulässigen Einsatz von Cookies auf der Webseite des Unternehmens. Im Rahmen des Kooperationsverfahrens hat die federführende Aufsichtsbehörde den anderen betroffenen Aufsichtsbehörden zunächst einen Beschlussentwurf zur Abstimmung vorgelegt.[30] Darin stellte die federführende Aufsichtsbehörde keinen Datenschutzverstoß fest, sondern kündigte die Einstellung des Verfahrens an. Da nach unserer Einschätzung jedoch mehrere Datenschutzverstöße vorlagen, haben wir Einspruch gegen diese Entscheidung eingelegt. Wir haben vorgetragen, dass das Unternehmen z.B. gegen Transparenzvorschriften verstoßen hat. Außerdem wurden Nutzende in der Datenschutzerklärung nur generell über den Einsatz von Cookies informiert, aber weder in Bezug auf den Einsatz und die Nutzung von Analysediensten noch in Bezug auf die Einbindung von Drittanbietern (Facebook, Twitter, Criteo). Da auch der überarbeitete Beschlussentwurf der federführenden Aufsichtsbehörde diese Mängel nicht beseitigte, muss nun der EDSA im Kohärenzverfahren über den Fall entscheiden, falls die federführende Aufsichtsbehörde nicht doch noch nachbessert.

28 Art. 63 DS-GVO

29 Art. 65 Abs. 1 lit. a DS-GVO

30 Siehe Art. 60 Abs. 3 S. 2 DS-GVO

Das europäische Kooperationsverfahren ist im Jahr nach Wirksamwerden der DS-GVO mit Leben gefüllt worden. Unsere Behörde arbeitet in einer Vielzahl von Fällen mit anderen Aufsichtsbehörden zusammen. Konflikte zwischen den Aufsichtsbehörden sind bislang eher selten und werden in der Regel einvernehmlich gelöst, sodass der EDSA noch keine Entscheidung treffen musste. Eine solche könnte aber bald bevorstehen.

2 Digitale Verwaltung und Justiz

2.1 Berliner Verwaltung auf Erfolgskurs?

Online-Portale werden zum virtuellen Eingang ins Rathaus. Mit wenigen Klicks sollen Bürgerinnen, Bürger und Unternehmen ihre Anliegen und Ansprüche digital geltend machen und vollständig elektronisch abwickeln können.

Aktueller Stand der Digitalisierung

Das im August 2017 vom Bundesgesetzgeber erlassene Onlinezugangsgesetz (OZG) gibt vor, dass bis Ende 2020 Verwaltungsleistungen für Bürgerinnen, Bürger und Unternehmen online zur Verfügung stehen müssen, wobei herkömmliche Zugangswege, z. B. postalisch oder über ein Bürgeramt, weiterhin offenstehen sollen. Mit der Einrichtung eines Portalverbundes sollen alle Verwaltungsportale von Bund, Ländern und Kommunen miteinander vernetzt werden. Von jedem Standort aus soll es künftig möglich sein, jeden Online-Dienst in Anspruch zu nehmen.

Die Koordination der Umsetzung des OZG erfolgt gemeinsam durch das Bundesministerium des Innern, für Bau und Heimat (BMI) und die Föderale IT-Kooperation (FITKO), die die Zusammenarbeit zwischen Bund, Ländern und Kommunen koordiniert. Der Bund und die Länder haben unter Einbeziehung der Kommunen 575 zu digitalisierende Verwaltungsdienstleistungen identifiziert, die in 14 verschiedene Themenfelder zusammengefasst wurden. Jedes Themenfeld soll nun federführend in jeweils einem Tandem aus Vertreterinnen und Vertretern des fachlich zuständigen Landesministeriums und des fachlich zuständigen Bundesressorts bearbeitet werden, unterstützt von Vertreterinnen und Vertretern anderer interessierter Bundesländer. Die Vorbereitung der Digitalisierung der konkreten Verwaltungsdienstleistungen für die einzelnen Themenfelder erfolgt behördenübergreifend gemeinsam durch die Fachleute aus Bund und Ländern in diesen Tandem-Gruppen. Die entwickelten Lösungen können dann von allen Bundesländern übernommen werden.

Das Land Berlin ist zusammen mit dem BMI federführend für das Themenfeld „Querschnitt" zuständig. Dabei geht es um Verwaltungsdienstleistungen, die in mehreren Themenkomplexen Anwendung finden; dazu zählen z.B. digitale Nachweise, wie etwa die Vorlage einer Geburtsurkunde. Sollte im Rahmen der Erbringung einer elektronischen Verwaltungsdienstleistung also z.B. die Vorlage einer Geburtsurkunde notwendig sein, so könnte dies auf verschiedenen Wegen realisiert werden. Um Medienbrüche zu vermeiden, wäre es denkbar, dass die Daten der Geburtsurkunde mit Einwilligung der Nutzenden direkt beim jeweiligen Geburtenregister abgefragt werden. Auch ein Hochladen einer eingescannten Geburtsurkunde durch die Nutzenden in ein Verwaltungsportal erscheint möglich. Sollte dies jedoch nicht gewünscht sein, soll es auch weiterhin möglich bleiben, eine Kopie des Nachweises in Papierform einzureichen.

Bei zunehmender Digitalisierung der Verwaltungsdienstleistungen sind erhöhte Anforderungen an die Transparenz des Verwaltungshandelns gegenüber den Nutzenden zu stellen. Art. 5 der Datenschutz-Grundverordnung (DS-GVO) legt die wesentlichen Grundsätze für die Verarbeitung personenbezogener Daten fest. Personenbezogene Daten dürfen nur auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden[31]. Besondere Bedeutung kommt hierbei dem sog. Datenschutzcockpit zu. Mit dem Datenschutzcockpit soll den Bürgerinnen und Bürgern veranschaulicht werden, welche Daten von ihnen, im Rahmen der Erbringung einer elektronischen Verwaltungsdienstleistung, „von wo nach wo" fließen. Die Anforderungen an ein Datenschutzcockpit werden derzeit in einem sog. Digitalisierungslabor unter Beteiligung verschiedenster Akteure[32] definiert. Wir sind daran beteiligt.

Aktueller Stand der Landesgesetzgebung

Im Rahmen der Umsetzung des Onlinezugangsgesetzes des Bundes (OZG) hat das Land Berlin landesrechtliche Regelungen für die Umsetzung der Verwaltungsdigitalisierung vorbereitet. In unserem letzten Jahresbericht haben wir darüber informiert, dass der Senator für Inneres und Sport einen Entwurf eines Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen der Berliner Ver-

31 Art. 5 Abs. 1 lit. a DS-GVO

32 U.a. Bundesministerium des Inneren, für Bau und Heimat sowie verschiedene Fachverwaltungen, darunter die Senatsverwaltung für Inneres und Sport Berlin, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit etc.

waltung (Onlinezugangsgesetz Berlin – OZG Bln) vorgelegt hatte[33]. In diesem Jahr wurde das parlamentarische Gesetzgebungsverfahren eingeleitet. Da unsere im Vorwege geäußerten Kritikpunkte nur unzureichend berücksichtigt wurden, haben wir diese noch einmal gegenüber den federführenden Fachausschüssen vorgebracht. Erfreulicherweise hat dies dazu geführt, dass wir noch einmal mit der Senatsverwaltung für Inneres und Sport in den fachlichen Diskurs eintreten und erhebliche datenschutzrechtliche Verbesserungen erreichen konnten.

Immer wieder hatten wir darauf hingewiesen, dass es erforderlich und zweckmäßig ist, eigene gesetzliche Grundlagen für die Verarbeitung personenbezogener Daten im Service-Konto-Berlin und den anderen IKT-Basisdiensten[34] zu schaffen. Die Datenverarbeitung allein auf die Einwilligung der Nutzenden zu stützen, wie es von der Senatsverwaltung für Inneres und Sport zunächst vorgesehen war, würde in der praktischen Umsetzung schon deshalb zu erheblichen Schwierigkeiten führen, da Einwilligungen jederzeit auch widerrufen werden können. Es ist sehr erfreulich, dass die Senatsverwaltung letztlich unserem Rat gefolgt ist. Denn für die Sicherstellung der Freiwilligkeit der Inanspruchnahme des digitalen Angebots war die Einführung einer Einwilligung nicht erforderlich. Die Freiwilligkeit der Inanspruchnahme des digitalen Angebots wird sichergestellt durch die Festlegung im E-Government-Gesetz Berlin[35], dass Bürgerinnen und Bürger auch weiterhin darüber entscheiden können, ob sie eine Dienstleistung auf herkömmliche Art oder aber elektronisch beantragen möchten.

Im Sinne möglichst optimaler Transparenz des Verwaltungshandelns war es uns darüber hinaus wichtig, dass eine Regelung im Gesetz sicherstellt, dass Bürgerinnen und Bürger in Fällen, in denen die für eine Dienstleistung beizubringenden Nachweise (z.B. eine Urkunde) unmittelbar aus anderen Registern angefordert oder abgerufen werden, diese vorab noch einmal einsehen können.

33 JB 2018, 2.1

34 Hierbei handelt es sich um informations- und kommunikationstechnische Anwendungen, die von verschiedenen Verwaltungsverfahren öffentlicher Stellen genutzt werden, um elektronische Verwaltungsleistungen zu erbringen.

35 § 4 Abs. 7 E-Government-Gesetz Berlin

Die Digitalisierung von Verwaltungsdienstleistungen kann nur erfolgreich verlaufen, wenn die Nutzenden bereit sind, diese wahrzunehmen. Für die notwendige Akzeptanz ist eine weitreichende Transparenz des elektronischen Verwaltungshandelns unabdingbar. Hierbei helfen klare gesetzliche Regelungen. Wir werden diesen Prozess weiterhin aktiv begleiten.

2.2 Digitales Schlüsselbrett für Behörden erforderlich

Aus der Praxis

Berliner Behörden verständigen sich immer mehr mithilfe von digitalen Kommunikationsmitteln, wie z.B. per E-Mail. Dies gilt sowohl für die Kommunikation zwischen den Behörden und Bürgerinnen und Bürgern als auch für die Kommunikation der Behörden untereinander. Die Vertraulichkeit der so übertragenen Nachrichten ist dabei sicherzustellen. Ganz besonders wichtig ist die Vertraulichkeit, wenn durch diese Nachrichten sensitive Daten wie etwa Gesundheits- oder Sozialdaten übertragen werden.

Sowohl die Absendenden als auch die Empfängerinnen und Empfänger elektronischer Kommunikation müssen technische und organisatorische Maßnahmen ergreifen, die geeignet sind, den Schutz der Vertraulichkeit der übertragenen Nachrichten zu garantieren. Dabei ist es die Aufgabe der empfangenden Stellen, eine Möglichkeit zu schaffen, Nachrichten vertraulich entgegenzunehmen. Aufgabe der Absendenden ist es, diese Möglichkeit zu nutzen. Eine geeignete Maßnahme hierfür ist die Verschlüsselung, insbesondere die Ende-zu-Ende-Verschlüsselung. Bei der Ende-zu-Ende-Verschlüsselung werden die Nachrichten vor dem Versand mit einem Schlüssel gesichert und erst danach versandt. Bevor die Nachricht gelesen werden kann, muss sie zunächst wieder mithilfe des zugehörigen Schlüssels entschlüsselt werden, der nur den Empfangsberechtigten bekannt ist. Wird eine verschlüsselte Nachricht auf dem Weg zu den Empfängerinnen und Empfängern abgefangen oder kopiert, können unbefugte Dritte die Nachricht trotzdem nicht lesen, da sie nicht über den passenden Schlüssel verfügen.

Dabei ergibt sich natürlich ein Problem: Um die Nachricht entschlüsseln zu können, muss die empfangende Stelle im Besitz des passenden Schlüssels sein. Bei

den klassischen, sog. symmetrischen Verschlüsselungsverfahren ist dies derselbe Schlüssel, wie er für die Verschlüsselung genutzt wurde. Um also die Vertraulichkeit des Inhalts der Nachricht zu schützen, muss der Schlüssel ebenso wie die Nachricht unter Erhalt der Vertraulichkeit an die Empfängerin oder den Empfänger übermittelt werden. Das ursprüngliche Problem der Gewährleistung der Vertraulichkeit wird bei diesen Verfahren also nur von der Vertraulichkeit der Übertragung der Nachricht auf die Vertraulichkeit der Übertragung des Schlüssels verschoben.

Glücklicherweise gibt es heute technische Verfahren, die dieses Problem lösen. Nutzt man sog. asymmetrische Verschlüsselungsverfahren, gibt es an Stelle des einen Schlüssels zwei Schlüssel. Einer dieser Schlüssel ist ein Verschlüsselungs-Schlüssel, der andere ist ein Entschlüsselungs-Schlüssel. Da Nachrichten mit dem Verschlüsselungs-Schlüssel nur verschlüsselt und nicht entschlüsselt werden können, ist es kein Problem, diesen Schlüssel anderen Personen mitzuteilen. Die Vertraulichkeit des Verschlüsselungs-Schlüssels ist keine Voraussetzung für die Vertraulichkeit der damit verschlüsselten Nachricht. Weil der Verschlüsselungs-Schlüssel öffentlich bekannt sein kann, nennt man ihn auch den öffentlichen Schlüssel. Der Entschlüsselungs-Schlüssel muss aber zwingend geheim gehalten werden, da die übertragenen Nachrichten mit ihm entschlüsselt werden können. Deshalb nennt man den Entschlüsselungs-Schlüssel auch privaten Schlüssel. Um eine Nachricht verschlüsselt zu übertragen, muss die absendende Stelle nur den Verschlüsselungs-Schlüssel der Empfängerin oder des Empfängers bekommen, verschlüsselt damit die Nachricht und überträgt die so verschlüsselte Nachricht. Die Empfängerin oder der Empfänger entschlüsselt die so empfangene Nachricht mit Hilfe ihres oder seines eigenen Entschlüsselungs-Schlüssels.

Wenn eine Nachricht mit einem falschen Verschlüsselungs-Schlüssel verschlüsselt wurde, kann die Empfängerin oder der Empfänger die Nachricht nicht entschlüsseln, weil sie oder er nicht den passenden Entschlüsselungs-Schlüssel hat. Wurde der absendenden Stelle absichtlich ein Verschlüsselungs-Schlüssel von jemandem untergeschoben, der den passenden Entschlüsselungs-Schlüssel besitzt, kann dieser dann die Nachricht entschlüsseln, die nicht für ihn bestimmt war. Es muss also einen Weg geben, wie die absendende Stelle sicherstellen kann, den richtigen Schlüssel zu verwenden. Ein geeigneter Weg, um das Problem zu

lösen, ist eine zentrale Stelle, der die Senderin oder der Sender vertraut und die mit einem Zertifikat bestätigt, dass ein Schlüssel zu einer Empfängerin oder einem Empfänger gehört. Ein solches digitales Schlüsselbrett nennt man „Public Key Infrastructure" oder kurz PKI. Eine absendende Stelle besorgt sich in diesem Verfahren aus irgendeiner Quelle – z.B. aus einer ungeschützt zugesandten E-Mail-Nachricht, aus einem Verzeichnisdienst, von der Webseite des Empfängers – den Verschlüsselungs-Schlüssel samt Zertifikat und prüft dieses. Fällt das Prüfungsergebnis positiv aus, dann weiß die Stelle, dass ihr der richtige Schlüssel vorliegt.

Zusätzlich zum Schutz der Vertraulichkeit einer Nachricht können die Schlüssel und die für sie ausgestellten Zertifikate eingesetzt werden, um Nachrichten durch digitale Signaturen zuverlässig ihren Autorinnen und Autoren zuordnen und ihre Unversehrtheit bestätigen zu können. Der konsequente Einsatz von digitalen Signaturen trägt im Übrigen dazu bei, gefälschte Dokumente als solche zu erkennen und zurückweisen zu können, ohne dass sie zur Ansicht geöffnet werden müssen, sodass eine in ihnen möglicherweise enthaltene Schadsoftware nicht ausgeführt wird.

Zur Erstellung einer digitalen Signatur wird eine Prüfsumme[36] des zu signierenden Dokuments erstellt und diese dann mit einem zu dem Zertifikat passenden, geheimen Schlüssel verschlüsselt. Der zum Zertifikat gehörende öffentliche Schlüssel kann dann von der empfangenden Stelle genutzt werden, um die Prüfsumme wieder zu entschlüsseln. Sofern die Prüfsumme des Dokuments mit der entschlüsselten Prüfsumme identisch ist, kann sich die empfangende Stelle darauf verlassen, dass das Dokument von der angegebenen absendenden Stelle stammt und durch keine dritte Partei verändert wurde. So kann durch den Einsatz von Zertifikaten und der zugehörigen PKI nicht nur die Vertraulichkeit, sondern auch die Authentizität und Integrität einer Nachricht geschützt werden. Beide Verfahren können je nach Anforderung kombiniert, aber auch jedes für sich eingesetzt werden.

36 Das ist eine kurze Zeichenkette, die eindeutig aus dem Dokument mit einem standardisierten Verfahren gebildet wird.

In Berlin betreibt das IT-Dienstleistungszentrum (ITDZ) eine solche PKI für die Berliner Verwaltung. Derzeit wird diese Dienstleistung leider nur von wenigen Behörden genutzt. Außerdem folgen die vom ITDZ ausgestellten Zertifikate technisch veralteten Standards, die nicht geeignet sind, die Vertraulichkeit der Kommunikation zu gewährleisten. Wir haben daher das ITDZ darauf hingewiesen, dass die Landes-PKI – das vom ITDZ betriebene digitale Schlüsselbrett – an die aktuell vom Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegten technischen Anforderungen anzupassen ist.

Mit der modernisierten PKI müssen dann alle Behörden konsequent und flächendeckend mit Schlüsseln ausgestattet werden, sodass die Vertraulichkeit und die Integrität der digitalen Kommunikation der Behörden gewährleistet werden kann. Dies gilt besonders für die Kommunikation der Behörden untereinander. Doch muss auch den Unternehmen sowie den Bürgerinnen und Bürgern eine Möglichkeit eröffnet werden, mit den verschiedenen Behörden unter Wahrung von Vertraulichkeit und Integrität in einfacher Weise digital zu kommunizieren.

Die Behörden und die Bürgerinnen und Bürger brauchen eine Möglichkeit, unter Wahrung von Vertraulichkeit und Integrität miteinander digital zu kommunizieren. Verschlüsselung und digitale Signatur bieten diese Möglichkeit, benötigen jedoch zertifizierte Schlüssel. Die PKI des ITDZ als digitales Schlüsselbrett für die Verwaltung muss für deren Bereitstellung modernisiert und die Behörden müssen flächendeckend mit Schlüsseln ausgestattet werden.

2.3 Datenschutzkonformer Einsatz von Windows 10

Der Umstieg der Verwaltung auf die aktuelle Version von Windows 10 ist aus Gründen der IT-Sicherheit unerlässlich, soweit sie nicht auf Alternativen[37] ausweichen kann oder will. Für einen datenschutzgerechten Einsatz von Windows 10 sind jedoch einige Hürden zu überwinden. Wir haben uns an der Erarbeitung eines Prüfkatalogs beteiligt, mit der die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) den Verantwortlichen eine Hilfestellung für die Entscheidung über den Einsatz von Windows 10 gibt.

Über die in Windows 10 integrierten Telemetrie-Funktionen wurde bereits vielfach berichtet. Telemetrie bedeutet „Fernmessung" und bei Windows 10 bedeutet es, dass Hintergrunddienste, d.h. bestimmte Programme, die für die Nutzerinnen und Nutzer unsichtbar arbeiten, Daten sammeln und zur Analyse regelmäßig an Server von Microsoft übermitteln. Besonders problematisch ist, dass Microsoft selbst festlegt, um welche Daten es sich dabei handelt: Die Definition von Art und Umfang der zu übermittelnden Daten wird von Microsoft ständig angepasst, was eine datenschutzrechtliche Bewertung der Übertragung erschwert. Hinzu kommt, dass Microsoft im Rahmen der Steuerung der Telemetrie-Funktion von Windows 10 auch beliebige Programme auf den Computern der Nutzerinnen und Nutzer ausführen kann. So ist es u. a. möglich, Inhalte aus dem Speicher des Computers an Microsoft zu übertragen. Microsoft begründet die Sammlung und Übertragung dieser Telemetrie-Daten damit, Fehlerbeseitigungen und Produktverbesserungen durchführen zu wollen.

Die Stellen, die Windows 10 einsetzen, können den Umfang der Übertragung von Telemetrie-Daten nur in von Microsoft festgelegten Stufen einstellen. Dabei steht die datensparsamste Variante „sicher" nur Nutzenden der „Enterprise"-Variante von Windows 10 zur Verfügung, welche an Privatpersonen nicht verkauft wird. Un-

37 In einigen deutschen Städten wurde der Umstieg auf andere Betriebssystem-Software wie Linux getestet – und im Fall der Stadtverwaltung München auch vollzogen –, um die Abhängigkeit von einem Anbieter zu verringern. Die alternative Betriebssystem-Software hat den weiteren Vorteil, dass die Programmlogik offenliegt und von Dritten überprüft und prinzipiell auch weiterentwickelt werden kann.

abhängig von der eingestellten Telemetrie-Stufe legt aber letztlich allein Microsoft fest, welche Daten dadurch erfasst werden. Es gibt zwar verschiedene Anleitungen, den Umfang der übertragenen Daten zu reduzieren. Die dort vorgestellten Maßnahmen helfen jedoch nicht dauerhaft. Spätestens mit dem nächsten Update müssen die Einstellungen überprüft und ggf. erneut angepasst werden.

Die DSK hat daher im Herbst 2019 ein Prüfschema zum Datenschutz bei Windows 10 als Anwendungshinweis herausgegeben. Mit Hilfe dieses Prüfschemas können Verantwortliche sicherstellen und dokumentieren, dass die datenschutzrechtlichen Anforderungen beim Einsatz von Windows 10 jederzeit eingehalten werden. Um dies zu gewährleisten, müssen je nach Art der verarbeiteten Daten gegebenenfalls zusätzliche technische Maßnahmen zur Verhinderung einer unbefugten Übermittlung zum Einsatz kommen.

Solche Maßnahmen müssen auch von den Berliner Behörden ergriffen werden, die das bisher eingesetzte Windows 7 durch Windows 10 ersetzen. Da Microsoft den regulären Support für Windows 7 am 14. Januar 2020 beendet, kann Windows 7 ab diesem Zeitpunkt nur noch datenschutzkonform eingesetzt werden, wenn kostenpflichtig erworbene zusätzliche Supportdienstleistungen in Anspruch genommen werden. Das ITDZ hat ein Konzept für den sog. Berlin-PC als Bestandteil des IKT-Arbeitsplatzes, der zukünftig nahezu flächendeckend in der Verwaltung zum Einsatz kommen soll, erarbeitet, welches auch den Sicherheits- und Datenschutzansprüchen genügen soll.

Wir haben dieses Konzept mit dem ITDZ erörtert und bewerten es als grundsätzlich geeignet, Windows 10 in der Verwaltung datenschutzkonform einzusetzen. Das ITDZ erreicht dies, indem die von den Verwaltungen benötigten Fachanwendungen ohne Internetzugang betrieben werden und es auf dem jeweiligen Arbeitsplatzcomputer zusätzlich eine getrennte Umgebung für die Internetnutzung gibt. Sofern das Konzept konsequent umgesetzt wird, kann so den Anforderungen der DSK entsprochen werden. Wir werden das Projekt weiter begleiten und überprüfen, ob das Konzept in der Verwaltung datenschutzkonform umgesetzt wird.

Da bei Weitem noch nicht alle Berliner Behörden den Berlin-PC einsetzen und der Einsatz von Windows 10 auch im nicht-öffentlichen Bereich alltäglich ist, wird das Thema Telemetrie-Daten uns voraussichtlich noch einige Zeit beschäftigen.

Der Einsatz von Windows 10 ist datenschutzrechtlich unzulässig, solange nicht mit technischen und organisatorischen Maßnahmen vermieden wird, dass personenbezogene Daten aus der Nutzung der Software oder gar aus den Inhalten von Dokumenten Microsoft zur Verwendung für dessen Zwecke übermittelt werden. Ein Prüfschema der deutschen Aufsichtsbehörden hilft den Verantwortlichen, einen datenschutzkonformen Einsatz sicherzustellen.

2.4 Schadsoftware-Befall am Kammergericht

Ein Schadsoftware-Befall am Kammergericht hat gravierende Schwächen beim Schutz der durch dieses Gericht verarbeiteten sensitiven Daten aufgezeigt. Wir haben uns die Sicherheitsmaßnahmen erläutern lassen, die einerseits vorbeugend und andererseits nach der Infektion zur Bewältigung der Probleme ergriffen wurden und haben Empfehlungen zur weiteren Problembehandlung erteilt. Entsprechende Gespräche führten wir auch in zwei Hochschulen, die in ähnlicher Weise betroffen waren.

Im September wurde das Kammergericht durch das ITDZ darüber informiert, dass ein Computer aus dem Netzwerk des Kammergerichts versuchen würde, einen Server zu erreichen, der von Kriminellen dafür genutzt werde, Befehle und Software an eine auf dem Computer laufende Schadsoftware zu übermitteln. Eine daraufhin durchgeführte Untersuchung deckte bei einer Reihe von Computern eine Infektion mit der Schadsoftware Emotet auf. Die lokal auf den Computern installierten Virenscanner hatten die Infektion nicht bemerkt.

Emotet wurde ursprünglich als Banking-Trojaner entwickelt. Er wird derzeit in Kombination mit anderen Schadsoftware-Komponenten dazu eingesetzt, Unternehmen und Behörden zu schaden und von ihnen Gelder zu erpressen. Dies geschieht oft durch die gründliche Verschlüsselung aller Daten, derer die Schadsoftware habhaft werden kann. Die Betroffenen sollen dann ein „Lösegeld" bezahlen, bevor sie – bestenfalls – einen Schlüssel erhalten, mit dem sie die Daten wieder entschlüsseln können. Darauf verlassen können sie sich nicht. Die erste Infektion durch eine derartige Software erfolgt oft durch eine manipulierte Datei, die einzelnen Personen per E-Mail zugesandt wird. Um diese Datei und die sie begleitende E-Mail möglichst glaubhaft erscheinen zu lassen, benutzt die Software Vorlagen,

die sie einem Kommunikationspartner des vorgesehenen Opfers bei einem vorherigen Befall stiehlt. Daher ist bei einer Infektion mit Emotet nicht nur mit einem Verlust des Zugangs zu bestimmten Daten, sondern auch mit deren Weitergabe an unbefugte Dritte zu rechnen.

Aufgrund der Information durch das ITDZ wurde zunächst der Internetzugang des Kammergerichts deaktiviert, wenig später das Kammergericht auch vom Berliner Landesnetz getrennt und nahezu die gesamte Informationstechnik des Gerichts stillgelegt. Diese Maßnahmen wurden ergriffen, bevor die Schadsoftware Daten verschlüsseln konnte. Unklar ist allerdings, auf welchem Weg die Erstinfektion stattgefunden hat und welche Schritte die Schadsoftware in der Folge unternommen hat. Daher steht auch nicht fest, welche und wie viele Daten abgeflossen sind. Aus den o. g. Gründen ist jedoch davon auszugehen, dass Emotet von den infizierten Computern zumindest E-Mail-Nachrichten ausgeleitet hat.

Da das Kammergericht nicht über ein System verfügt, mit dem es zuverlässig die Schadsoftware-Freiheit der alten Systeme und der mit ihnen gespeicherten Daten feststellen kann, entschied es sich, sein gesamtes Netzwerk neu aufzubauen. In diesem Zusammenhang werden die meisten vom Kammergericht benötigten Dienste zum ITDZ verlegt. Die ursprünglich im alten System abgelegten Unterlagen bleiben isoliert und stehen lediglich als Archiv zur Einsichtnahme zur Verfügung. Dieses konsequente Vorgehen steht im positiven Gegensatz zu den deutlich eingeschränkteren Maßnahmen, welche die ebenfalls von dem Virus befallenen Hochschulen ergriffen haben. Diese überprüften einige, aber keineswegs alle Speicherorte, in welche die Schadsoftware sich hätte einnisten können, und sahen keinen Anlass, strukturelle Änderungen vorzunehmen.

Der Neuaufbau der Informationstechnik des Kammergerichts wird diesem die Möglichkeit eröffnen, auch die Struktur der Netze und Anwendungen besser aufzustellen, als es bislang der Fall war. So sollte das neue System über eine scharfe Trennung zwischen den intern für die unterschiedlichen Fachverfahren genutzten Komponenten und den externen Komponenten für Internetnutzung und E-Mail-Kommunikation verfügen. Nur durch eine Abschottung der mit dem Internet verbundenen Komponenten und eine Aufteilung des Netzes in separate, voneinander getrennte Bereiche ist es möglich, eine Infektion daran zu hindern, sich auf die gesamte Informationstechnik auszubreiten.

Ein weiterer wesentlicher Schritt besteht in der Ausstattung der Richterinnen und Richter des Gerichts mit mobilen Dienstgeräten, die ihnen eine Arbeit auch in ihrer häuslichen Umgebung erlauben. Bisher fand diese Heimarbeit – auf gesetzlicher Grundlage – mit Privatgeräten statt. In der Folge wurden Daten zwischen diesen Privatgeräten und der dienstlichen Informationstechnik unkontrolliert ausgetauscht, vornehmlich über USB-Sticks oder durch den Versand per E-Mail. Die erste Form des Datenaustauschs hat das Gericht unmittelbar nach dem Vorfall zu Recht gesperrt. Doch auch die zweite, weiterhin gestattete Form bietet Schadsoftware einen Weg in das innere Netz des Gerichts.

Der nachvollziehbare Wunsch nach Heimarbeit kann jedoch auch ohne eine Gefährdung der Datensicherheit in einer Weise erfüllt werden, dass dienstliche Daten den besonders geschützten, internen Bereich nicht verlassen. Dazu müssen die für die Heimarbeit vorgesehenen Laptops so konfiguriert werden, dass sie sich ausschließlich mit dem internen Netzwerk des Gerichts verbinden können und die genutzten Büroprogramme alle bearbeiteten Dokumente ausschließlich auf Servern des Gerichts speichern. Die Konfiguration der Laptops muss sicherstellen, dass die eingesetzten Sicherheitsmaßnahmen nicht umgangen werden können.

Aus dem Vorfall sind Lehren nicht nur für das Kammergericht, sondern für alle Behörden und öffentlichen Stellen des Landes Berlin zu ziehen. Diese unterscheiden sich in Maßnahmen zur Vermeidung einer Infektion und solchen, die zu ergreifen sind, wenn ein Schadsoftware-Befall eintritt.

Für die Landesbehörden wird die im Zuge der Umsetzung des E-Government-Gesetzes Berlin (EGovG Bln) erfolgende Zentralisierung der Datenverarbeitung dazu beitragen, dass Software in Zukunft in einer Umgebung ausgeführt wird, in der die Sicherheit mit gebündelter Kompetenz gewährleistet werden kann. Die Hochschulen, die ihre Informationstechnik auch weiterhin selbst betreiben werden, sollten ihre Rechenzentren zu solchen Umgebungen ausbauen und nicht nur die Verwaltung, sondern auch die Verarbeitung aller sensitiven personenbezogenen Daten für Forschungszwecke in diese gesicherten Umgebungen verlagern, soweit dies möglich ist, ohne die Freiheit der Forschung einzuschränken.

Alle öffentlichen Stellen werden zusätzliche Beratung insbesondere zur sicheren Administrationspraxis, zur Gestaltung von Netzwerken und zur Risikoanalyse be-

nötigen. Es bedarf eines zentral bereitgestellten Dienstes, der über die Fähigkeiten üblicher Anti-Viren-Software hinaus potenzielle Risiken in Dateien erkennen kann, welche die Behörden aus fremden Quellen insbesondere über E-Mail erreichen. Und für den Fall, dass dennoch eine Infektion mit Schadsoftware eintritt, benötigen die öffentlichen Stellen einen Handlungsleitfaden und ein Computer-Notfall-Team, das ihnen schnell zur Seite steht.

Zu beenden ist zudem die Vermischung der Verarbeitung von privaten und dienstlichen Daten, sowohl im dienstlichen Umfeld als auch bei der Heimarbeit. Wer im Heimbüro arbeitet, benötigt ein dienstlich gestelltes Gerät. Wir empfehlen dem Gesetzgeber, die Regelung des § 23 des Gesetzes zur Ausführung des Gerichtsverfassungsgesetzes (AGGVG) aufzuheben, die Richterinnen und Richtern sowie Staats- und Amtsanwältinnen und -anwälten den Einsatz privater informationstechnischer Geräte erlaubt.

Die Sicherheit der eingesetzten Systeme ist Voraussetzung datenschutzkonformer Behördentätigkeit. Daher ist es zwingend notwendig, die Architektur der eingesetzten Informationstechnik im Hinblick auf den Schutz gegen Schadsoftware auszugestalten. Privates und Dienstliches ist strikt zu trennen. Mit entschiedenem, proaktivem Handeln muss weiteren Infektionen mit Schadsoftware entgegengetreten und dennoch eingetretene Infektionen müssen entschlossen, kompetent und schnell eingedämmt und beseitigt werden.

2.5 Zusammenarbeit mit behördlichen Datenschutzbeauftragten der Gerichte und Staatsanwaltschaften

Seit fast zehn Jahren führen wir regelmäßig Arbeitstreffen mit den behördlichen Datenschutzbeauftragten aller Berliner Gerichte und Staatsanwaltschaften durch. Hierbei diskutieren wir aktuelle datenschutzrechtliche Probleme und Fragestellungen aus der praktischen Tätigkeit der Datenschutzbeauftragten.

Es gab bereits früher regelmäßige Treffen zwischen unserer Behörde und den behördlichen Datenschutzbeauftragten der Amtsgerichte. Diese Tradition setzen wir

seit 2011 in einem größeren Rahmen fort. Anlass hierfür war damals ein von uns durchgeführtes Seminar zum Thema „Datenschutz in der Justiz“ in der Justizakademie in Königs Wusterhausen[38]. Bei dieser Veranstaltung wurde von vielen Teilnehmenden der Wunsch nach einem regelmäßigen Zusammentreffen zur Erörterung datenschutzrechtlicher Fragen sowie zum Erfahrungsaustausch geäußert.

Die behördlichen Datenschutzbeauftragten der Gerichte und Staatsanwaltschaften haben überwiegend eine juristische Ausbildung und führen in diesen Runden gemeinsam mit uns sehr qualifizierte und engagierte Diskussionen zu anstehenden datenschutzrechtlichen Belangen.

Immer wiederkehrende Themen sind solche zur Umsetzung datenschutzrechtlich erforderlicher technisch-organisatorischer Maßnahmen in den Gerichten und zur Zulässigkeit der Verwendung von Gerichts- und Verwaltungsakten zu verfahrensübergreifenden Zwecken. Von den Kolleginnen und Kollegen in den Häusern werden zudem regelmäßig Fragen zum Beschäftigtendatenschutz an die internen Datenschutzbeauftragten herangetragen, die wir bei unseren Arbeitstreffen gemeinsam besprechen. Zudem werden häufig die Rolle, die Aufgaben und die Rechte der behördlichen Datenschutzbeauftragten thematisiert.

Die Arbeit der behördlichen Datenschutzbeauftragten ist insbesondere deshalb so wichtig, weil diese die Datenverarbeitungsprozesse und deren Schwachstellen vor Ort sehr gut kennen. Von diesem Wissen können wir durch Zusammenarbeit und Austausch profitieren, und so wiederum den internen Datenschutzbeauftragten bei der Erfüllung ihrer Aufgaben helfen.

38 Zentrale Fortbildungsstätte für die Justiz des Landes Brandenburg und für den höheren Dienst des Landes Berlin

3 Inneres und Sport

3.1 Drohbriefe an die linke Szene mit Daten aus Polizeidatenbanken

Die Drohbriefe an die linke Szene beschäftigten uns auch im Jahr 2019. Bei verschiedenen als politisch links einzustufenden Einrichtungen waren im Dezember 2017 Briefe mit personenbezogenen Daten (u. a. Namen und Fotos) und einem für die Betroffenen bedrohlichen Text eingegangen. Die verwendeten Fotos und Informationen ließen den Schluss zu, dass sie aus polizeilichen Datenbanken stammten. Daher haben wir unmittelbar nach Bekanntwerden dieses Falls umfangreiche Prüfungen durchgeführt und eine langwierige Korrespondenz mit der Polizei sowie der Staatsanwaltschaft Berlin geführt.[39]

Nachdem wir im Oktober 2018 die Mitteilung erhalten hatten, dass ein Polizeibeamter des Landes Berlin als Verfasser der Drohbriefe ermittelt und gegen ihn bereits ein Strafbefehl erlassen worden war, haben wir uns erneut an die Polizei gewandt. Eine weitere Prüfung war notwendig, da uns keine Informationen dazu vorlagen, woher die in den versendeten Briefen enthaltenen personenbezogenen Daten konkret stammten, wie der Verfasser an diese Daten gelangen konnte und ob er sie sich allein beschafft hatte oder ob es in den Reihen der Polizei Mittäterinnen oder Mittäter gab. Eine zentrale Frage war dabei, inwiefern der Täter über die technische Berechtigung verfügte, auf die Daten der betroffenen Personen zuzugreifen und (Bild-)Dateien aus den Polizeidatenbanken herunterzuladen und extern zu speichern. Im Gegensatz zur strafrechtlichen Sanktionierung des konkreten Vorfalls durch die Justiz ging es uns darum, mögliche Schwachstellen bei den technischen und organisatorischen Maßnahmen zur Nutzung der Datenbanksysteme der Polizei festzustellen, um durch Empfehlung geeigneter Gegenmaßnahmen solche Vorfälle in der Zukunft möglichst zu verhindern.

Zur Klärung der offenen Punkte haben wir zum einen mehrere schriftliche Stellungnahmen der Polizei eingeholt. Zum anderen haben wir Protokolldaten der

39 Siehe die ausführliche Darstellung im JB 2018, S. 55 ff.

polizeilichen Datenbank POLIKS in dem für die Tat relevanten Zeitraum ausgewertet, um die erfolgten Zugriffe auf die Daten der Betroffenen zu überprüfen.

Bedauerlicherweise konnte nicht eindeutig aufgeklärt werden, wie der Verfasser der Drohbriefe an die personenbezogenen Daten der Betroffenen, insbesondere die Bilddateien, gelangt ist. Denkbar ist, dass er zu einem früheren Zeitpunkt die Berechtigungen besessen hat, POLIKS-Inhalte herunterzuladen und zu speichern. Nicht auszuschließen ist aber auch, dass ihm die Daten durch andere Berechtigte zur Verfügung gestellt wurden, auch wenn sich aus den uns vorliegenden Protokolldaten keine eindeutigen Hinweise auf konkrete Mittäterinnen oder Mittäter ergeben haben.

Zwar kann ein Missbrauch der polizeilichen Datenbanken durch einzelne Polizeimitarbeitende nicht gänzlich verhindert werden. Die Polizei ist allerdings dazu angehalten, geeignete technische-organisatorische Maßnahmen zu ergreifen, die den Schutz der personenbezogenen Daten in den Datenbanken bestmöglich gewährleisten.[40]

3.2 Kontrolle des polizeilichen Informationssystems POLIKS

Insbesondere die Schwierigkeiten bei der Ermittlung des Täters, der Drohbriefe an die linke Szene mit personenbezogenen Daten aus Polizeidatenbanken versandt hatte,[41] waren Anlass für uns, grundsätzlich die Datenverarbeitung im polizeilichen Informationssystem POLIKS im Rahmen einer Vor-Ort-Kontrolle zu überprüfen.

Schwerpunkte der Prüfung waren die Kontrolle der Einhaltung der für POLIKS geltenden Prüf- und Löschfristen und die Untersuchung der Möglichkeiten von Beschäftigten der Polizei, in POLIKS Einsicht zu nehmen.

40 Siehe hierzu 3.2
41 Siehe 3.1

Wir haben festgestellt, dass die Polizei seit Juni 2013 die automatisierte Löschung in POLIKS komplett ausgeschaltet hatte. Anlass hierfür war eine Weisung der Senatsverwaltung für Inneres und Sport, keine Akten und Dateien „mit Bezügen zum Rechtsextremismus" zu vernichten bzw. zu löschen, damit sichergestellt ist, dass der Untersuchungsausschuss des Deutschen Bundestages zum sog. „NSU" Einsicht in alle relevanten Daten und Unterlagen erhalten kann.[42] Diese Weisung wurde seitdem jährlich verlängert. Sie wurde zudem durch ein zweites Löschmoratorium aus Anlass des Anschlags auf dem Breitscheidplatz im Dezember 2016 ergänzt.[43] Die Polizei sollte sicherstellen, dass keine Akten oder Daten vernichtet bzw. gelöscht werden, „die mit dem Anschlag in Verbindung stehen oder stehen könnten", da mit der Einsetzung eines Untersuchungsausschusses gerechnet wurde. Zwischenzeitlich wurden entsprechende Untersuchungsausschüsse durch das Abgeordnetenhaus von Berlin und den Deutschen Bundestag eingesetzt. Auch das Breitscheidplatz-Löschmoratorium wurde seither jährlich verlängert. Eine Löschung von Daten bei der Polizei erfolgt seitdem lediglich manuell aufgrund konkreter Anfragen oder Löschersuchen zu bestimmten Vorgängen.

Die Nichtvornahme der Löschung personenbezogener Daten in POLIKS ist rechtswidrig, soweit eine Speicherung nicht zur Erfüllung der in der Zuständigkeit der Polizei liegenden Aufgaben bzw. für Zwecke der Untersuchungsausschüsse zum sog. „NSU" und zum Breitscheidplatzattentat erforderlich ist.[44]

Die löschreifen, jedoch aufgrund der Löschmoratorien fortdauernd gespeicherten Daten wurden mindestens bis zum Zeitpunkt unserer Prüfung auch nicht im Zugriff beschränkt. Erst im September 2019 begann die Polizei mit dem Verschieben dieser Daten in einen dafür eingerichteten Schutzbereich.

Auch diese fehlende Zugriffsbeschränkung war rechtswidrig. Soweit die Daten aufgrund der Löschmoratorien weiterhin gespeichert werden durften, hätten sie dem allgemeinen Zugriff über POLIKS entzogen werden müssen.[45] Nur so wird gewährleistet, dass die zur Benutzung von POLIKS Berechtigten ausschließlich zu

42 Sog. NSU-Löschmoratorium

43 Sog. Breitscheidplatz-Löschmoratorium

44 Siehe §§ 48 Abs. 2 Satz 1 Nr. 1; 42 Abs. 1 Satz 1 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG)

45 Siehe § 32 Abs. 1 Nr. 5, § 50 Abs. 3 Satz 1 Nr. 5 Berliner Datenschutzgesetz (BlnDSG)

den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.[46]

Weiterhin stellten wir bei unserer Prüfung fest, dass die Polizei im Rahmen der Zugriffskontrolle bei POLIKS auch keine geeigneten Stichprobenverfahren durchführt. Die derzeit von der Polizei durchgeführten Kontrollen werden inhaltlich nicht von einer organisatorisch sowie thematisch getrennten und somit unabhängigen Stelle durchgeführt, was deren Ergebnisse in ihrer Aussagekraft schwächt.

Zudem sind die Kontrollen offensichtlich nicht effektiv, weil bisher in keinem einzigen Fall Unregelmäßigkeiten oder unberechtigte Zugriffe festgestellt worden sind, obwohl unserer Behörde regelmäßig unberechtigte Abrufe in POLIKS durch Polizeimitarbeitende gemeldet und durch uns auch geahndet werden. Deshalb und aufgrund der Vielzahl der Abrufe, die täglich in POLIKS erfolgen, ist eine hohe Dunkelziffer zu befürchten.

Besonders problematisch war zudem der Befund, dass die Systemeinstellung von POLIKS Datenabrufe ohne die Angabe konkreter Gründe ermöglicht. Bei der innerhalb der Datenbank möglichen Personensuche können zum Teil sehr allgemeine Abfragegründe wie etwa „Vorgangsbearbeitung“ oder „sonstiger Grund“ ausgewählt werden. Für die notwendige Ergänzung des ausgewählten Abfragegrunds genügt es sogar, in einem Freitextfeld drei beliebige Zeichen wie z.B. „xxx“ einzugeben. Eine Rückverfolgung und Prüfung der Rechtmäßigkeit von Abfragen wird damit unmöglich. Allgemeine Schlagwörter enthalten für sich genommen keine Aussage über den konkreten Grund der Abfrage und sind somit nicht revisionssicher. Nur formal ausfüllbare Freitextfelder stellen eine nachträgliche Überprüfbarkeit nicht sicher.

Das derzeitige System der Personensuche ist rechtswidrig.[47] Das Gesetz schreibt vor, dass Abfragen aus POLIKS auch hinsichtlich ihrer Begründung protokolliert werden müssen. Gesetzgeberisches Ziel ist die Gewährleistung der nachträglichen Überprüfbarkeit der Berechtigung der Abfragen durch die Betroffenen, durch Verantwortliche im Rahmen einer internen Revision und durch die Berliner

46 Sog. Zugriffskontrolle

47 Siehe § 62 Abs. 1 Nr. 3, Abs. 2 BlnDSG

Beauftragte für Datenschutz und Informationsfreiheit. Die Protokollierung ist insoweit elementar für die Durchsetzung von Betroffenenrechten und nicht zuletzt für die Erfüllung der gesetzlichen Aufgabe auch unserer Behörde, die Anwendung datenschutzrechtlicher Vorschriften zu überwachen und durchzusetzen.[48]

Wir haben die festgestellten Verstöße gegenüber der Polizei beanstandet und gesetzeskonforme Anpassungen gefordert.

POLIKS ist eine der wichtigsten elektronischen Arbeitshilfen der Polizei und enthält dementsprechend viele, zum Teil sehr sensitive personenbezogene Daten. Daher ist es ausgesprochen wichtig, dass die Polizei die Zulässigkeit der dort vorgenommenen Datenspeicherungen sowie den Zugang zu diesem System engmaschig und effektiv kontrolliert sowie nachträgliche Überprüfungen ermöglicht.

3.3 Verzögerte Beantwortung von Auskunftsanfragen durch die Polizei

Uns erreichten vermehrt Beschwerden darüber, dass an die Polizei gerichtete Auskunftsanträge und Löschersuchen auch nach längerer Wartezeit noch nicht beantwortet worden seien.

Wir haben die Polizei um Stellungnahme hierzu gebeten und darauf hingewiesen, dass die Beantwortung vorgenannter Anträge regelmäßig ohne Verzögerung erfolgen sollte. Die Polizei muss die hierfür erforderlichen organisatorischen Maßnahmen treffen. Es wurde uns daraufhin mitgeteilt, dass die durchschnittliche Bearbeitungszeit von Anträgen bei der Polizei derzeit aufgrund der enorm gestiegenen Antragszahl etwa sieben Monate dauere. Mit der Bearbeitung seien regelmäßig drei Personen und zwei Zuarbeitende beschäftigt.

Auch unsere eigenen Schreiben an die Polizeibehörde werden oft nur verzögert beantwortet. Es sind regelmäßig Mahnungen erforderlich, die eine unnötige

48 Siehe § 11 Abs. 1 Satz 1 Nr. 1 BlnDSG

Mehrarbeit für uns bedeuteten. Dies hat auch zur Folge, dass sich die Bearbeitung von Beschwerden bei uns verzögern.

In einem Gespräch mit der Polizeipräsidentin wiesen wir nochmals auf die Problematik hin. Sie begründete die lange Bearbeitungsdauer mit personellen Engpässen. Sie werde jedoch prüfen lassen, ob weitere Mitarbeitende für die Erfüllung dieser Aufgaben eingesetzt werden könnten. Wir empfahlen eine zumindest vorübergehende personelle Verstärkung des Bereichs zur Abarbeitung der bisherigen Anträge.

Die Rechte auf Auskunft über die Speicherung personenbezogener Daten und die Löschung derartiger Daten sind Bestandteile der Betroffenenrechte, die ein Kernbestandteil des informationellen Selbstbestimmungsrechts sind. Zur Gewährleistung dieser Rechte muss die Verfahrensprozedur effizient gestaltet und ggf. auch mehr Personal zur Bearbeitung von Anträgen freigestellt werden.

3.4 Bußgeldverfahren: Aktenzeichen sichtbar im Adressfeld

Die Polizeibehörde führte bei allen automatisiert erstellten Schreiben der Bußgeldstelle neben der Anschrift auch das Aktenzeichen des jeweiligen Bußgeldverfahrens im sichtbaren Adressfeld der Briefe an die Betroffenen auf. Hierüber beschwerte sich ein Betroffener bei uns. Wir haben die Beschwerde zum Anlass genommen, diese Adressierungspraxis der Polizei zu prüfen.

Die Polizei teilte uns im Rahmen der Prüfung mit, dass die Wiedergabe des Aktenzeichens im Adressfenster notwendig sei, um bei der amtlichen Zustellung von Schreiben das ordnungsgemäße Ausfüllen einer Postzustellungsurkunde zu ermöglichen. Erst durch die Übereinstimmung des Aktenzeichens auf dem Briefumschlag mit dem auf der Postzustellungsurkunde hinterlegten Aktenzeichen werde es ermöglicht, nachzuweisen, dass das konkrete Schriftstück auch zugestellt wurde. Dieser Bewertung stimmen wir zu.

Regelmäßig werden jedoch nur bestimmte Schreiben, insbesondere der Bußgeldbescheid im Rahmen von Bußgeldverfahren, mittels einer Postzustellungsurkunde amtlich zugestellt. Bei allen anderen automatisiert erstellten Schreiben wie z.B. Anhörungen, Verwarnungen und Mahnungen erfolgt die Bekanntgabe lediglich durch Einwurf in den Briefkasten. Auch in diesen Fällen glaubte man sich bei der Polizei zum Abdruck des Aktenzeichens im Adressfeld befugt, weil man dadurch ein Sortierkriterium bei unzustellbar rücklaufender Post habe. Hinzu komme, dass aus der Angabe des Aktenzeichens kein Erkenntnisgewinn bezüglich einer konkreten Tat möglich sei und man auch auf anderem Wege (online, telefonisch oder vor Ort) keine Auskünfte allein durch Kenntnis des jeweiligen Aktenzeichens erhalte.

Für die Frage der Zulässigkeit einer Datenverarbeitung ist jedoch nicht entscheidend, ob Dritte hierdurch weitere Informationen erhalten können. Vielmehr ist ausschlaggebend, ob der Abdruck eines Aktenzeichens im Adressfeld von Briefen für die Polizei erforderlich ist. Bei dem Aktenzeichen eines Bußgeldverfahrens handelt es sich gerade in Verbindung mit einer Anschrift um ein personenbezogenes Datum, dessen Angabe im Adressfeld eines Briefes für die normale Übersendung eines Schreibens auf dem Postweg nicht notwendig ist. Postrückläufe können auch ohne dieses Sortierkriterium bearbeitet werden, da die Identifikation der Betroffenen über die Adressdaten erfolgt und in Zweifelsfällen der betreffende Briefumschlag auch geöffnet werden kann.

Wir haben die Polizei daher aufgefordert, die bestehende Praxis abzustellen und die Vordrucke anzupassen. Die Polizei sagte daraufhin eine Änderung ihrer Adressierungspraxis zu.

Nur bei Bußgeldbescheiden, die amtlich zugestellt werden, darf das Aktenzeichen im Adressfeld von Briefen sichtbar sein.

3.5 Datenverarbeitung im Melderegister: Personenverwechslungen & mehr

Aus der Praxis

Meldebehörden[49] sind gesetzlich verpflichtet, die in ihrem Zuständigkeitsbereich wohnenden Personen zu registrieren, um deren Identität und Wohnungen feststellen und nachweisen zu können. Hierzu führen sie ein Melderegister, in das bestimmte Daten eingetragen werden, die bei der betroffenen Person erhoben, von öffentlichen Stellen übermittelt oder in sonstiger Weise amtlich bekannt werden. § 3 Bundesmeldegesetz (BMG) legt dabei fest, welche personenbezogenen Daten im Melderegister gespeichert werden dürfen. Weitere Daten bzw. Hinweise dürfen nur unter bestimmten Voraussetzungen gespeichert werden. Die Meldebehörden sind auch dazu befugt, Melderegisterauskünfte zu erteilen, bei der Durchführung von Aufgaben anderer Behörden oder sonstiger öffentlicher Stellen mitzuwirken und Daten zu übermitteln. Personenbezogene Daten dürfen dabei jedoch nur dann verarbeitet werden, wenn dies gesetzlich geregelt ist.[50]

Uns erreichten im Jahr 2019 zahlreiche Anfragen und Beschwerden über die Datenverarbeitung der Meldebehörden. Im Rahmen der Prüfung der Beschwerden ist sichtbar geworden, wie wichtig ein sorgfältiger Umgang im Zusammenhang mit der Speicherung und dem Abruf der im Melderegister enthaltenen Daten ist. Welche Auswirkungen es haben kann, wenn hierbei Fehler passieren, soll nachfolgend anhand einiger ausgewählter Fälle dargestellt werden.

Ein Betroffener schilderte uns, dass er von verschiedenen behördlichen Stellen Schreiben erhalten hat, in denen er als Halter eines Kraftfahrzeugs angeschrieben wurde. Darunter waren ein Bescheid der Berliner Kraftfahrzeugzulassungsbehörde, ein Schreiben zu einer Pfändungs- und Einziehungsverfügung des Hauptzollamts Berlin sowie eine Mahnung hinsichtlich der Fälligkeit einer Kfz-Steuer des Hauptzollamts Frankfurt/Oder. Der Betroffene erklärte uns in nachvollziehbarer Weise, dass er nicht der richtige Adressat dieser Schreiben sein könne, da er weder einen Führerschein noch ein Kraftfahrzeug besitze. Bei un-

49 Dies sind in Berlin die Bezirksämter und das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) – siehe § 1 Abs. 1 BlnAGBMG

50 Siehe zu den vorgenannten Aufgaben und Befugnissen die Regelungen in § 2 BMG

seren Nachforschungen stellte sich heraus, dass die Schreiben aufgrund einer Personenverwechslung an den Beschwerdeführer versandt worden waren und eigentlich eine Person betrafen, die sowohl den gleichen Vor- und Nachnamen hat, als auch am gleichen Tag und in der gleichen Stadt geboren wurde. Einzig in den beiden weiteren Vornamen des Beschwerdeführers unterschieden sich seine Daten von dem tatsächlichen Halter des Kraftfahrzeugs. Eine Behörde hatte eine Melderegisterabfrage veranlasst, um die neue Anschrift der namensgleichen Person herauszufinden. Da bei einer solchen Melderegisterabfrage als Angaben zur Personenidentifizierung in der Regel nur ein Vorname sowie der Nachname und das Geburtsdatum eingegeben werden, erhielt die abfragende Stelle die Anschrift unseres Beschwerdeführers. Auf die beiden weiteren Vornamen, an denen die beiden Personen zu unterscheiden gewesen wären, wurde offenbar nicht geachtet.

In einem anderen Fall erhielt eine Person die Information über die Ausstellung eines Führungszeugnisses, obwohl sie keines beantragt hatte. Das zuständige Bezirksamt räumte ein, dass dies auf eine Personenverwechslung zurückzuführen war. Eine namensgleiche Person hatte in der Sprechstunde eines mobilen Bürgeramtes die Erstellung eines Führungszeugnisses beantragt. Aufgrund technischer Probleme sowie der zahlreichen wartenden Kundinnen und Kunden entschied sich der Sachbearbeiter, zunächst nur die Antragsdaten hierfür aufzunehmen, die Verwaltungsgebühren zu erheben und den Antrag im Nachhinein im stationären Bürgeramt zu bearbeiten. Allerdings vergaß er bei der Antragsannahme, das Geburtsdatum der antragstellenden Person aufzunehmen. Bei der späteren Bearbeitung des Antrags erfolgte die Suche nach der antragstellenden Person über die Suchmaske der Bearbeitungssoftware lediglich mit dem Vor- und Familiennamen. Dabei wurde übersehen, dass in Berlin zwei Personen mit diesem Namen gemeldet sind, die sich jedoch im Hinblick auf das Geburtsdatum unterscheiden. Für die Antragsbearbeitung wurden so versehentlich die falschen Daten aus dem Melderegister ausgewählt.

Schließlich wandten sich zwei Betroffene an uns, die mehrfach Schreiben von der Polizei erhalten hatten, mit denen sie als Vormund eines minderjährigen Geflüchteten angeschrieben wurden. Zwar hatten sie die Vormundschaft für einen geflüchteten Jugendlichen übernommen, allerdings nicht für den in den polizeilichen Schreiben angesprochenen Minderjährigen. Auf Nachfrage teilte die Polizei den Betroffenen mit, dass die Daten für die polizeilichen Vorladungsschreiben aus

dem Melderegister bezogen wurden. Es musste also davon ausgegangen werden, dass im Melderegister falsche Daten gespeichert waren. Gesetzlich ist festgelegt, dass in den Datensatz minderjähriger Kinder auch bestimmte personenbezogene Daten der gesetzlichen Vertreter einzutragen sind.[51] Informationen hierzu werden regelmäßig direkt bei den betroffenen Personen, z.B. durch Ausfüllen des Meldescheins, erhoben. Darüber hinaus können die Meldebehörden solche Informationen auch aufgrund von gesetzlich angeordneten Datenübermittlungen von anderen öffentlichen Stellen erhalten oder diese durch Ermittlungen von Amts wegen erheben. Im Rahmen unserer Prüfung fanden wir heraus, welches Bezirksamt die beiden Beschwerdeführer als Sorgeberechtigte im Datensatz des betreffenden minderjährigen Geflüchteten gespeichert hatte. Als Grundlage diente laut Eintrag im Melderegister der Beschluss eines Amtsgerichts, der jedoch nicht mehr aufzufinden war. Aufgrund fehlender Unterlagen ließ sich somit zwar nicht abschließend klären, was zu der Eintragung der falschen Vormundschaft geführt hatte. Da das Jugendamt dem Bezirksamt jedoch die tatsächlichen Sorgeberechtigten mitteilte, muss von einem Versehen des zuständigen Bezirksamtsmitarbeitenden bei der Melderegistereintragung ausgegangen werden.

Namensgleichheiten von Personen sind in der Praxis keine Seltenheit. Um Personenverwechslungen beim Abruf von Daten aus dem Melderegister zu vermeiden, muss die behördliche Stelle bei einer Personensuche ausreichende Angaben zur Identifizierung der betroffenen Person als Suchmerkmale eingeben. Eine zweifelsfreie Identifizierung ist regelmäßig möglich, wenn zumindest der Familienname, ggf. der Geburtsname, der Vorname bzw. die Vornamen, das Geburtsdatum und die letzte bekannte Anschrift vorliegen. Auch bei der Pflege der Melderegisterdaten muss die eintragende Stelle sorgfältig vorgehen, um sicherzustellen, dass nur zutreffende Daten zu den jeweiligen Personen gespeichert werden.

51 § 3 Abs. 1 Nr. 9 BMG

3.6 Auskunftssperre im Melderegister wegen Änderung des Vornamens oder der Geschlechterzugehörigkeit

Im Rahmen eines Beschwerdeverfahrens informierte uns ein Bürger über Schwierigkeiten im Zusammenhang mit der Einrichtung einer Auskunftssperre im Melderegister. Der Betroffene hatte während eines Termins im Bürgeramt einen Antrag auf Einrichtung einer Auskunftssperre wegen der Änderung des Vornamens gemäß § 1 Transsexuellengesetz (TSG) gestellt. Die Sachbearbeiterin des Bürgeramts nahm irrtümlich an, dass er eine Auskunftssperre wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen[52] beantragen wollte und händigte ihm den dazugehörigen Antrag aus. Erst im Rahmen der weiteren Bearbeitung des Antrags durch das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) und nachdem wir uns an das LABO gewandt hatten, klärte sich auf, dass der Betroffene tatsächlich eine Sperrung seines Datensatzes wegen einer Vornamensänderung wünschte.[53] Hierfür wäre gar keine Antragstellung erforderlich gewesen, denn Betroffene haben in diesen Fällen Anspruch auf automatische Auskunftssperre. Das LABO prüfte daraufhin die im Melderegister zum Betroffenen enthaltenen Datensätze und informierte uns, dass zum Beschwerdeführer bereits aufgrund der bei einem anderen Bezirksamt durchgeführten Namensänderung tatsächlich bereits eine Auskunftssperre eingerichtet worden war.

Dieser Fall hat uns gezeigt, dass das Vorgehen bei der Einrichtung einer Übermittlungssperre im Melderegister aufgrund einer Änderung des Vornamens oder der Geschlechterzugehörigkeit offenbar nicht bei allen Betroffenen sowie Bürgerämtern bekannt ist, sodass es zu dem beschriebenen Missverständnis bzw. der nicht sachgerechten Bearbeitung des Bürgeranliegens kommen konnte.

Personen, die sich nicht ihrem Geburtsgeschlecht, sondern einem anderen Geschlecht als zugehörig empfinden, haben das Recht, in einem gerichtlichen Verfahren ihren Vornamen und ihr Geschlechtsmerkmal (Personenstand) von weib-

52 Siehe § 51 Abs. 1 BMG

53 Siehe § 51 Abs. 5 BMG i. V. m. dem Personenstandsgesetz (PStG), TSG

lich auf männlich oder umgekehrt ändern zu lassen. Das TSG sieht zwei Verfahren mit unterschiedlicher rechtlicher Wirkung vor. Zum einen betrifft dies die Vornamensänderung der betroffenen Person ohne Änderung der im Geburts- und Melderegister registrierten Geschlechtszugehörigkeit (§ 1 TSG) und zum anderen die gerichtliche Feststellung eines Wechsels der Geschlechtszugehörigkeit (§ 8 TSG). Wenn die gerichtliche Entscheidung rechtskräftig ist, so dürfen die zur Zeit der Entscheidung geführten Vornamen bzw. das Geschlecht ohne Zustimmung des Antragstellers grundsätzlich nicht offenbart oder ausgeforscht werden.[54]

Die Meldebehörde ändert den Vornamen oder die Geschlechterzugehörigkeit im Melderegister nur dann, wenn durch die Vorlage eines Gerichtsbeschlusses die jeweilige Änderung nachgewiesen wurde oder das Standesamt die Personenstandsänderung mitgeteilt hat. Für die Vornahme der Sperrung des Datensatzes im Melderegister ist kein gesonderter Antrag der betroffenen Person notwendig. Vielmehr wird die Auskunftssperre von Amts wegen eingetragen, wenn die Meldebehörde eine Änderung des Vornamens oder des Geschlechts im Melderegister vornimmt. Der Datensatz mit dem früheren Vornamen bzw. Geschlecht wird automatisch im Fachverfahren geschlossen und es wird ein neuer Datensatz aufgebaut.[55]

Betroffene haben bereits nach der Vornamensänderung gemäß § 1 TSG einen Anspruch darauf, ihrem neuen Rollenverständnis entsprechend angeredet und angeschrieben zu werden.[56] Um dies zu gewährleisten, sind die entsprechenden Änderungen der Melderegisterdaten unverzüglich vorzunehmen. Im Rahmen einer Melderegisterauskunft besteht jedoch das grundsätzliche Risiko, dass durch Übermittlung des früheren Vornamens auch die Tatsache der transsexuellen Vorgeschichte bekannt wird. Daher hat die Meldebehörde von Amts wegen eine Auskunftssperre ins Melderegister einzutragen. Die Bezirksämter bzw. deren zuständige Stellen sollten sich mit dieser weniger bekannten Auskunftssperre im Melderegister vertraut machen, damit die Bürgerinnen und Bürger sachgerecht beraten werden können.

54 § 5 Abs. 1 TSG bzw. § 10 Abs. 2 TSG

55 Siehe Nr. 3.1.1.3 i. V. m. Nr. 3.1.1.1 Allgemeine Verwaltungsvorschrift zur Durchführung des Bundesmeldegesetzes (BMGVwV)

56 BVerfG, Beschluss vom 15. August 1996 – 2 BvR 1833/959

3.7 Verschwiegenheitserklärung der Polizei für Abgeordnete

Von einem Mitglied des Abgeordnetenhauses von Berlin wurden wir darüber unterrichtet, dass die Polizeibehörde von ihm im Rahmen seiner regelmäßigen Hospitationen, aber auch bei regulären Gesprächen, die er in seiner Eigenschaft als Abgeordneter wahrnehme, die Abgabe einer schriftlichen „Verpflichtungserklärung zur Wahrung des Datengeheimnisses („Verschwiegenheitserklärung") im Zusammenhang mit der Durchführung von Dienststellenbesuchen, Hospitationen und Einsatzbegleitungen" verlange. Wir wurden gebeten zu prüfen, inwieweit durch die Pflicht zur Abgabe der Erklärung die verfassungsrechtlichen Aufgaben des Abgeordneten beschränkt werden.

Die Einholung einer Verschwiegenheitsverpflichtung im Vorfeld von Hospitationen bei Behörden ist allgemein üblich und stellt eine wichtige Maßnahme zur Wahrung von Dienstgeheimnissen dar. Generell ist es sinnvoll, eine solche Verschwiegenheitserklärung nicht nur auf Dienstgeheimnisse zu beziehen, sondern sie auch auf personenbezogene Daten zum Zweck des Datenschutzes zu erstrecken. Dienstgeheimnisse und personenbezogene Daten können zwar dieselben Inhalte betreffen (wie bspw. Patientendaten im Rahmen der ärztlichen Schweigepflicht), sind jedoch in aller Regel verschiedene Informationen und daher voneinander zu trennen. Die Nutzung einer Verschwiegenheitserklärung im Rahmen von Hospitationen bei Behörden, die auch den Schutz personenbezogener Daten umfasst, die von den jeweiligen Hospitanten zur Kenntnis genommen werden, ist daher grundsätzlich zu befürworten und zu empfehlen.

Bei der Frage nach der Rechtmäßigkeit einer Verschwiegenheitserklärung, die von Abgeordneten verlangt wird, sind sowohl datenschutzrechtliche als auch (landes-)verfassungsrechtliche Aspekte berührt.

Es ist allgemein anerkannt, dass aus Art. 45 Abs. 2 Verfassung von Berlin (VvB) ein verfassungsrechtlicher Informationsanspruch der Abgeordneten gegenüber öffentlichen Einrichtungen des Landes abgeleitet werden kann. Das normierte Einsichtsrecht von Abgeordneten gilt jedoch nicht schrankenlos. Die Einsichtnahme eines Abgeordneten in Akten kann abgelehnt werden, wenn überwie-

gende öffentliche oder private Interessen an der Geheimhaltung dies zwingend erfordern.[57]

Zu den geschützten öffentlichen Interessen gehört der Schutz der Strafverfolgung sowie der präventiven polizeilichen Ermittlung; überwiegende private Interessen sind insbesondere solche des Schutzes personenbezogener Daten. Sind bei der Einsicht personenbezogene Daten besonderer Kategorien, wie etwa Gesundheitsdaten, berührt, ist Art. 45 VvB europarechtskonform im Lichte des Art. 9 DS-GVO über die Zulässigkeit der Verarbeitung solcher sensitiver Daten auszulegen, mit dem Ergebnis, dass in diesem Fall zwingend von einem überwiegenden privaten Interesse und einem Erfordernis der Geheimhaltung auszugehen ist.

Es kann somit festgestellt werden, dass eine Verschwiegenheitserklärung, die es den Abgeordneten generell untersagt, personenbezogene Daten zu verarbeiten, das Informationsrecht der Abgeordneten unverhältnismäßig beschränken würde und damit unzulässig wäre. Eine Erklärung mit dem Inhalt, die Weitergabe von personenbezogenen Daten besonderer Kategorien[58] an Dritte zu unterlassen und keine dieser Daten zu veröffentlichen, wäre dagegen zulässig. Dies gilt auch für eine Erklärung, die es den Abgeordneten untersagt, Bildaufnahmen, Privatanschriften sowie Telefonnummern von einzelnen Personen an Dritte weiterzuleiten oder zu veröffentlichen.

Der Senatsverwaltung für Inneres und Sport haben wir diese Auffassung in einer schriftlichen Stellungnahme mitgeteilt. Der Text der Erklärung, der zunächst die Verpflichtung enthielt, jegliche Verarbeitung personenbezogener Daten (sowie einsatz- und/oder kriminaltaktischer Informationen) zu unterlassen, wurde daraufhin geändert.

Gegen die Verwendung der überarbeiteten Fassung der „Verpflichtung zur Wahrung des Dienstgeheimnisses („Verschwiegenheitserklärung“) im Zusammenhang mit der Durchführung von Dienststellenbesuchen, Hospitationen und Einsatzbegleitungen der Polizei Berlin“ auch bei Mitgliedern des Abgeordnetenhauses von Berlin bestehen keine grundlegenden datenschutzrechtlichen

57 Art. 45 Abs. 2 S. 2 VvB

58 i. S. v. Art. 9 DS-GVO

Bedenken. Dies gilt auch für die Regelung, die eine Weitergabe von personenbezogenen Daten (insbesondere bei besonderen Kategorien von personenbezogenen Daten) an Dritte für grundsätzlich unzulässig erklärt. Allerdings sollte der Begriff „Dritte“ hier näher definiert werden. Soweit durch die Regelung Abgeordnete daran gehindert wären, Erkenntnisse, die sie bei Hospitationen gewonnen haben, im Rahmen ihrer parlamentarischen Tätigkeit insbesondere an Personen innerhalb des parlamentarischen Raums (z.B. andere Abgeordnete) weiterzugeben, könnte deren Funktion als Kontrollorgan der Exekutive unzulässig eingeschränkt sein.

3.8 Einwilligung bei „mini-Meisterschaften“ im Tischtennis

Der Deutsche Tischtennis-Bund e. V. veranstaltet zum Zwecke der Mitgliedergewinnung die sog. mini-Meisterschaften, an denen Kinder bis 12 Jahre ohne vorherige Anmeldung teilnehmen können. Die Kinder konnten dabei ihre Einwilligung in die Verarbeitung der Daten geben, damit sie die nächsten Austragungsorte und -termine der Meisterschaften erfahren. Hierzu ging eine Beschwerde bei uns ein.

Eine Datenverarbeitung kann grundsätzlich nicht auf eine Einwilligung[59] von Kindern gestützt werden. Bei Kindern der hier in Rede stehenden Altersgruppe fehlt es regelmäßig an der Fähigkeit, eine informierte Einwilligung zu erteilen. Denn eine solche Einwilligung setzt voraus, dass die Kinder die Konsequenzen der Verwendung ihrer Daten verstehen und zudem in der Lage sind, ihre Datenschutzrechte selbstständig auszuüben.

Unter bestimmten Voraussetzungen lässt sich die Verarbeitung der Daten jedoch auf die DS-GVO als gesetzliche Grundlage[60] stützen. Demnach wäre sie zulässig, wenn sie zur Wahrung berechtigter Interessen der Verantwortlichen erforderlich ist, „sofern nicht die Interessen oder Grundrechte und -freiheiten der betroffenen

59 Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO
60 Art. 6 Abs.1 lit. f DS-GVO

Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt".

Die Mitgliedergewinnung durch die Veranstaltungen von Meisterschaften ohne vorherige Anmeldung stellt ein berechtigtes Interesse des Tischtennisbundes dar. Die Erhebung und Speicherung der Daten ist auch erforderlich, da die Kinder zum einen die nächsten Austragungstermine und -orte nicht immer kennen, zum anderen ausschließlich die Daten der Kinder erfasst werden, die sich für die nächste Runde qualifiziert haben. Zwar weist der europäische Gesetzgeber[61] darauf hin, dass insbesondere bei Kindern grundsätzlich von einem Überwiegen derer Interessen auszugehen ist. Allerdings kann eine Betrachtung im Einzelfall ergeben, dass die Interessenabwägung zugunsten des Veranstalters ausfällt. Dies ist abhängig von der konkreten Ausgestaltung und den getroffenen Schutzmaßnahmen. Die Kinder sollen vorliegend nur einmalig postalisch und ausschließlich zur Mitteilung des Austragungstermins und -ortes angeschrieben werden. Darüber hinaus soll den Eltern der Kinder ein Widerspruchsrecht zur Datenverarbeitung eingeräumt werden. Nach dem Anschreiben und der Durchführung der nächsten Runde sollen zudem die Daten gelöscht werden. Daher ist lediglich von geringen Beeinträchtigungen auszugehen.

Kinder unter 12 Jahren können regelmäßig keine informierte Einwilligung zu einer Datenverarbeitung erteilen, da sie die Folgen ihrer Einwilligung nur schwer abschätzen können. Eine einzelfallbezogene Interessenabwägung kann jedoch zum Ergebnis führen, dass eine Datenverarbeitung in solchen Fällen dennoch zulässig ist.

61 Art. 6 Abs.1 lit. f letzter HS DS-GVO

3.9 Veröffentlichung von Kontaktdaten auf einem Sportportal

Der Tischtennisverband Berlin-Brandenburg e. V. veröffentlichte private Kontaktdaten von in Funktionen gewählte sowie mannschaftsführenden Personen (Mobiltelefonnummer und E-Mail-Adresse) im öffentlich zugänglichen Bereich ihrer Internetseite. Dies sollte die Kommunikation im Zusammenhang mit Tischtennisturnieren ermöglichen. Die Daten wurden von einem Verein des Verbandes auf der Plattform eingestellt.

Der Tischtennisverband nutzt für die Veranstaltung von Verbandsspielen zwischen Mitgliedsvereinen eine Internetseite. Dieses Portal dient vor allem als Kommunikationsplattform und zur Veröffentlichung von Turnierergebnissen. Es hat einen öffentlich zugänglichen Bereich sowie einen passwortgeschützten Mitgliederbereich.

Verantwortlich waren vorliegend sowohl der Verband, der die Plattform zur Verfügung stellt, als auch der Verein selbst, der die Daten in der Rubrik „Vereinsinfo" öffentlich zugänglich eingestellt hat.

Sofern keine Einwilligung der betroffenen Personen vorliegt, ist eine Veröffentlichung der privaten Kontaktdaten von Vereinsmitgliedern nur dann rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Grundrechte und Grundfreiheiten der Betroffenen nicht überwiegen[62]. Zwar stellt die Ermöglichung der Kommunikation im Zusammenhang mit den vom Tischtennisverband organisierten Turnieren ein berechtigtes Interesse dar. Allerdings war die Veröffentlichung der privaten Kontaktdaten im öffentlich zugänglichen Bereich hierfür nicht erforderlich. Insoweit steht ein weniger einschneidendes Mittel zur Verfügung. Die Kontaktdaten müssen nur für Teilnehmerinnen und Teilnehmer des Turniers einsehbar sein. Da der Tischtennisverband auch einen geschlossenen Mitgliederbereich des Portals zur Verfügung stellt, wäre es dem Verein sowie dem Tischtennisverband möglich gewesen, die für notwendig gehaltenen Daten dort zu veröffentlichen.

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

Die Veröffentlichung privater Kontaktdaten im öffentlich zugänglichen Bereich einer Webseite eines Sportverbands ist in der Regel nicht erforderlich und damit rechtswidrig. Es ist ausreichend, wenn solche Kontaktdaten in einem passwortgeschützten Mitgliederbereich einsehbar sind.

4 Verkehr und Tourismus

4.1 Jelbi“ – Die Mobilitäts-App der BVG

Die BVG verfolgt zunehmend das Ziel, neben dem eigenen auch Angebote weiterer Verkehrsunternehmen im Sinne eines „intermodalen Verkehrs“ über eigene Apps anzubieten. Als intermodal werden Angebote bezeichnet, die verschiedene Verkehrsmittel miteinander kombinieren und abgleichen, um für die gewünschte Route der Nutzerin oder des Nutzers eine möglichst optimale Verbindung zu entwickeln. Das kann beispielsweise dazu führen, dass eine Strecke, welche die Interessenten bisher stets mit dem Auto zurückgelegt haben, ihnen nun alternativ in einer Kombination von öffentlichem Nahverkehr und Leihfahrrädern vorgeschlagen wird, da dies eine noch schnellere, ökologische oder sogar kostensparende Alternative wäre.

Durch derartige Angebote sollen verschiedene Fortbewegungsmittel sinnvoll miteinander verknüpft werden. Neben weiteren Anbietern, die derartige Dienste schon seit längerem bereitstellen, hat nun auch die BVG zu diesem Zweck vor einigen Monaten eine eigene App namens „Jelbi“ veröffentlicht, die neben Fahrauskünften auch Buchungen und die Bezahlung von Fahrmöglichkeiten anbietet.

Der Ansatz der BVG, den intermodalen Verkehr zu fördern, ist grundsätzlich durchaus begrüßenswert. Allerdings fallen bei derartigen Angeboten auch sehr viele personenbezogene Daten an[63], die datenschutzkonform behandelt werden müssen. Dies wurde bei der Entwicklung der „Jelbi“-App weitgehend missachtet. Die Anwendung wurde von der BVG vielmehr entwickelt und der Öffentlichkeit präsentiert, ohne dass die Berliner Beauftragte für Datenschutz und Informationsfreiheit vorab über das Vorhaben informiert und um Stellungnahme gebeten worden wäre.

63 U. a. Bewegungsdaten, genutzte Verkehrsmittel, Adressdaten, Führerscheinbesitz und Zahlungsdaten

Wir konnten das Angebot daher leider erst überprüfen, nachdem wir aus der Presse von dem Vorhaben erfahren haben. Schon bei kursorischer Überprüfung des Angebots stellten wir verschiedene Datenschutzverstöße fest. So wurden die Bewegungsdaten der Nutzenden anfangs nur unzureichend anonymisiert, wodurch individualisierbare Bewegungsprofile entstanden. Zu monieren war darüber hinaus die unzureichende Transparenz gegenüber den Kundinnen und Kunden hinsichtlich der im Rahmen des „Jelbi"-Angebots beauftragten Dritt-Unternehmen. Auch bei Kleinstbeträgen wurden bereits Bonitätsauskünfte durch den beauftragten Zahlungsdienstleister eingeholt, sofern die Nutzenden nicht vorher bereits bekannt waren. Dies sogar in Fällen, in denen eine Bonitätsprüfung schon deshalb nicht notwendig gewesen wäre, weil – wie z.B. bei der Bezahlung mit Kreditkarte – die Zahlung bereits über das kartenausgebende Institut garantiert wird. Weiter war festzustellen, dass bei der Suche nach geeigneten Verkehrsmitteln mitunter auch personenbezogene Daten der Nutzenden schon dann weitergegeben wurden, wenn lediglich eine Verkehrsinformation gewünscht war und noch keine verbindliche Buchung. Bei Buchungen fehlte die detaillierte Angabe, welche Stammdaten an den jeweiligen Mobilitätspartner weitergegeben werden. Sofern ein Führerschein erforderlich war, z.B. bei der Buchung von Mietwagen, mussten die Nutzenden zur Bestätigung der Echtheit der im Führerschein enthaltenen Personendaten außer ihrem Führerschein auch ihren Personalausweis sowie ein Video oder Bild zur Verifizierung an den Dienstleister Veriff übermitteln.

Insgesamt hat sich gezeigt, dass die BVG noch diverse Datenschutzprobleme beheben musste und das „Jelbi"-System zum Zeitpunkt unserer Prüfung nicht als datenschutzkonform angesehen werden konnte.

Wir haben der BVG daher aufgetragen, die benannten Probleme zu beheben und für eine datenschutzfreundliche Möglichkeit zur Nutzung des Angebots Sorge zu tragen. Die BVG hat daraufhin begonnen, ihre Apps insgesamt einer datenschutzrechtlichen Revision zu unterziehen. Zudem wird auch vorerst von der Speicherung von Bewegungsdaten bei „Jelbi" abgesehen, bis die BVG ein ausgereiftes Anonymisierungskonzept ausgearbeitet hat.

Im Sinne eines erhöhten Komforts für die Kundinnen und Kunden sowie zur Förderung nachhaltiger und umweltschonender Mobilität sind intermodale Verkehrsangebote wie „Jelbi" durchaus zu begrüßen. Jedoch sollte hier stets der zu erwartende Nutzen durch die Technik mit den möglichen datenschutzrechtlichen Risiken abgewogen werden. Neben der Datensicherheit und dem Datenschutz ist auch eine ausreichende Transparenz gegenüber den Kundinnen und Kunden wichtig, damit diese stets umfassend darüber informiert sind, welche Daten ggf. gesammelt werden und welche Stellen Zugriff auf ihre Daten haben. Nur so kann das Recht auf informationelle Selbstbestimmung der Nutzenden auch effektiv verwirklicht werden. Wir werden die weitere Entwicklung bei „Jelbi" daher aufmerksam beobachten.

4.2 Eine komplette Datenbank? – Das kostenlose Schülerticket der BVG

Der Berliner Senat hat beschlossen, ab dem Schuljahr 2019/20 ein sog. kostenloses Schülerticket für den öffentlichen Nahverkehr einzuführen. Die Beantragung des Tickets ist bei der BVG ausschließlich online über ein Formular möglich, bei dem auch jeweils ein Passfoto der Schülerinnen und Schüler hochzuladen ist. Bei uns sind deshalb mehrere Beschwerden und allgemeine Anfragen zu dem Verfahren und der Speicherung der Daten bei der BVG eingegangen. Eine Sorge war, dass die BVG eine Datenbank über alle Schülerinnen und Schüler aufbaut.

Ermäßigte Monats- und Jahrestickets für Schülerinnen und Schüler wurden bereits bisher im Abonnement verkauft. Sie wurden durch das Land Berlin subventioniert, weshalb sie regelmäßig bedeutend günstiger als reguläre Abonnements waren. Der Senat hat nun beschlossen, für alle Schülerinnen und Schüler ein kostenfreies Jahresticket anzubieten, bei dem es sich weiterhin um ein Abonnement handelt, nicht um ein schlichtes kostenfreies Fahren für alle Schülerinnen und Schüler, bei dem bspw. der Schülerausweis als Nachweis genügen würde. Der einzige Unterschied zur bisherigen Situation besteht darin, dass die Familien nunmehr einen hundertprozentigen Zuschuss vom Land Berlin für diese Tickets erhalten anstelle der bisherigen Teilsubventionierung. Das Abonnementmodell wurde dabei gewählt, weil auf der einen Seite die BVG auf diese Weise die durch

die kostenlosen Schülertickets bei ihr entstehenden Kosten mit dem Land Berlin abrechnen und der Senat im Gegenzug u. a. nachvollziehen kann, wie viele Personen dieses Angebot wahrnehmen.

Das kostenlose Schülerticket wird von allen Berliner Nahverkehrsunternehmen, also der S-Bahn, dem Verkehrsverbund Berlin-Brandenburg (VBB) und der BVG, ausgegeben. Die Eltern, Erziehungsberechtigten oder Schülerinnen und Schüler schließen einen Abonnement-Vertrag mit einem dieser Nahverkehrsunternehmen. Für diesen Vertrag erhebt die BVG die Daten und speichert sie während der Laufzeit des Abonnements in einer Datenbank zusammen mit anderen aktiven Abonnement-Verträgen. Wird der Vertrag nicht fortgeführt, werden die Daten in ein getrenntes und zugriffsbeschränktes System verschoben. In diesem System werden die Daten noch so lange gespeichert, wie dies handels- und steuerrechtlich vorgeschrieben ist.

Die BVG ist ebenso wie auch die anderen Verkehrsunternehmen gegenüber dem Land Berlin rechenschaftspflichtig. Sie muss also nachweisen, wie viele Fahrscheine ausgegeben wurden, um die Ausgleichszahlungen zu erhalten und dies im Falle einer Wirtschaftsprüfung im Einzelnen belegen zu können. Dementsprechend ist die BVG verpflichtet, Daten auch von allen Personen zu erheben und zu speichern, die ein kostenfreies Schülerticket abonnieren.

Grundsätzlich bestehen hiergegen keine datenschutzrechtlichen Bedenken. Wir überprüfen allerdings aktuell, inwieweit es an einzelnen Stellen noch Verbesserungsmöglichkeiten gibt, bspw. ob alle geforderten Daten auch tatsächlich erhoben werden müssen, wie z.B. das Geburtsdatum von Erziehungsberechtigten. Zudem muss die BVG die Speicherfristen im Einzelnen noch auf das absolut Notwendige reduzieren; auch hier befinden wir uns noch in der Prüfung. Beispielsweise werden die Fotos für den Fahrschein derzeit erst nach acht Wochen gelöscht, um für den Fall des Verlustes eines Fahrscheins diesen noch einmal ausstellen zu können. Hier ist eine deutliche Reduzierung der Frist denkbar. Ein weiterer Punkt ist das Erfordernis, eine Kopie des Schülerausweises hochzuladen, um die grundsätzliche Berechtigung für das Schülerticket nachzuweisen. Hier prüft die BVG, ob sie die Kopien für eine Rechnungsprüfung durch das Land vorhalten muss oder ob diese unmittelbar nach der Überprüfung der Berechtigung gelöscht werden können. Die weiteren erhobenen Daten, auch die E-Mail-Adresse der Person, die

ein Ticket online bestellt, sind Teil der erhebungs- und aufbewahrungspflichtigen Unterlagen.

Einige Kritik gab es allerdings auch daran, dass die Anträge ausschließlich online gestellt werden können. Es ist für die BVG gesetzlich nicht zwingend vorgegeben, Anträge auch auf nicht elektronischem Wege entgegenzunehmen. Da die BVG sich kurzfristig auf eine große Zahl an Neuanträgen einstellen musste, ist das ausschließlich elektronische Antragsverfahren in dieser Situation vielleicht noch vertretbar gewesen. Entsprechend der Verpflichtung von Berliner Behörden, Anträge auch analog entgegenzunehmen,[64] sollte die BVG als Anstalt öffentlichen Rechts als datenschutzfreundliche Alternative jedoch zukünftig auch wieder ein nicht elektronisches Antragsverfahren bereitstellen.

Die BVG schließt auch bei dem kostenfreien Schülerticket weiterhin Abonnement-Verträge mit den Eltern, Erziehungsberechtigten oder Schülerinnen und Schülern selbst ab. Im Rahmen dieser Verträge ist sie befugt, Daten zu erheben und muss diese Unterlagen für ihre Buchhaltung zeitweise aufbewahren. Dabei ist jedes einzelne Datum jedoch auf seine Erforderlichkeit hin zu überprüfen. Technisch muss auf aktuelle Verschlüsselungsstandards geachtet werden.

4.3 Warum Fahrräder Bewegungsprofile erstellen

Seit November 2017 stehen mehrere tausend Mietfahrräder der Mobike Germany GmbH (Mobike) auf Berliner Straßen. Wie auch andere Leihfährräder, Mietroller oder -autos lassen sie sich über eine App ausleihen. Kritisch betrachtet wurde vor allem, dass die Mobike-App viele Daten erhebt, die im Auftrag in China verarbeitet werden.

Die Mobike-App erfasst die Bewegungsdaten der Nutzenden, während diese mit der App auf der Suche nach einem Fahrrad sind sowie durchgehend während der Fahrzeit, solange die App im Hintergrund läuft. Sie kann während der Fahrzeit aber auch geschlossen werden; in diesem Fall werden keine weiteren

64 § 4 Abs. 7 E-Government-Gesetz Berlin (EGovG Bln)

Bewegungsdaten erfasst. Abgesehen davon teilt das Fahrrad per GPS selbst alle vier Stunden Mobike seinen Standort mit. Eine Verknüpfung dieser per GPS mitgeteilten Standortdaten des Fahrrads mit den Daten der App findet nicht statt. Ferner erhebt Mobike eine Vielzahl von Gerätedaten des Smartphones wie das Hardware-Modell, die eindeutige Gerätekennung oder wahlweise die eindeutige Werbekennung eines Geräts.

Um den Leihvertrag abzuwickeln, dürfen nur die hierfür unbedingt notwendigen Daten erhoben werden. Dies ist bei den Standortdaten der jeweilige Start- und Zielpunkt. Hiermit können die Mietzeit sowie eventuelle Verstöße gegen die Regeln von Mobike zum Abstellen der Fahrräder festgestellt werden. Auch die Erfassung von Gerätedaten ist nur in dem Umfang zulässig, in dem die App die Informationen benötigt, um zu funktionieren. Darüber hinausgehende Datenerhebungen sind nur mit einer rechtlich zulässigen Begründung oder einer freiwilligen Einwilligung der Nutzenden zulässig. Beides konnte Mobike bei unserer Prüfung nicht vorweisen. Eine vollständige Erfassung der Route ist weder zum Schutz vor Diebstahl noch aus anderen Gründen notwendig. Auch die Übermittlung von eindeutigen Gerätekennungen zur Verbesserung der App ist nicht zulässig.

Wir haben das Unternehmen aufgefordert, die Erhebung der Daten deutlich einzuschränken, und ihm hierfür eine Frist bis Anfang 2020 gesetzt.

Die erhobenen Daten lässt Mobike von dem in Beijing (China) ansässigen Mutterunternehmen im Auftrag verarbeiten. Beide Unternehmen haben Verträge abgeschlossen, welche den Rahmen der zulässigen Verarbeitung über nach der DS-GVO zulässige Standardvertragsklauseln festschreiben.[65] Dies ist rechtlich nach derzeitigem Kenntnisstand formal nicht zu beanstanden, allerdings werden die Standardvertragsklauseln vom EuGH gerade überprüft.[66]

65 Dies sind Verträge auf Basis der Standardvertragsklauseln gemäß dem Beschluss der Europäischen Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (2010/87/EU).

66 EuGH-Verfahren zum Az. C-311/18 (sog. Schrems II-Verfahren)

Auf der Grundlage eines Vertrags zwischen einer Person, deren Daten verarbeitet werden, und den für die Verarbeitung verantwortlichen Unternehmen dürfen nur die Daten verarbeitet werden, die für den Vertrag unerlässlich sind. Daten, die darüber hinaus erhoben werden, dürfen nur mit rechtlich nachvollziehbarer Begründung und unter Berücksichtigung der Auswirkungen auf die informationelle Selbstbestimmung der Betroffenen erhoben werden.

4.4 Besichtigung mit Spam-Begleitung

Täglich erhalten wir viele Anfragen zur unerlaubten Zusendung von Werbe-E-Mails. Hierbei handelt es sich z.B. um Beschwerden wie: „Bei der Registrierung auf einer Online-Plattform musste zugleich in die Zusendung von Werbe-E-Mails eingewilligt werden“ oder „An meine E-Mail-Adresse erhalte ich unerwünschte Newsletter, obwohl niemals eine Einwilligung zum Erhalt von Newslettern erteilt wurde“.

Ein Beispiel von vielen: Für den bevorstehenden Berlinbesuch wollte eine Familie Eintrittskarten für eine Sehenswürdigkeit sowie eine Tischreservierung im dortigen Restaurant buchen. Hierbei wurde ihr mitgeteilt, dass sie mit der Anmeldung auch eine Einwilligung in die Zusendung von Nachrichten des Anbieters, z.B. für Newsletter o. Ä., abgebe. Der entsprechende Hinweistext suggerierte eine Einwilligung durch eine entsprechende Voreinstellung. Diese kann jedoch nicht als wirksam angesehen werden, da es an einer eindeutigen Handlung (z.B. Setzen eines Hakens) und der Freiwilligkeit der Einwilligungserklärung fehlt.

Wir haben versucht, den Anbieter davon zu überzeugen, schon allein aus Gründen der Kundenzufriedenheit den Hinweis in eine wirksame Einwilligung zu ändern – schließlich wird die Sehenswürdigkeit i. d. R. von Touristen besucht, die nach ihrer Rückreise kaum an weiteren Informationen zum Restaurant etc. interessiert sein dürften. Das war jedoch nicht erfolgreich.

Nach ersten anderslautenden Mitteilungen stellte der Anbieter dann jedoch klar, dass er gar keine Werbe-E-Mails versende, sondern lediglich die Kundinnen und Kunden bitte, ihm eine Rückmeldung zu ihrem Besuch zu geben. Diese Bewertungsbitten würden nach dem jeweiligen Besuch versendet.

Dies ist anders zu beurteilen als etwa der Versand eines Newsletters. Die Zusendung einzelner einfacher Kundenzufriedenheitsabfragen im Nachgang zu einer Bestellung erfolgt im berechtigten Interesse des Anbieters, das – im Gegensatz zur reinen Werbung – das Interesse der Kunden, keine solche Nachfragen zu erhalten, überwiegt. Allerdings nur unter der Voraussetzung, dass die Kundinnen und Kunden einen klaren und deutlichen Hinweis auf dieses Vorgehen erhalten und jederzeit widersprechen können.

Jedoch dürfen auch für eine Bitte um Bewertung Kundendaten nicht endlos gespeichert werden. Sofern die Speicherung einer E-Mail-Adresse für die Zwecke, für die sie erhoben bzw. verarbeitet worden ist, nicht mehr erforderlich ist, ist sie in einem angemessenen Zeitrahmen zu löschen. Für die Durchführung von Kundenzufriedenheitsabfragen wäre allenfalls ein Zeitraum von einem Monat nach dem Besuch der jeweiligen Sehenswürdigkeit begründbar. Die Verpflichtung zur Löschung beinhaltet im Übrigen, dass Verantwortliche ihre Löschungsverpflichtungen selbstständig und laufend überprüfen.

Ein Löschkonzept für alte Einträge in der Werbeliste existierte in diesem konkreten Fall offensichtlich nicht; entsprechende Nachfragen bezüglich Speicherdauer und Löschkonzept wurden nur mit dem Hinweis beantwortet, dass Kundinnen und Kunden per E-Mail oder Abmeldelink widersprechen könnten. Wir prüfen daher die Einleitung eines Ordnungswidrigkeitenverfahrens.

Grundsätzlich ist bei E-Mail-Werbung von einer unzulässigen Belästigung auszugehen. Bei Bestands-Kundinnen und -Kunden darf die speichernde Stelle im Rahmen der Kundenbeziehung die E-Mail-Adresse jedoch für weitere Werbung nutzen, sofern die folgenden Voraussetzungen gegeben sind:

- Ein Unternehmen hat im Zusammenhang mit dem Verkauf einer Ware oder der Erbringung einer Dienstleistung die elektronische Postadresse der Kundin oder des Kunden erhalten,

- das Unternehmen verwendet die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen,

- die Kundin oder der Kunde hat der Verwendung nicht widersprochen und

- bei Erhebung der Adresse und bei jeder Verwendung wird klar und deutlich darauf hingewiesen, dass der Verwendung jederzeit widersprochen werden kann.

Nur wenn alle hier genannten Voraussetzungen erfüllt sind, ist der Newsletter-Versand gesetzlich legitimiert und bedarf keiner gesonderten Einwilligung.

Gegen die Zusendung nicht berechtigter Werbe-E-Mails gibt es Mittel und Wege. Sollte ein Widerspruch nicht zum Erfolg führen, so kann die zuständige Aufsichtsbehörde helfen.

5 Jugend und Bildung einschließlich Medienkompetenz

5.1 Film- und Fotoaufnahmen von Kindern – Verunsicherung durch die Datenschutz-Grundverordnung

Aus der Praxis

In unserem letzten Jahresbericht haben wir darüber berichtet, dass mit dem Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) gerade im Hinblick auf den Umgang mit personenbezogenen Daten bei der Anfertigung und Veröffentlichung von Film- und Fotoaufnahmen von Kindern eine besondere Unsicherheit eingetreten ist.[67] Verwirrende Presseberichte über die angebliche Notwendigkeit der Schwärzung sämtlicher personenbezogener Angaben über die Kinder aus datenschutzrechtlichen Gründen haben diese Unsicherheit noch verstärkt.

Das Interesse an der Thematik hat auch in diesem Jahr nicht nachgelassen. Noch immer erreichen uns zahlreiche Anfragen und Beschwerden, in denen es um den datenschutzgerechten Umgang mit Film- und Fotoaufnahmen von Kindern, insbesondere in Kindertageseinrichtungen, geht. Die Thematik lässt sich jedoch auch auf Schulen oder auch Veranstaltungen, an denen Kinder teilnehmen, z.B. Ausstellungen, beliebig erweitern.

Voranzustellen ist, dass die Anfertigung von Film- und Fotoaufnahmen von Kindern und ggf. auch deren Veröffentlichung aus datenschutzrechtlichen Gründen nicht von vornherein unzulässig ist, sondern sich mit entsprechenden Einwilligungserklärungen durchaus datenschutzgerecht ausgestalten lässt. Explizite Einwilligungen sind jedoch erforderlich, da die Anfertigung von Foto- und Filmauf-

67 JB 2018, 5.4

nahmen von Kindern in Kindertageseinrichtungen oder auch Schulen nicht für die Betreuung der Kinder bzw. schulbezogene Aufgaben erforderlich ist und sich damit auch nicht durch Datenschutzvorschriften abdecken lässt. So lassen sich entsprechende Aufnahmen nicht darauf stützen, dass diese angeblich zur Wahrung der berechtigten Interessen des Verantwortlichen, d.h. der Einrichtung oder der Schule, erforderlich seien. Hierbei ist nämlich zu prüfen, ob das Schutzbedürfnis der betroffenen Person überwiegt, insbesondere dann, wenn es sich bei ihr um ein Kind handelt.[68] Die DS-GVO geht ausdrücklich von der besonderen Schutzbedürftigkeit von Kindern aus und stellt besondere Anforderungen hinsichtlich der Verarbeitung ihrer Daten. Daher ist unabhängig von der Frage, ob berechtigte Interessen des Verantwortlichen in Bezug auf die Anfertigung und Veröffentlichung von Fotoaufnahmen bestehen, davon auszugehen, dass die Interessen der betroffenen Personen von vornherein überwiegen, wenn es sich hierbei um Kinder handelt. Solche Aufnahmen lassen sich insoweit ausnahmslos nur auf Einwilligungen stützen.

Bei der Gestaltung entsprechender Erklärungen sind folgende Anforderungen zu beachten:

Die Einwilligung, die von den Eltern einzuholen ist, muss freiwillig und informiert erfolgen. Konkret bedeutet dies, dass den Eltern transparent gemacht werden muss, für welche möglichst genau beschriebenen Zwecke die Aufnahmen angefertigt werden sollen. Die Einwilligung der Eltern muss sich explizit sowohl auf die Anfertigung als auch auf die Veröffentlichung der Aufnahmen auf der Homepage oder in anderer Weise (z.B. Printpublikationen, Aushänge in den Räumlichkeiten) beziehen, sodass in der Erklärung zwischen Anfertigung und Veröffentlichung unterschieden werden sollte. In der Praxis bietet es sich an, für die unterschiedlichen Zwecke, z.B. Fotoaufnahmen auf Ausflügen oder Veranstaltungen, Zeigen von Filmsequenzen auf einem Elternabend oder Nutzung für die Erstellung von Lehrmaterial, jeweils Ankreuzfelder vorzusehen. Angesichts der mit Internetveröffentlichungen verbundenen Gefahren für die Persönlichkeitsrechte durch die Möglichkeit des weltweiten Abrufs bzw. die Möglichkeit, diese über Suchmaschinen aufzufinden und zu missbrauchen, empfehlen wir in unseren Beratungsgesprächen regelmäßig, hierauf in der Einwilligungserklärung auch deutlich hinzu-

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

weisen. Wichtig ist es auch, in der Einwilligungserklärung festzulegen, was mit den Aufnahmen geschehen soll und wie lange diese wo und wie aufbewahrt werden. Zudem ist es notwendig, die Eltern in der Erklärung darüber zu informieren, dass sie das Recht haben, ihre einmal erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Dies wird nach unseren Erfahrungen in der Praxis oft vergessen, ist jedoch ein notwendiges Kriterium für die Wirksamkeit einer Einwilligungserklärung. Schließlich sollten die Eltern darauf hingewiesen werden, dass die Aufnahme ihres Kindes in eine Einrichtung nicht von der Erteilung einer Einwilligungserklärung abhängig gemacht werden darf und ihnen auch keine Nachteile entstehen dürfen, wenn sie ihre Einwilligung später widerrufen.

Es ist unser Anliegen, den Einrichtungen die entstandene Unsicherheit im Umgang mit Foto- und Filmaufnahmen von Kindern zu nehmen. Dass das Interesse an der Thematik unverändert hoch ist, zeigt uns die Nachfrage nach unserem Handlungsleitfaden zum Datenschutz bei Bild-, Ton- und Videoaufnahmen[69], den wir gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Familie herausgegeben haben. Anfang 2020 werden wir daher gemeinsam mit der Senatsverwaltung eine Neuauflage dieses Handlungsleitfadens erstellen, in dem wir unsere ersten Erfahrungen mit der DS-GVO berücksichtigen werden.

5.2 Wer darf was im Jugendamt sehen?

Aus der Praxis

Seit mehreren Jahren berichten wir über die Einführung des verwaltungsübergreifenden Fachverfahrens ISBJ[70] als zentrale IT-Lösung in den Berliner Jugendämtern, mit der die Geschäftsprozesse in der Jugendhilfe vereinheitlicht werden sollen.[71] Hierzu gehört es auch, zu definieren, in welcher Weise die Zugriffsrechte für die Beschäftigten auf die jeweils erforderlichen personenbezogenen Daten technisch zu beschränken sind. In der Praxis erfordert dies teilweise eine Anpassung langjährig gewohnter Verfahrensweisen an die neuen Gegebenheiten.

69 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/informationsmaterialien/2018-BlnBDI_Flyer_Datenschutz_Inhalt_Web.pdf

70 Integrierte Software Berliner Jugendhilfe

71 JB 2018, 5.3; JB 2017, 2.3; JB 2016, 5.4

Wir wurden darüber informiert, dass innerhalb eines Jugendamts der durch die Fachsoftware beschränkte Zugriff einzelner Organisationseinheiten, die jeweils unterschiedliche Aufgaben wahrnehmen, dadurch umgangen wurde, dass Hilfepläne nunmehr in Papierform zwischen den Einheiten ausgetauscht wurden. Diese Hilfepläne enthalten sämtliche Festlegungen zum erzieherischen Bedarf, die zu gewährende Art der Hilfe sowie die Ausgestaltung und den Erfolg der Hilfe im jeweiligen Einzelfall.

Konkret werden Familien im Jugendamt durch den Regionalen Sozialpädagogischen Dienst (RSD) pädagogisch betreut. Die Wirtschaftliche Jugendhilfe (WJH) kümmert sich als weitere Organisationseinheit um die Finanzierung der gewährten Leistungen. Beide Stellen benötigen hierfür Informationen über die betreuten Familien. Wegen der Unterschiede in den wahrgenommenen Aufgaben dieser beiden Organisationseinheiten im Jugendamt sind die benötigten Informationen jedoch nicht deckungsgleich. Gerade die sozialpädagogische Betreuung erfordert es, auch sehr sensible Informationen über die Problemlagen in den Familien zu kennen. Deren Kenntnis ist jedoch in vielen Fällen nicht notwendig, um die Finanzierung der Hilfe sicherzustellen. Aus diesem Grund sind die Zugriffsmöglichkeiten auf die personenbezogenen Daten in der Fachsoftware beschränkt.

Eine Weitergabe der Hilfepläne in Papierform durch den RSD an die WJH ist mit datenschutzrechtlichen Grundsätzen ebenso wenig vereinbar wie die Weitergabe in digitaler Form, da für die Finanzierung der Leistungen nicht alle Informationen, die für die pädagogische Arbeit mit den Familien notwendig sind, erforderlich sind. Wir haben das Jugendamt gebeten, uns mitzuteilen, wie ein datenschutzgerechtes Verfahren etabliert werden soll. Das Jugendamt hat uns darüber informiert, dass verschiedene Maßnahmen geprüft würden. So sei ein Formular entwickelt worden, durch das gesichert werde, dass nur die wirklich notwendigen Daten innerhalb des Jugendamts weitergegeben werden. Auch werde geprüft, ob die nicht erforderlichen Daten in den Hilfeplänen geschwärzt werden könnten. Wir haben darauf hingewiesen, dass es entscheidend ist, organisatorisch sicherzustellen, dass nur die tatsächlich erforderlichen Daten zwischen den beiden Organisationseinheiten ausgetauscht werden. Neben den Stammdaten, auf die ein Zugriff in der Fachsoftware eingeräumt ist, darf die WJH nur diejenigen zusätzlichen Daten zur Kenntnis nehmen, die nach den konkreten Umständen im Einzelfall für ihre Aufgabenerfüllung erforderlich sind.

Wir gehen davon aus, dass das Jugendamt eine Verfahrensweise etablieren wird, die den datenschutzrechtlichen Anforderungen genügt. Das Beispiel zeigt, dass die Umstellung von Prozessen auf IT-Lösungen sehr gut geeignet sein kann, langjährig etablierte, aber unzulässige Verfahrensweisen zu hinterfragen, um einen datenschutzgerechten Zustand zu entwickeln.

5.3 Zum Einsatz von Office 365 in Schulen

Immer wieder erreichen uns Anfragen aus dem Schulbereich zur Zulässigkeit des Einsatzes von Office 365. Hierbei handelt es sich um ein Produkt des Unternehmens Microsoft Corp., das in der Regel die Office-Anwendungen in einer cloudbasierten Variante bereitstellt. Da sich die Frage der Zulässigkeit des Einsatzes nicht nur in Berlin, sondern bundesweit stellt und auch für andere Teile der öffentlichen Verwaltung relevant ist, befinden sich die Datenschutzaufsichtsbehörden des Bundes und der Länder seit mehreren Jahren mit Microsoft im Gespräch darüber, wie das Produkt datenschutzkonform genutzt werden kann.

Das Grundproblem liegt darin, dass Microsoft aufgrund der Beauftragung durch eine Behörde Kenntnis von Daten erhält, die auch für eigene Zwecke des Unternehmens genutzt werden, ohne dass hierfür eine Rechtsgrundlage ersichtlich wäre. Bei den Daten handelt es sich neben den Inhalten, die die Behörde verarbeitet, auch um Angaben über die Nutzerinnen und Nutzer, seien es Beschäftigte oder Schülerinnen und Schüler. Dies geschieht insbesondere über die Verwendung der Software.

Grundsätzlich ist es datenschutzrechtlich zwar denkbar, cloudbasierte Dienste privater Anbieter auch in öffentlichen Bereichen wie z.B. Schulen einzusetzen. Welche Anforderungen dabei jedoch erfüllt werden müssen, um die Vorgaben der DS-GVO einzuhalten, ist Gegenstand von Gesprächen zwischen den Datenschutzaufsichtsbehörden und Microsoft.

Ein besonderes Problem stellen die zwischen den Verantwortlichen und Microsoft abzuschließenden Verträge über eine Auftragsverarbeitung durch Microsoft dar. Microsoft verlangt von den Auftraggeberinnen und -gebern, dass diese die Weiterverarbeitung ihrer ggf. personenbezogenen Daten durch Microsoft auch für

Zwecke der Produktverbesserung zulassen. Für eine dementsprechende Beauftragung durch öffentliche Stellen und eine Bereitstellung von personenbezogenen Daten, die sich auf Beschäftigte oder Bürgerinnen und Bürger beziehen, ist eine Rechtsgrundlage nicht erkennbar.

Die deutschen Datenschutzaufsichtsbehörden befinden sich derzeit in einem engen Abstimmungsprozess darüber, wie gegenüber Microsoft erreicht werden kann, dass eine derartige Datenverwendung unterbleibt. Bis dahin bleibt es den Verantwortlichen überlassen, Office 365 so einzusetzen, dass die personenbezogenen Daten lediglich ohne Verwendung der Cloud in der eigenen Informationstechnik abgespeichert werden.

Uns ist sehr wohl bewusst, dass die Zeit bei den Verantwortlichen, die sich mit der Frage der Zulässigkeit eines Einsatzes von Office 365 in ihren Institutionen beschäftigen, drängt. Daher bringen wir uns intensiv in den Klärungsprozess der rechtlichen und technischen Probleme ein, um bei den Schulen, aber auch den anderen Akteuren in der öffentlichen Verwaltung für Rechtssicherheit zu sorgen. Wir gehen davon aus, dass die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zeitnah die Voraussetzungen für einen zulässigen Einsatz von Office 365 aufzeigen wird. Es wird an Microsoft liegen, seinen Teil zur Erfüllung dieser Voraussetzungen beizutragen.

5.4 Die Schuldatenverordnung – Eine neue Großbaustelle auf dem Weg zur Digitalisierung

Nachdem wir im vergangenen Jahr die Senatsverwaltung für Bildung, Jugend und Familie hinsichtlich der Anpassung des Berliner Schulgesetzes an die DS-GVO beraten haben,[72] stand in diesem Jahr die Novellierung der Schuldatenverordnung auf der Agenda.

72 JB 2018, 5.1

Die aus dem Jahr 1994 stammende Schuldatenverordnung wurde zuletzt im Jahr 2010 ergänzt, die wesentlichen Regelungen sind jedoch mittlerweile 25 Jahre alt. In der Zwischenzeit haben sich die tatsächlichen Gegebenheiten, insbesondere im Hinblick auf die Digitalisierung, allerdings so erheblich geändert und weiterentwickelt, dass die alte Verordnung dieser Entwicklung in keiner Weise mehr gerecht wird.

Um die Anforderungen an den Betrieb einer modernen Schule widerzuspiegeln, insbesondere auch vor dem Hintergrund des Berliner Digitalpakts, besteht erheblicher Änderungsbedarf. Daher hatten wir bereits seit Herbst 2018 sowohl schriftlich, als auch in mehreren Gesprächen empfohlen, eine vollständige Neustrukturierung der Verordnung vorzunehmen. Diesem Vorschlag ist die zuständige Senatsverwaltung jedoch bislang leider nicht gefolgt, obwohl dies in der mittlerweile verstrichenen Zeit hätte unproblematisch möglich sein müssen.

Der letzte uns vorliegende Entwurf für eine Novellierung vom August 2019 bedarf noch immer einer erheblichen Überarbeitung. Neben unklaren Regelungen zur Schulstatistik sowie zur Datenverarbeitung der Senatsverwaltung im Rahmen der Berufs- und Studienorientierung waren insbesondere Regelungen, mit denen auf die zunehmende Digitalisierung reagiert werden soll, unzureichend.

Um für die Akteure im Schulbereich Rechtssicherheit zu schaffen und „Wildwuchs“ zu verhindern, müssen in einer modernen Schuldatenverordnung die Rahmenbedingungen für die Nutzung digitaler Medien festgelegt werden. Als regelungsbedürftig sind insbesondere die Nutzung von privaten Geräten durch das Lehrpersonal und die Schülerschaft, die Nutzung sozialer Netzwerke und von Lernplattformen, die Anforderungen an die Netzwerkinstallation sowie die Nutzung von Messenger-Diensten zu nennen. Hierzu haben wir die Senatsverwaltung intensiv beraten. Es ist dringend erforderlich, dass die Schuldatenverordnung nunmehr zielorientiert und so schnell wie möglich verabschiedet und dieses wichtige Thema nicht noch länger verschleppt wird.

Um eine datenschutzkonforme Umsetzung der Digitalisierung in den Schulen sicherzustellen, muss die Senatsverwaltung zügig die dafür erforderlichen rechtlichen Rahmenbedingungen schaffen, an denen sich die Schulen orientieren können.

5.5 Forschung mit den Akten der Jugendämter – Möglichkeiten und Grenzen

Im vergangenen Jahr haben wir die Senatsverwaltung für Bildung, Jugend und Familie mehrfach dazu beraten, ob und unter welchen Bedingungen sie Anträgen von Forschenden auf Akteneinsicht bzw. auf Übermittlung einzelner Akten der Jugendämter stattgeben kann.

Die Akten der Jugendämter sind beliebte Objekte für die wissenschaftliche Forschung. Hierbei darf aber nicht außer Acht gelassen werden, dass diese Akten besonders schützenswerte Sozialdaten der betroffenen Familien enthalten. Eine Übermittlung von Sozialdaten an Dritte ist daher aus gutem Grunde an enge Voraussetzungen geknüpft.

Ob Jugendämter die durch sie verarbeiteten Sozialdaten zu Forschungszwecken an Dritte übermitteln dürfen, regelt das Sozialgesetzbuch (SGB).[73] Die strengen Voraussetzungen sehen vor, dass die Jugendämter – und andere Sozialleistungsträger – nicht selbst darüber entscheiden dürfen, Sozialdaten an Forschende herauszugeben. Vielmehr hat der Gesetzgeber wegen der besonderen Schutzbedürftigkeit von Sozialdaten ein Genehmigungserfordernis vorgesehen. So bedarf es vor der Übermittlung derartiger Daten stets einer Genehmigung durch die oberste Bundes- bzw. Landesbehörde, die für den Bereich, aus dem die Daten kommen, zuständig ist.[74] Für die Forschung im Kinder- und Jugendhilfebereich in Berlin ist dies die Senatsverwaltung für Bildung, Jugend und Familie.

Genehmigungsvoraussetzung ist zunächst, dass es sich nicht um „irgendein" Forschungsprojekt handelt, sondern um ein konkretes Vorhaben, das sich auf den Sozialleistungsbereich bezieht.[75] Weiter kommt eine Übermittlung von Sozialdaten überhaupt nur dann in Betracht, wenn diese für die Durchführung des Forschungsvorhabens auch tatsächlich erforderlich, also unumgänglich sind. Sind

73 Siehe § 75 SGB X

74 § 75 Abs. 4 SGB X

75 Darüber hinaus kann auch ein bestimmtes Vorhaben der wissenschaftlichen Berufs- und Arbeitsmarktforschung in Betracht kommen, § 75 Abs. 1 Satz 1 Nr. 1 SGB X.

diese „Eingangsvoraussetzungen“ erfüllt, bedarf es zudem grundsätzlich der Einwilligung der betroffenen Personen in die Übermittlung ihrer Sozialdaten. Allenfalls in Ausnahmefällen, nämlich dann, wenn die Einholung der Einwilligungen nicht zumutbar ist (z.B. weil der Zweck des Forschungsvorhabens vereitelt werden würde), kann eine Übermittlung auch möglich sein, ohne dass die Betroffenen zuvor gefragt werden.[76] In diesen Fällen sieht das SGB als weiteren Schutzmechanismus jedoch eine Güterabwägung vor. Eine Übermittlung ohne Einwilligung ist demnach nur dann möglich, wenn die schutzwürdigen Interessen der betroffenen Personen entweder überhaupt nicht beeinträchtigt werden oder aber eine Abwägung ergibt, dass das öffentliche Forschungsinteresse das Interesse der betroffenen Person an der Geheimhaltung erheblich überwiegt.

Die Senatsverwaltung für Bildung, Jugend und Familie hat uns im Rahmen mehrerer Forschungsprojekte um Beratung gebeten. In einem Projekt, in dem es um Forschung zur häuslichen Gewalt in Familien mit Kindern ging, haben wir die bereits von der Senatsverwaltung gegenüber den Forschenden vertretenen Ansicht, dass im konkreten Fall die Einholung von Einwilligungen der betroffenen Personen zumutbar und daher unumgänglich ist, bekräftigt und deren konkrete Gestaltung mit Hinweisen begleitet.

In einem weiteren Projekt, das die Senatsverwaltung selbst gegenüber der Universität Hildesheim in Auftrag gegeben hat und in dem es um die auch in der Öffentlichkeit viel beachtete Aufarbeitung der Rolle der Senatsverwaltung bei der Unterbringung von Jugendlichen bei pädophilen Männern im Rahmen des sog. „Kentler-Experiments“ ging, haben wir die Senatsverwaltung hingegen dahingehend beraten, die Akten vor der Übermittlung an die Forscherinnen und Forscher zu anonymisieren, da das Einholen von Einwilligungen betroffener Personen und Dritter, deren Daten ebenfalls in den Akten enthalten waren, praktisch nicht durchführbar gewesen wäre.

Wir können das große Interesse an der Einsichtnahme in Jugendhilfeakten für Forschungszwecke gut nachvollziehen. Obwohl eine Übermittlung von Sozialdaten der Jugendämter zu Forschungszwecken nicht von vornherein ausge-

76 Dass die Einholung von Einwilligungen mit einem mitunter beträchtlichen Aufwand verbunden sein kann, führt hingegen nicht von vorherein zu einer Unzumutbarkeit.

schlossen ist, sind doch die strengen Vorgaben des SGB zu beachten. Angesichts der besonderen Sensitivität der in den Jugendhilfeakten enthaltenen Daten bedarf es oftmals komplizierter Abwägungen zwischen dem Recht auf informationelle Selbstbestimmung der betroffenen Familien und dem Forschungsinteresse der Wissenschaftlerinnen und Wissenschaftler. Die Praxis zeigt, dass eine möglichst frühzeitige Inanspruchnahme unserer Beratung helfen kann, sachgerechte Ergebnisse zu erzielen.

5.6 Datenschutz und Medienkompetenz

Seit Ende 2016 entwickeln wir Angebote für Kinder, um sie für den Schutz ihrer eigenen Daten in der sich rasant digitalisierenden Welt zu sensibilisieren.[77] In diesem Jahr haben wir unsere Angebote für Kinder weiter optimiert und insbesondere unsere Kinderwebseite www.data-kids.de grundlegend überarbeitet und neu gestaltet. Auch haben wir begonnen, Projekttage in Schulen durchzuführen, um die entwickelten Materialien mit den Grundschulkindern auszuprobieren, Rückmeldungen unserer Zielgruppe einzuholen und auf diese Weise Erkenntnisse für die weitere Entwicklung unserer Angebote zu gewinnen.

Neuere Studien beweisen, dass bereits Kinder im Grundschulalter regelmäßig digitale Medien nutzen. Die Spuren, die sie dabei im Internet und auf den genutzten Geräten hinterlassen, sind ihnen oft gar nicht bewusst. Viele Kinder machen erste Erfahrungen mit Smartphones und Tablets, noch bevor sie flüssig lesen und schreiben können. Oftmals werden Apps und Angebote genutzt, die keineswegs datenschutzgerecht ausgestaltet sind.

Uns ist es ein besonderes Anliegen, die Kinder so früh wie möglich zu sensibilisieren und ihnen Datenschutzkompetenz zu vermitteln. Bei der völligen Neugestaltung unserer Kinderwebseite www.data-kids.de war es unser Ziel, Spiel und Spaß mit dem Lernen zu verbinden. Neben der bereits aus dem bisherigen Angebot bekannten Roboterfamilie, die die Kinder bei allen Themen rund um Technik und Selbstdatenschutz begleitet, haben wir Tierfiguren in einem für die Kinder besonders ansprechenden Manga-Stil entwickelt. Die Tiere vermitteln im Kinderlexikon

77 JB 2017, 6.6; JB 2018, 5.5

die wichtigsten Begriffe rund um das Thema Datenschutz mit interaktiven Karten, Erklär-Videos und vielen bunten Grafiken. Neben den Angeboten für Kinder, wie Spiele und Bastelmaterialien, wollen wir auch Eltern und Lehrkräften nützliche Angebote an die Hand geben. Daher stellen wir neben einer umfangreichen Linksammlung z.B. auch Arbeitshefte zur Verfügung, die heruntergeladen und bei uns auch in Papierform kostenlos bezogen werden können.

Besonders gefreut hat uns, dass wir in diesem Jahr mit unserer Kinderwebseite für den deutschen Kindersoftwarepreis TOMMI nominiert worden sind. Für diesen Preis trifft eine Jury aus Fachleuten aus den Bereichen Medien, Medienpädagogik und Bildungswissenschaften eine Auswahl aus den eingereichten Softwareprodukten, wie z.B. Spiele oder Apps. Diese gibt sie an eine Kinderjury zur endgültigen Abstimmung weiter. Wir haben die Endrunde des diesjährigen Wettbewerbs erreicht. Uns wurde bescheinigt, dass unser Angebot www.data-kids.de als erstes Angebot seiner Art gezielt Kinder im Grundschulalter für den Datenschutz sensibilisiert. Die Nominierung zeigt uns, dass wir den richtigen Weg eingeschlagen haben.

Für das Jahr 2020 haben wir uns vorgenommen, unser Angebot stetig weiterzuentwickeln. Neben neuen Inhalten und Materialien für unsere Kinderwebseite werden wir die an den Schulen durchgeführten Projekte auswerten und Konzepte entwickeln, wie diese noch besser etabliert werden können, um möglichst viele Schulen zu erreichen. Ein Schwerpunkt wird aber auch in der Netzwerkarbeit liegen, um mit weiteren Akteuren aus dem medienpädagogischen Bereich im Land Berlin Kooperationen einzugehen und so die Vermittlung von Datenschutzkompetenz möglichst breit aufzustellen.

6 Gesundheit und Pflege

6.1 Gesundheits-Apps mit unzureichendem Schutz

Die Entwicklung von Gesundheits-Apps stellt einen Tätigkeitsschwerpunkt der digitalen Gesundheitswirtschaft in Berlin dar. Da solche Apps mit sensitiven Daten umgehen, ist es wichtig, dass die Verarbeitung auch in den Cloudsystemen, die hinter den Apps stehen, sicher abläuft. Wir haben uns in einem Beispiel angesehen, wie erfolgreich die Betreiber dabei sind.

Wer den Weg in die Arztpraxis scheut, findet heute eine Reihe von Unterstützungsangeboten im Netz, vielfach in Form von Apps für Smartphones. Die Bundesregierung treibt die Versorgung mit digitalen Gesundheitsangeboten voran und hat insbesondere mit dem Digitale-Versorgung-Gesetz (DVG) die rechtlichen Voraussetzungen für eine Finanzierung dieser Dienste durch die gesetzliche Krankenversicherung geschaffen.

Gesundheits-Apps werden für Beratungs- und für therapeutische Zwecke eingesetzt. In beiden Fällen können sie nur funktionieren, wenn die Nutzenden medizinische Daten in sie eintragen oder diese Daten auf anderem Weg an die Betreiber der Angebote übermitteln. Daraus resultieren hohe Anforderungen an den Schutz von Vertraulichkeit und Integrität der durch die Betreiber verarbeiteten Daten. Einige der Angebote sind zudem als Medizinprodukte einzuordnen und unterliegen damit besonders hohen Anforderungen an die Zuverlässigkeit.

Die als Start-Ups gegründeten kleinen oder mittleren Unternehmen, welche solche Angebote betreiben, nutzen vielfach keine eigene Rechentechnik, sondern Cloud-Angebote großer Anbieter. Diese stellen die Netzwerke zur Verfügung, betreiben die Software und die Datenbanken und bieten zugleich auch Sicherheitsfunktionen. Auch die Anwendungsentwicklung stützt sich weitgehend auf fremdbetriebene Dienste. Aus diesen Entwicklungsumgebungen wird die Software weitgehend automatisiert in die IT-Systeme übernommen, mit denen die Nutzerdaten verarbeitet werden.

Damit greifen die herkömmlichen Maßnahmen zur Gewährleistung von Informationssicherheit nur noch bedingt. Für die Gewährleistung der Sicherheit kommt keine sorgfältig und über längere Zeit geprüfte Hard- und Software zum Einsatz, die nur selten überarbeitet oder ersetzt wird. Es sind nicht mehr Kabelverbindungen, die bestimmen, welche Geräte aus dem Internet ansprechbar und damit angreifbar sind, sondern leicht veränderbare Softwareeinstellungen. Daher müssen die Sicherheitsmaßnahmen an die neue dynamische Umgebung angepasst werden.

Zusätzlich treten neue Risiken auf, die in der Natur der umfassenden Inanspruchnahme von Clouddiensten liegen. Die eigenen Sicherheitsmaßnahmen müssen mit denen der Cloudanbieter so verflochten werden, dass sich das gleiche Sicherheitsniveau ergibt, wie es bei einem Betrieb auf eigener Informationstechnik unter einheitlicher Steuerung möglich wäre. Dies betrifft auch die Kontrolle über den Zugriff auf einzelne Systeme und Dienste. Um nachzuweisen, dass ein Mensch oder eine Software zur Verwendung von Diensten in der Cloud und zum Setzen von Einstellungen berechtigt ist, kommen geheim zu haltende Folgen von Buchstaben, Ziffern und anderen Zeichen, sog. Zugriffsschlüssel, zum Einsatz. Wer auch nur einzelne dieser Schlüssel besitzt, hat die Gewalt über Teile der Informationstechnik des Unternehmens, möglicherweise sogar über das gesamte System. Geht die Kontrolle über die Schlüssel verloren, ist dem Missbrauch Tür und Tor geöffnet.

Uns hat interessiert, inwieweit Unternehmen mit den Herausforderungen adäquat umgehen, die aus ihrer Entscheidung resultieren, vollständig in die Cloud zu wechseln. Das Datenschutzrecht verpflichtet sie dazu, den Aufsichtsbehörden nachzuweisen, dass sie Vertraulichkeit und Integrität der ihnen anvertrauten Daten gewährleisten können.

Das Ergebnis der von uns durchgeführten Prüfung eines Unternehmens mit einer beeindruckend großen Zahl von Nutzenden war nicht zufriedenstellend. Es wurde uns dabei zwar durchaus dargestellt, dass eine ganze Reihe sinnvoller Einzelmaßnahmen ergriffen wurden. Doch fügten sich diese nicht zu einem Gesamtkonzept zusammen, mit dem die Risiken auf ein adäquates Maß hätten reduziert werden können. Zu beschränkt war der Blickwinkel des Unternehmens auf gängige Methoden für Cyberangriffe, denen seine Informationstechnik ausgesetzt ist. Nicht berücksichtigt wurden hingegen z.B. das mögliche Abgreifen von Zugangsinfor-

mationen auf den Computern der Entwicklerinnen und Entwickler sowie an weiteren Speicherorten oder die mögliche Manipulation von Daten, die den Diensten zur Verarbeitung übergeben werden, oder auch die Ableitung von sicherheitskritischen Informationen aus dem beobachtbaren Verhalten der Dienste und Systeme. Die vollständige Betrachtung möglicher Gefährdungen ist jedoch angesichts möglicherweise weitreichender Folgen unverzichtbar, weil eine unvollständige Risikoanalyse in der Regel auch ein unvollständiges Spektrum an Sicherheitsmaßnahmen zur Folge hat.

Wir werden, soweit erforderlich, unsere Abhilfebefugnisse einsetzen, um das geprüfte Unternehmen zu einer risikogerechten Ausgestaltung seines Dienstes zu bewegen. Gleichzeitig werden wir im Rahmen unserer Kapazitäten Betreiber elektronischer Gesundheitsdienste verstärkt in unser Prüfprogramm einbeziehen. Einige Risiken sind bei der Nutzung elektronischer Gesundheitsdienste schon deswegen unausweichlich, weil viele Privatpersonen nicht mit Smartphones ausgerüstet sind, die ein adäquates Sicherheitsniveau garantieren. Davon abgesehen darf aber jede Person erwarten, dass ihr bei der Verarbeitung ihrer Gesundheitsdaten, ob bei den Leistungserbringern, der informationstechnischen Infrastruktur im Gesundheitswesen, den Leistungsträgern und eben auch bei den privaten nichtärztlichen Anbietern von Gesundheitsdienstleistungen ein einheitlich hohes Sicherheitsniveau geboten wird.

Wer elektronische Gesundheitsdienstleistungen anbietet, ist zu einem zuverlässigen Schutz von Vertraulichkeit und Integrität der verarbeiteten Daten verpflichtet. Sollen neuartige Herangehensweisen – bspw. die kontinuierliche Entwicklung und der Betrieb in der Cloud – zur Bereitstellung der Dienstleistungen für eine Vielzahl von Personen eingesetzt werden, ist in der Datenschutz-Folgenabschätzung vorab eine gründliche Analyse der mit diesen Herangehensweisen verbundenen Risiken und die Bestimmung von Gegenmaßnahmen erforderlich.

6.2 Offene Patientenakten im Krankenhaus

Wir haben geprüft, ob die beiden großen Krankenhaus-Betreiberinnen in Berlin, die Charité und die Vivantes Netzwerk für Gesundheit GmbH, so mit gespeicherten Angaben über die Behandlung bereits entlassener Patientinnen und Patienten umgehen, wie es gesetzlich vorgeschrieben ist, insbesondere, ob sie den Zugriff auf die Daten spätestens ein Jahr nach Abschluss der Behandlung sperren und diese nach Ablauf der Aufbewahrungsfrist löschen.

Krankenhäuser haben die Verpflichtung, medizinische Behandlungen zu dokumentieren. Hierbei werden völlig legitim große Mengen sensitiver Daten gespeichert. Diese müssen über einen gesetzlich vorgegebenen Zeitraum zwischen zehn und dreißig Jahren gespeichert bleiben. Innerhalb dieses Zeitraums sollen Zugriffe auf die Daten nach Abschluss der jeweiligen Behandlung nur noch möglich sein, wenn es dafür einen besonderen Bedarf gibt. Dementsprechend müssen die Zugriffsberechtigungen in dieser Zeitspanne stark eingeschränkt werden. Nach Ablauf der Fristen hingegen ist auch eine weitere Aufbewahrung nur noch zulässig, wenn es einen besonderen Grund dafür gibt.

In beiden geprüften Krankenhäusern mussten wir feststellen, dass diese Anforderungen nicht erfüllt werden. In der Charité blieben Patientendaten auch nach Entlassung und Abrechnung der Behandlung auf Dauer im Zugriff der überwiegenden Mehrzahl der Beschäftigten, was eine grobe Verletzung der gesetzlichen Vorgaben darstellt. Vivantes schränkte den Zugriff deutlich stärker ein. Die Zugriffsmöglichkeiten waren von vornherein an den Bedürfnissen der Behandlung ausgerichtet. Zudem wurden sie nach dem Ende der Behandlung in den meisten Fällen zeitlich beschränkt. Doch griff diese Beschränkung nicht durchgehend und trat in einigen Fällen zu spät ein.

Mit der gesetzlichen Vorgabe konfrontiert, haben beide Häuser unverzüglich Maßnahmen eingeleitet, um die Defizite abzustellen. Die Charité legte einen ambitionierten Plan mit Maßnahmen zur Ertüchtigung oder Auswechslung der geprüften technischen Systeme und Einrichtung der zeitlich definierten Zugriffsbeschränkungen vor. Bereits wenige Monate nach der Prüfung konnte sie vermelden, dass in einem der geprüften Systeme der Schutz der Patientendaten gegen einen un-

begründeten Zugriff nunmehr den gesetzlichen Ansprüchen entspricht. Vivantes handelte ebenfalls schnell und legte einen Plan vor, mit dem die existierenden Zugriffsmöglichkeiten justiert und Lücken geschlossen werden sollen.

Bei Daten aus der ambulanten Behandlung haben wir geprüft, ob sie nach Ablauf der Aufbewahrungsfrist von regelmäßig zehn Jahren gelöscht werden.[78] Dabei fanden wir Defizite in beiden Häusern vor. Diese müssen jetzt durch eine nachholende Löschung und die Einrichtung regelmäßiger Löschroutinen aufgearbeitet werden. Den Häusern bleibt es dabei unbenommen, Patientinnen und Patienten, die dies wünschen, auch eine längere Aufbewahrung anzubieten.

Wir werden die Mängelbeseitigung bei Charité und Vivantes im Weiteren eng verfolgen und, sollten sich wider Erwarten inakzeptable Verzögerungen ergeben, von unseren Abhilfebefugnissen Gebrauch machen.

Krankenhäuser müssen dafür sorgen, dass die Daten von Patientinnen und Patienten, die bereits entlassen wurden, nur einem eng umrissenen Personenkreis für genau definierte Zwecke zur Verfügung stehen und nach dem Ende der Aufbewahrungsfrist gelöscht werden.

6.3 Terminierung mit mehreren Unbekannten?

Eine Verbesserung der Terminverwaltung von Arztpraxen kann der Verbesserung der Gesundheitsvorsorge dienen und ist daher zu begrüßen. Allerdings ist es zwingend notwendig, dass die Verarbeitung der Patientendaten dabei für die Patientinnen und Patienten transparent bleibt und zusätzliche Dienste, wie Terminerinnerungen per SMS oder E-Mail, nur mit Einwilligung der Patientinnen und Patienten erfolgen.

2019 erreichten uns wiederholt Beschwerden von Bürgerinnen und Bürgern, die über SMS oder E-Mail an Arzttermine erinnert wurden, ohne dass sie darin einge-

78 Daten aus der stationären Behandlung sind dagegen in der Regel dreißig Jahre aufzubewahren; keines der geprüften Systeme enthielt jedoch Daten aus Behandlungen, die so weit zurückliegen.

willigt hatten. Absender dieser Nachrichten war ein Berliner Unternehmen, das die Terminerinnerung für Patientinnen und Patienten als Dienstleister für Arztpraxen durchführt.

Die Terminerinnerung war in einem konkreten Einzelfall als eine zusätzliche Dienstleistung für den Arzt ausgestaltet, die neben der Übernahme der gesamten Terminverwaltung angeboten wurde. Erst durch den Erhalt der Erinnerung wurden die Betroffenen auf die vom Arzt ausgelagerte Terminverwaltung und den dahinterstehenden Dienstleister aufmerksam.

Gewünschtes Ziel der zusätzlichen Terminerinnerungen ist die Optimierung der Arbeitsabläufe in der Praxis. Durch die Erinnerungen soll die Anzahl der Termine, die ausfallen, weil die Patientinnen und Patienten einen Termin vergessen, deutlich reduziert werden.

Zusätzlich bietet das Unternehmen durch die Kenntnis der noch freien Zeiten bei den Ärztinnen und Ärzten den Patientinnen und Patienten die Möglichkeit, über eine Internetseite direkt Termine zu buchen.

Patientinnen und Patienten, die selbst über ein Benutzerkonto auf der Internetseite verfügen, wählen die Erinnerungsfunktion aktiv aus. Wenn dies jedoch nicht der Fall ist, ein Termin vielmehr telefonisch oder direkt in der Praxis vereinbart wird und nicht vom Praxispersonal auf die Erinnerungsfunktion hingewiesen wird, werden die Patientinnen und Patienten von einer derartigen Nachricht überrascht. Besonders kritisch ist ein solches Terminerinnerungssystem insbesondere deshalb, weil darin Daten enthalten sein können, die sehr sensitiv sind. So kann eine Terminerinnerung bei Ärztinnen oder Ärzten bestimmter Fachrichtungen Hinweise auf den Gesundheitszustand der Patientin oder des Patienten geben.

Eine rechtlich zulässige Ausgestaltung einer ausgelagerten Terminverwaltung von Arztpraxen ist grundsätzlich durchaus möglich. Dies setzt allerdings voraus, dass die Ärztinnen und Ärzte die jeweiligen Dienstleister im Rahmen der Beauftragung zur Geheimhaltung verpflichten. Soweit dies erfüllt ist, unterliegt ein Dienstleister dann selbst der gesetzlichen Schweigepflicht.[79]

79 Siehe § 203 Abs. 4 Strafgesetzbuch (StGB)

Nach der DS-GVO dürfen von einer Arztpraxis die Daten der Patientinnen und Patienten verarbeitet werden, die zur Erfüllung des jeweiligen Behandlungsvertrags erforderlich sind.[80] Für die über die Terminverwaltung hinausgehende Terminerinnerung bedarf es allerdings einer Einwilligung durch die Patientinnen und Patienten, da die Erinnerung an den Termin nicht zur Durchführung der Behandlung selbst erforderlich ist und insoweit nicht aufgrund einer gesetzlichen Verarbeitungsbefugnis erfolgen kann. Verantwortlich für das Einholen dieser Einwilligung ist dabei die Stelle, bei der der Termin vereinbart wird. Werden Termine über die Internetseite des Dienstleisters gebucht, muss dieser die Nutzenden um Einwilligung bitten. Wird der Termin durch das Personal der Arztpraxis vereinbart, sind die Praxen dafür verantwortlich. Dienstleister von Arztpraxen stehen allerdings in der Pflicht, die Praxen über das Erfordernis einer Einwilligung zu informieren.

Wenn Ärztinnen und Ärzte einen Dienstleister mit der Terminverwaltung für ihre Praxis beauftragen, müssen sie dies ihren Patientinnen und Patienten gegenüber transparent machen. Gerade wenn es um Gesundheitsdaten geht, ist es besonders wichtig, dass den Betroffenen bewusst ist, durch welche Stellen ihre Daten verarbeitet werden. Anbieter solcher Dienstleistungen sollten den Ärztinnen und Ärzten die Einhaltung ihrer gesetzlichen Pflichten so einfach wie möglich machen. Dazu gehört auch, dass sie unmissverständlich auf diese Pflichten hingewiesen werden.

6.4 Lösung eines alten Streits? Qualitätssicherung bei der Kassenärztlichen Vereinigung Berlin

Im letzten Jahresbericht haben wir über das Urteil des Landessozialgerichts Berlin-Brandenburg zum Qualitätssicherungsverfahren der Kassenärztlichen Vereinigung Berlin (KV) berichtet.[81] Durch dieses wurden wir in unserer Rechtsauffassung bestätigt, dass bei der Qualitätssicherung durch die KV Patientendaten nur in pseudonymisierter Form erhoben werden dürfen.

80 Siehe Art. 6 Abs. 1 lit. b i. V. m. Art. 9 Abs. 2 lit. h DS-GVO

81 JB 2018, 6.1

Mit Wirkung zum 1. Juli 2019 hat der Gemeinsame Bundesausschuss (GBA) aufgrund seiner sich aus dem Sozialgesetzbuch (SGB) ergebenden Richtlinienkompetenz[82] die „Qualitätsprüfungsrichtlinie vertragsärztliche Versorgung" aufgehoben und neu gefasst. Die Richtlinie des GBA ist sowohl für die KV als auch für die Versicherten und Vertragsärztinnen und -ärzte bindendes Satzungsrecht. Die Richtlinie des GBA sieht nunmehr explizit die Einreichung von Behandlungsdokumentationen in nicht pseudonymisierter Form in allen Fällen der Qualitätssicherung vor.

Diese Änderung der rechtlichen Ausgangslage führt dazu, dass wir gegenüber der KV die Durchführung der Qualitätssicherung mit identifizierenden Daten nunmehr für zulässig zu bewerten hatten.

Wir haben jedoch erhebliche Zweifel, ob die erlassene Richtlinie einer gerichtlichen Überprüfung standhalten würde. So sieht die Richtlinienermächtigung des § 299 SGB V ausdrücklich vor, dass die Datenerhebung in der Regel auf eine Stichprobe der betroffenen Patientinnen und Patienten begrenzt wird und die versichertenbezogenen Daten pseudonymisiert werden. Lediglich in Ausnahmefällen, wenn bspw. die Richtigkeit der Behandlungsdokumentation Gegenstand der Qualitätsprüfung ist, können identifizierende Daten erhoben werden.

Der GBA hat in der Richtlinie festgelegt, dass bei allen Qualitätsprüfungen, für die die Richtlinie Anwendung findet, die Richtigkeit der Behandlungsdokumentation Gegenstand der Prüfung ist.

Durch diese Festlegung wird das in § 299 SGB V vorgegebene Regel-Ausnahmeverhältnis nicht nur umgekehrt, sondern sogar ignoriert, da vorgesehen ist, in allen Fällen identifizierende Daten der Patientinnen und Patienten zu erheben.

Durch die Anpassung der Richtlinie zur Qualitätssicherung durch den GBA wurde eine Regelung getroffen, die sowohl für die KV, als auch für die betroffenen Ärztinnen und Ärzte verbindlich ist. Inwieweit diese Richtlinie einer gerichtlichen Überprüfung standhalten würde, ist sehr zweifelhaft, da die durch

82 Siehe § 299 SGB V

den Bundesgesetzgeber festgelegte Maßgabe, dass die Datenerhebung „in der Regel" mit pseudonymisierten Daten zu erfolgen hat, durch die Richtlinie umgangen wird.

6.5 Ohne Moos nichts los? – Der Anspruch auf die Patientenakte in Kopie

Im vergangenen Jahr sind wir von Ärztinnen und Ärzten mehrfach mit der Frage konfrontiert worden, ob sie Patientinnen und Patienten, die eine Kopie ihrer Patientenakte verlangen, auch nach dem Wirksamwerden der DS-GVO weiterhin die entstandenen Kosten in Rechnung stellen dürfen.

Zum Hintergrund: Bereits seit dem Jahr 2013 räumt das Bürgerliche Gesetzbuch (BGB) Patientinnen und Patienten explizit das Recht ein, auf Wunsch eine Kopie ihrer Patientenakte zu erhalten. Voraussetzung ist, dass sie hierfür die Kosten tragen.[83] Auch die Berufsordnung sieht vor, dass Ärztinnen und Ärzte berufsrechtlich nur dann zur Herausgabe von Kopien verpflichtet sind, wenn ihnen die Kosten erstattet werden.[84] Mit anderen Worten: Zumindest in der Vergangenheit war die Rechtslage eindeutig.

Doch wie sieht es nun seit dem 25. Mai 2018 aus? Die Regelungen im BGB und in der Berufsordnung haben sich zwar nicht geändert. Mit Art. 15 Abs. 3 DS-GVO ist jedoch eine Vorschrift hinzugekommen, die einen ähnlichen Regelungsgehalt aufweist. Konkret sieht diese Regelung vor, dass jeder Verantwortliche – und dazu zählen selbstverständlich auch Ärztinnen und Ärzte – den betroffenen Personen auf Verlangen eine Kopie ihrer personenbezogenen Daten zur Verfügung stellen muss. Allerdings steht diese Vorschrift im Widerspruch zum BGB: Einen Anspruch auf ein angemessenes Entgelt räumt die DS-GVO den Verantwortlichen nämlich ausdrücklich nur für „alle weiteren Kopien" ein – die erste Kopie ist hingegen stets kostenlos herauszugeben.

83 § 630g Abs. 2 Satz 2 BGB

84 § 10 Abs. 2 Satz 2 Berufsordnung der Ärztekammer Berlin

Wie also umgehen mit diesem Widerspruch?

Unsere Antwort: Das europäische Recht geht dem deutschen Recht vor. Die Kostentragungspflicht der Patientinnen und Patienten kann jedenfalls dann nicht aufrechterhalten werden, wenn die Patientinnen und Patienten erstmals eine Kopie ihrer personenbezogenen Daten anfordern.

Zwar erlaubt die DS-GVO unter bestimmten Voraussetzungen grundsätzlich die Einschränkung der Betroffenenrechte, zu denen auch das Auskunftsrecht bzw. das „Recht auf Kopie" zählt, durch mitgliedsstaatliche Rechtsvorschriften. Die Beschränkung muss jedoch aufgrund in der DS-GVO näher beschriebener gesellschaftlich übergeordneter Interessen erforderlich und zugleich verhältnismäßig sein.[85] Diese Voraussetzungen liegen hier aber nicht vor. Insbesondere stellt die Kostentragungspflicht nach dem BGB keine notwendige Maßnahme zum Schutz der Rechte und Freiheiten der Ärztinnen und Ärzte dar. Dass die Erfüllung von Betroffenenrechten für Verantwortliche mitunter auch Kosten verursacht, ist für sich noch kein Grund, eine Verletzung ihrer Rechte anzunehmen.[86]

Dass sich die DS-GVO nicht an allen Stellen reibungslos in das mitgliedsstaatliche Recht einfügt und es mitunter zu Rechtsunsicherheiten kommen kann, verwundert nicht. Letztendlich ist hier aber der Bundesgesetzgeber gefragt, durch eine Anpassung des BGB wieder für einen Gleichklang zu sorgen. Bis dahin dürften Ärztinnen und Ärzte gut beraten sein, die Aushändigung der Patientenakte in Kopie bei erstmaliger Anfrage der Patientinnen und Patienten nicht von einer Kostenübernahme abhängig zu machen.

6.6 Informierte Einwilligung bei Forschungsvorhaben – Kein Auslaufmodell!

Im Bereich der Forschung werden wir in unserer Beratungspraxis immer wieder mit Einwilligungserklärungen konfrontiert, die zwar mit bestem Wissen und Gewissen verfasst wurden, inhaltlich aber nicht den Anforderungen an eine in-

85 Art. 23 Abs. 1 DS-GVO

86 Auf Art. 15 Abs. 4 DS-GVO kann die Einschränkung des § 630g Abs. 2 Satz 2 BGB wiederum nicht gestützt werden – bei dieser Vorschrift handelt es sich schon nicht um eine Öffnungsklausel für den mitgliedsstaatlichen Gesetzgeber.

formierte Einwilligung entsprechen. Festzustellen ist, dass die für konkret festgelegte Zwecke eingeholte Einwilligung im Forschungsbereich auch nach Wirksamwerden der DS-GVO weiterhin der Regelfall bleibt.

Dabei ist die Verarbeitung von personenbezogenen Daten auf der Grundlage einer Einwilligung der betroffenen Personen nur dann möglich, wenn diese Erklärung strenge Voraussetzungen erfüllt. Sie muss freiwillig und – bezogen auf einen bestimmten Fall – in informierter Art und Weise abgegeben worden sein.[87] Zudem sind die betroffenen Personen darauf hinzuweisen, dass sie ihre Einwilligung jederzeit widerrufen können und dass durch den Widerruf die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung nicht berührt wird.[88] Ist beabsichtigt, auch besondere Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) zu verarbeiten, muss sich die Erklärung ausdrücklich auch auf diese Angaben beziehen.[89] Die Einhaltung der Schriftform hingegen ist gesetzlich nicht (mehr) vorgeschrieben. Es reicht eine unmissverständliche Willensbekundung in Form einer eindeutig bestätigenden Handlung (z.B. aktiver Mausklick auf den Button „Einverstanden"). Natürlich bleibt die Schriftform zulässig und u. U. auch sinnvoll.

Um einerseits die notwendige Informiertheit der betroffenen Personen sicherzustellen und andererseits die eigentliche Einwilligungserklärung nicht zu überfrachten, hat es sich bei Forschungsvorhaben in der Praxis bewährt, den betroffenen Personen zusätzlich zur eigentlichen Einwilligungserklärung einen gesonderten Informationstext zur Verfügung zu stellen. Die betroffenen Personen sollen in einer klaren und einfachen Sprache[90] über das jeweilige Forschungsprojekt und die damit verbundenen Datenverarbeitungen aufgeklärt werden. So sollen sie überhaupt erst in die Lage versetzt werden, entscheiden zu können, ob sie mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten einverstanden sind. Diese Information ist damit essentiell für die Wirksamkeit einer Einwilligung.

87 Art. 4 Nr. 11 DS-GVO
88 Art. 7 Abs. 3 DS-GVO
89 Art. 9 Abs. 2 lit. a DS-GVO
90 Siehe EG 42 DS-GVO

Hiervon zu unterscheiden sind die allgemeinen Informationspflichten[91] aus der DS-GVO, die grundsätzlich jeden Verantwortlichen treffen – und zwar unabhängig davon, ob dieser personenbezogene Daten auf Grundlage einer Einwilligung oder einer Rechtsvorschrift verarbeitet. Diese Pflichtangaben überschneiden sich zwar inhaltlich mit denjenigen Informationen, die erforderlich sind, um von einer „informierten Einwilligung" ausgehen zu können (z.B. Angabe des Verantwortlichen und der Zwecke der Datenverarbeitung). Sie sind aber nicht gänzlich deckungsgleich. Unsere Erfahrungen zeigen, dass diese Unterscheidung in der Praxis oftmals zu Unklarheiten in der Abgrenzung führt.

Doch woran genau hapert es nun in der Praxis? – Aus unserer Erfahrung geht es hier im Wesentlichen um zwei Aspekte:

Zum einen müssen wir immer wieder feststellen, dass die uns vorgelegten Erklärungen bzw. Informationsschreiben die beabsichtigten Datenverarbeitungen nicht ausreichend oder sogar unzutreffend wiedergeben. Ein „Klassiker" ist hier etwa der unrichtige Hinweis, die Verarbeitung erfolge „anonym", obwohl tatsächlich eine Verarbeitung in pseudonymisierter und damit personenbezogener Form[92] erfolgt. Zum anderen ist es aber auch immer wieder die verwendete Sprache selbst. So wird von den Projektverantwortlichen häufig nicht berücksichtigt, an welche Zielgruppe sich die Informationen richten. Bspw. gehören Fachausdrücke nicht in ein Informationsschreiben. Diese sind einfach und allgemein verständlich zu formulieren und sollten sich im Übrigen auch auf eine zumutbare Länge beschränken.

Werden diese Vorgaben nicht beachtet, können sich die Studienteilnehmerinnen und -teilnehmer auch kein umfassendes Bild von der Tragweite ihrer Erklärung machen. Dies geht zulasten der informationellen Selbstbestimmung.

Ein Abrücken vom Prinzip der für konkret festgelegte Zwecke eingeholten Einwilligung ist auch nach dem Wirksamwerden der DS-GVO keineswegs angezeigt. Zwar hat die wissenschaftliche Forschung an vielen Stellen der DS-GVO Erleichterun-

91 Siehe Art. 13, 14 DS-GVO

92 Das ist z.B. der Fall, wenn – wie häufig – die Namen der Teilnehmerinnen und Teilnehmer durch eine Identifikationsnummer ersetzt werden und eine Liste, die die Zuordnung zwischen Namen und Nummern ermöglicht, nach wie vor existiert.

gen erfahren,[93] das heißt aber nicht, dass Forschende zukünftig nicht mehr die konkreten Zwecke der Datenverarbeitung festlegen müssen, wenn sie die Teilnehmerinnen und Teilnehmer um ihre Einwilligung bitten. Die DS-GVO weist in ihren Erwägungsgründen[94] darauf hin, dass es den betroffenen Personen erlaubt sein sollte, ihre Einwilligung für „bestimmte Bereiche wissenschaftlicher Forschung" zu geben. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat inzwischen klargestellt, dass nur im Einzelfall und auch nur dann, wenn die konkrete Gestaltung des Forschungsvorhabens absehbar bis zum Zeitpunkt der Datenerhebung eine vollständige Zweckbestimmung schlechthin nicht zulässt, die Erklärung in diesem Punkt etwas „offener" bzw. „breiter" gestaltet werden kann.[95] Voraussetzung ist aber u. a., dass spezifische Sicherungsmaßnahmen eingehalten werden.[96]

Die informierte Einwilligung ist nach wie vor der Normalfall. Ein Abrücken von dem Prinzip der eindeutigen Zweckbestimmung im Bereich der wissenschaftlichen Forschung ist auch in Zeiten der DS-GVO nur in seltenen Einzelfällen und auch nur dann möglich, wenn konkrete Ausgleichsmaßnahmen vorgesehen sind.

93 Z.B. hat der Verordnungsgeber den Mitgliedsstaaten durch Art. 89 Abs. 2 DS-GVO die Möglichkeit eingeräumt, die Betroffenenrechte unter bestimmten Bedingungen einzuschränken, wenn die Datenverarbeitung zu Zwecken der wissenschaftlichen Forschung erfolgt. Hiervon hat der deutsche Gesetzgeber mit § 27 Abs. 2 Bundesdatenschutzgesetz (BDSG) Gebrauch gemacht. Auch besteht mit Art. 14 Abs. 5 lit. b DS-GVO bspw. eine gesetzliche Ausnahmemöglichkeit von den Informationspflichten bei sog. „Dritterhebungen".

94 EG 33 DS-GVO

95 Siehe Beschluss der 97. DSK zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO vom 3. April 2019

96 Z.B. Verwendung einer für die Einwilligenden einsehbaren Nutzungsordnung und Einrichtung einer Internetpräsenz, durch die die Studienteilnehmer und -teilnehmerinnen über laufende und künftige Studien informiert werden

7 Integration, Soziales und Arbeit

7.1 Beschwerdestelle für geflüchtete Menschen – Ohne Datenschutz?

Aus der Praxis

Im Rahmen von Beratungen des Landesamts für Flüchtlingsangelegenheiten (LAF) hat dieses uns darüber informiert, dass die Senatsverwaltung für Integration, Arbeit und Soziales plane, eine vom LAF unabhängige Beschwerdestelle für geflüchtete Menschen zu schaffen, die „niedrigschwellig" Beschwerden über die Einrichtungen und über Vorgänge im Zusammenhang mit der Unterbringung entgegennehmen solle. Angesichts der dabei zu erwartenden umfangreichen Verarbeitung personenbezogener Daten über die Geflüchteten bat uns das LAF um datenschutzrechtliche Beratung.

Der Plan ist, neben dem in Berlin bereits existierenden behörden- bzw. wohnheiminternen Beschwerdesystem eine zusätzliche Beschwerdestelle zu schaffen, die außerhalb von Unterkünften und Behörden unabhängig betrieben werden soll als neutrale und niedrigschwellige Anlaufstelle für Betroffene. Zum einen soll diese Beschwerdestelle Sprechstunden anbieten und zum anderen durch sog. Integrationslotsen direkt in den Einrichtungen Beratung anbieten.

Da noch wesentliche Fragen zur Einrichtung und insbesondere zur Rechtsnatur der geplanten Beschwerdestelle offen waren, haben wir das LAF zunächst auf die rechtliche Problematik der Verarbeitung personenbezogener Daten durch private Dritte im Rahmen der Wahrnehmung staatlicher Aufgaben hingewiesen und diese Bedenken auch auf Leitungsebene gegenüber der Senatorin für Arbeit, Integration und Soziales formuliert. Insbesondere haben wir problematisiert, dass es sich bei der Qualitätssicherung um eine staatliche Aufgabe handelt, die auch nur von einer staatlichen Stelle wie dem LAF wahrgenommen werden kann. Die Aufgabe könne nicht ohne Weiteres auf einen privaten Dritten wie die geplante Beschwerdestelle übertragen werden. Wir haben mehrfach darum gebeten, uns nähere Informationen zur rechtlichen Einordnung der Beschwerdestelle zukom-

men zu lassen. Leider haben wir die erwünschten Informationen von der Senatsverwaltung jedoch nicht bekommen. Nach mehreren Monaten kam es im Herbst zu einem persönlichen Gespräch auf fachlicher Ebene unter Beteiligung der Koordinierungsstelle Flüchtlingsmanagement der Senatsverwaltung und dem LAF.

Wir haben dabei deutlich gemacht, dass wir den von der Senatsverwaltung mit der Einrichtung der Beschwerdestelle verfolgten Ansatz, die Hemmschwelle für die Bewohnerinnen und Bewohner der Einrichtungen, sich mit einer Beschwerde an eine staatliche Institution zu wenden, so weit wie möglich herabzusetzen, sehr gut nachvollziehen können. Auch konnten wir die mit der geplanten Konstruktion der Beschwerdestelle verbundenen datenschutzrechtlichen Schwierigkeiten verdeutlichen. Vonseiten der Senatsverwaltung wurde uns demgegenüber jedoch mitgeteilt, dass die Schaffung einer behördenunabhängigen Beschwerdestelle beabsichtigt sei, ohne die bestehenden gesetzlichen Weisungsverhältnisse und Zuständigkeiten anzutasten. Es sei daher auch gerade nicht geplant, die Aufgaben der Beschwerdestelle gesetzlich zu verankern. Den Einsatz der Beschwerdestelle habe die Senatsverwaltung seit 2018 bereits in einem Pilotprojekt, in das unsere Behörde jedoch nicht einbezogen war, erprobt. Die daraus gewonnenen Erkenntnisse sollten genutzt werden, um im Jahr 2020 die Beschwerdestelle nunmehr dauerhaft zu etablieren.

Wir haben erläutert, dass mangels einer gesetzlichen Aufgabenzuweisung für die Beschwerdestelle auch die Verarbeitung personenbezogener Daten der Bewohnerinnen und Bewohner nicht auf Datenschutzvorschriften gestützt werden kann, sondern lediglich auf Einwilligungen. Da eine Einwilligungserklärung jedoch nur dann wirksam ist, wenn in ihr sämtliche Datenverarbeitungsprozesse genau benannt werden, entstehen vielfältige praktische Probleme.

Insbesondere sind praktische Probleme dann zu erwarten, wenn Rückmeldungen aus einem gesetzlich vorgesehenen Beschwerdeverfahren, z.B. beim LAF oder im Zusammenhang mit Widerspruchsverfahren bei den bezirklichen Sozialämtern, an die unabhängige Beschwerdestelle erfolgen sollen. Bei Beschwerden über Dritte, bspw. hinsichtlich etwaiger Übergriffe durch Mitbewohnerinnen oder Mitbewohner oder auch das Personal der Einrichtungen bzw. durch Sicherheitsdienste, könnten deren Daten nicht auf der Grundlage von Einwilligungen der Beschwerdeführenden verarbeitet werden. Die unabhängige Beschwerdestelle

könnte dann nicht tätig werden, sondern müsste an die staatlichen Stellen verweisen.

Darauf haben wir hingewiesen und empfohlen, die Aufgaben der Beschwerdestelle perspektivisch doch gesetzlich zu verankern. Konkrete Vorschläge hierzu haben wir ebenfalls unterbreitet. Diese haben wir mit den Beteiligten intensiv diskutiert.

Da der politische Wille besteht, die Beschwerdestelle mittelfristig auch für Beschwerden wohnungsloser Menschen zu öffnen, sollte frühzeitig geprüft werden, wie eine gesetzliche Verankerung dieser Stelle umsetzbar wäre. Die Einwilligungslösung sollte aus unserer Sicht lediglich angesichts des hohen Zeitdrucks für den Start der Beschwerdestelle als Übergangslösung in Betracht gezogen werden.

Die Senatsverwaltung für Integration, Arbeit und Soziales und das LAF wird die geplanten Aufgaben der unabhängigen Beschwerdestelle anhand der erörterten Aspekte überprüfen. Wir gehen davon aus, dass uns die noch zu entwickelnden Einwilligungserklärungen zur Prüfung vorgelegt werden. Die Angelegenheit zeigt, dass bei einer frühzeitigen Einbindung unserer Behörde die datenschutzrechtlichen Anforderungen an die Einrichtung der Beschwerdestelle von vornherein hätten Berücksichtigung finden können, ohne dass wertvolle Zeit verstrichen wäre. Wir gehen aber davon aus, dass der begonnene konstruktive Austausch fortgesetzt wird und werden die Etablierung der Beschwerdestelle weiterhin beratend begleiten.

7.2 Zählung wohnungsloser Menschen in Berlin – „Nacht der Solidarität“

Aus der Praxis

Zu Beginn des Jahres trat die Senatsverwaltung für Integration, Arbeit und Soziales mit der Bitte um Beratung hinsichtlich eines Projekts zur Zählung wohnungsloser Menschen an uns heran. Da aus den uns übermittelten Unterlagen der konkrete Ablauf des Vorhabens nicht ersichtlich wurde, haben wir der Senatsverwaltung zunächst Gespräche auf fachlicher Ebene angeboten, um offene Fragen zu klären und das Projekt von Beginn an zu begleiten. Im Rahmen eines

Treffens im Mai haben wir die datenschutzrechtlichen Aspekte des Vorhabens besprochen und gebeten, unsere Hinweise in der weiteren Projektplanung zu berücksichtigen sowie uns zeitnah die für unsere Bewertung notwendigen Unterlagen zuzuleiten. Im Nachgang zu diesem Gespräch wurde uns das notwendige Datenschutzkonzept jedoch leider nicht vorgelegt. Erst im Oktober und nachdem die Senatsverwaltung eine ganz neue Projektgruppe eingesetzt hatte, wandte sie sich mit der Bitte um ein erneutes Treffen an uns. Nach diesen Startschwierigkeiten konnten die zu berücksichtigenden Datenschutzaspekte dann aber auf Fachebene konstruktiv erörtert werden.

Da dem Berliner Senat lediglich Schätzungen zur aktuellen Anzahl der auf der Straße lebenden Menschen vorliegen, sollen diese künftig regelmäßig mithilfe von Ehrenamtlichen im gesamten Stadtgebiet in jeweils einer Nacht gezählt werden. Eine erstmalige Zählung ist für die Nacht vom 29. auf den 30. Januar 2020 geplant. Hintergrund der Zählung ist, dass obdachlose Menschen vom bestehenden Hilfesystem bisher nur ungenügend erreicht werden. Anhand der festgestellten Wohnungsnotfälle soll eine qualifizierte Planung der Hilfsangebote für wohnungslose Menschen ermöglicht werden.

Zusätzlich zu der Zählung möchte die Senatsverwaltung von den auf der Straße angetroffenen Menschen auch Daten erheben. Geplant ist, dass die wohnungslosen Menschen von den bei der Zählung mitwirkenden Helferinnen und Helfern einen Fragebogen in ihrer jeweiligen Muttersprache ausgehändigt bekommen. Die Teilnahme soll freiwillig sein. Anhand des Fragebogens werden von den wohnungslosen Menschen dann Angaben zum Geschlecht, zum Alter, zur Nationalität, zur Dauer der Wohnungslosigkeit sowie ggf. zum Familienstand abgefragt. Diese sog. Erhebungsmerkmale sind – soweit dies möglich ist – weit gefasst bzw. in Kategorien eingeteilt. So sollen bei der Angabe des Alters die Antwortmöglichkeiten auf Altersgruppen (z.B. „21 bis unter 25") und bei der Nationalität auf die Kategorien „Deutsch", „sonstige EU" und „andere" beschränkt sein. Namen und Geburtsdaten werden nicht erfragt.

Die bloße Zählung wohnungsloser Menschen auf der Straße ist datenschutzrechtlich unproblematisch, da hierbei keine personenbezogenen Daten verarbeitet werden. Bei der Verarbeitung der Daten aus dem Fragebogen muss die Senatsverwaltung jedoch dafür Sorge tragen, dass eine Identifizierung der einzelnen be-

fragten Personen im Nachhinein nicht möglich ist. Dies ist zwar bereits dadurch erschwert, dass weder Name noch Geburtsdatum verarbeitet werden. Aber auch die anderen Informationen dürfen keine Rückschlüsse auf die jeweiligen wohnungslosen Menschen ermöglichen. Ferner müssen die befragten Personen spätestens vor der Befragung über die damit zusammenhängenden Datenverarbeitungen und die Freiwilligkeit der Teilnahme informiert werden.

Das geplante Vorhaben der Zählung und Befragung wohnungsloser Menschen in Berlin ist ein unterstützenswertes Anliegen des Senats im Hinblick auf die Verbesserung der persönlichen Situation der betroffenen Personen und zur Bekämpfung der Wohnungslosigkeit in Berlin. Dennoch müssen datenschutzrechtliche Aspekte bei der Durchführung berücksichtigt werden. Wir werden das Projekt daher weiter begleiten, um sicherzustellen, dass die personenbezogenen Daten – soweit ihre Erhebung überhaupt erforderlich ist – datenschutzkonform verarbeitet werden.

7.3 Neuer Ausweis – Altes Foto

Aus der Praxis

Eine Bürgerin schilderte uns, sie habe beim Landesamt für Gesundheit und Soziales (LAGeSo) die Ausstellung eines Schwerbehindertenausweises beantragt und ein aktuelles Passfoto mitgeschickt. Daraufhin habe ihr das LAGeSo einen Schwerbehindertenausweis zugesandt, der statt mit dem aktuellen Passfoto der Bürgerin mit einem ca. 25 Jahre alten Lichtbild von ihr ausgestellt war.

Es stellte sich heraus, dass es sich dabei um ein Passfoto handelte, das die Bürgerin einige Jahrzehnte zuvor beim Versorgungsamt eingereicht hatte, um ihren alten DDR-Schwerbehindertenausweis umzutauschen. Wir haben versucht, die Angelegenheit mit dem LAGeSo aufzuklären. Im Ergebnis muss es sich hierbei um einen ungewöhnlichen Einzelfall gehandelt haben, bei dem das alte Lichtbild wohl seit den 1990er Jahren beim Schwerbehindertenvorgang der Bürgerin im Archiv „schlummerte“. Bei der Ausstellung des neuen Ausweises war offenbar nicht aufgefallen, dass es sich um ein nicht mehr aktuelles Foto handelte.

Im Rahmen der Prüfung des Einzelfalls konnten wir feststellen, dass eine Wiederholung eines solchen Falles unwahrscheinlich ist. Bei der Ausstellung von

Schwerbehindertenausweisen werden die Fotos unmittelbar nach Bescheiderstellung digitalisiert, das Foto wird danach sofort vernichtet. Die digitalisierte Datei wird regelmäßig automatisch nach vier Wochen gelöscht.

Die Angelegenheit wurde vom LAGeSo zum Anlass genommen, mit uns ein Verfahren abzustimmen, das im Sinne einer Kundenorientierung mit schriftlicher Zustimmung der Antragstellenden die Speicherung des Lichtbildes für die Dauer von zehn Jahren vorsieht, um die Bearbeitungszeit bei der Ausstellung eines neuen oder eines verloren gegangenen Ausweises zu verkürzen. Gegen die Einverständniserklärung bestehen keine datenschutzrechtlichen Bedenken, sodass wir von einem normalerweise datenschutzgerechten Verfahren bei der Ausstellung von Schwerbehindertenausweisen ausgehen.

7.4 Gehören Krankenkassenkarten in die Sozialamtsakte?

Ein Bürger beschwerte sich bei uns darüber, dass das Sozialamt von ihm bei der Beantragung von Leistungen der Sozialhilfe Kopien seines Personalausweises und der elektronischen Gesundheitskarte seiner Krankenkasse angefordert hatte.

Das Sozialamt räumte den Sachverhalt ein und teilte uns mit, die Vorlage des Personalausweises sei zur Identitätsprüfung notwendig gewesen. Die Vorlage der elektronischen Gesundheitskarte der Krankenkasse sei erforderlich gewesen, um die Angaben zur Krankenversicherung überprüfen zu können. Die Anforderung der Kopien habe dem Zweck gedient, eine persönliche Vorsprache im Sozialamt zu vermeiden.

Datenschutzrechtlich ist das Sozialamt berechtigt, vor der Bewilligung von Leistungen die Vorlage des Personalausweises zu verlangen. Dies gilt jedenfalls dann, wenn Leistungen erstmalig beantragt werden. Nicht umfasst von dieser Befugnis ist jedoch die Speicherung der Unterlagen in der Leistungsakte. Denn nach erfolgter Identitätsfeststellung ist der Personalausweis zur Prüfung des Anspruchs nicht mehr relevant.

Die Notwendigkeit zur Vorlage der elektronischen Gesundheitskarte der Krankenkasse konnten wir nicht nachvollziehen. Es ist ausreichend, wenn der Name der Krankenkasse und die Versicherungsnummer im Antragsvordruck benannt werden. Im konkreten Fall bezog der Beschwerdeführer eine Erwerbsminderungsrente, sodass ohnehin davon auszugehen war, dass die Beiträge für seine Sozialversicherungen von dem Rententräger direkt abgeführt werden und insoweit eine Kenntnis der Daten über die Krankenversicherung kaum notwendig gewesen sein dürfte.

Wir haben das Sozialamt über unsere rechtliche Bewertung informiert und dazu aufgefordert, ein datenschutzgerechtes Verfahren zum Umgang mit Personaldokumenten und elektronischen Gesundheitskarten zu etablieren. Das Sozialamt hat uns zugesichert, die Verfahrensabläufe bei der Antragsaufnahme und der weiteren Bearbeitung nach unseren Vorgaben anzupassen.

8 Beschäftigtendatenschutz

8.1 Umfang des Auskunftsersuchens von Beschäftigten

Die Beschwerdeführerin war Mit-Geschäftsführerin in einem Berliner Unternehmen. Nach ihrem Ausscheiden forderte sie das Unternehmen auf, ihr Auskunft über ihre personenbezogenen Daten zu erteilen. Dies betraf insbesondere ihre E-Mails (auch die, die nach ihrem Ausscheiden gesendet wurden), da sie ihre E-Mail-Adresse auch für private Zwecke nutzte. Das Unternehmen hat auch nach einem Vierteljahr keine Auskunft erteilt.

Wir haben bei dem Unternehmen einen Verstoß festgestellt. Der Verantwortliche ist gesetzlich verpflichtet, der betroffenen Person spätestens innerhalb eines Monats nach Eingang eines Antrags bestimmte Informationen zur Verfügung zu stellen.[97] Dieser Auskunftsverpflichtung kam das Unternehmen nicht fristgemäß nach. Das Auskunftsrecht gewährt jedoch keinen umfassenden Anspruch auf Herausgabe der kompletten Kommunikation, die über das E-Mail-System eines Unternehmens geführt wird.

Eine vollständige Herausgabe aller E-Mails aus dem System des Unternehmens, in denen der Name der Beschwerdeführerin auftaucht, ist schon allein deshalb nicht möglich, weil das Recht auf Herausgabe einer Datenkopie[98] durch die Rechte und Freiheiten anderer Personen beschränkt wird.[99] In der von der Beschwerdeführerin verlangten E-Mail-Kommunikation tauchten zahlreiche andere Personen (insbesondere andere Mitarbeitende des Unternehmens und Externe) auf, sodass hier umfangreiche Rückschlüsse auf personenbezogene Daten Dritter möglich gewesen wären, an denen die Beschwerdeführerin zudem kein konkretes Interesse vorgetragen hatte. Des Weiteren wäre mit einer umfassenden Herausgabe auch die Kenntniserlangung über interne Abläufe, Betriebsgeheimnisse und

97 Art. 15 Abs. 1 und Art. 12 Abs. 3 Satz 1 DS-GVO
98 Art. 15 Abs. 3 DS-GVO
99 Art. 15 Abs. 4 DS-GVO

Know-how des Unternehmens oder der mit ihm verbundenen Unternehmen verbunden gewesen. Dem standen berechtigte Unternehmensinteressen entgegen.

Im Ergebnis waren also die Daten von Unterhaltungen, die die Beschwerdeführerin im erlaubten Umfang zu privaten Zwecken geführt hatte, an sie herauszugeben. An der rein dienstlich veranlassten Korrespondenz war jedoch aufgrund der Beendigung ihres Arbeitsverhältnisses kein berechtigtes Interesse der Beschwerdeführerin (mehr) anzunehmen.

Ehemalige Beschäftigte haben grundsätzlich einen Anspruch darauf, ihre privaten E-Mails zu erhalten.

8.2 Löschung von Daten nach Beendigung des Beschäftigungsverhältnisses

Aus der Praxis

Eine Beschäftigte hatte mit ihrem Arbeitgeber einen Aufhebungsvertrag zur Beendigung des Beschäftigungsverhältnisses geschlossen. Dieser enthielt die Verpflichtung des Arbeitgebers, spätestens sechs Wochen nach Beendigung des Arbeitsverhältnisses das Profil der Beschäftigten auf der Webseite des Unternehmens zu löschen. Eine Bestätigung dieser Löschung erhielt die Beschwerdeführerin wenig später. In der Folgezeit stellte sie jedoch fest, dass durch Verlinkung auf der Webseite des Unternehmens noch ein Lebenslauf von ihr zu finden war. Nachdem sie hiergegen Widerspruch eingelegt hatte, hat das Unternehmen diese Verlinkungen unverzüglich gelöscht.

Ungeachtet einer möglichweise erteilten Einwilligung der Beschwerdeführerin während des Beschäftigungsverhältnisses war die Verarbeitung ihres Lebenslaufs jedenfalls nach Beendigung des Arbeitsverhältnisses unzulässig. Zwar kennt die DS-GVO keine Geltungsdauer einer Einwilligung, allerdings unterliegt auch die Verarbeitung personenbezogener Daten aufgrund einer Einwilligung im Rahmen eines Arbeitsverhältnisses dem Gebot der Zweckbindung.[100] Unter Berücksichtigung dieses Gebots muss deshalb davon ausgegangen werden, dass

100 Siehe Art. 5 Abs. 1 lit. b DS-GVO

eine Einwilligung zur Veröffentlichung eines Lebenslaufs auf den Zeitraum des Beschäftigungsverhältnisses beschränkt ist.

Personenbezogene Daten von Beschäftigten sind nach Beendigung des Arbeitsverhältnisses unverzüglich zu löschen, sofern sie nicht mehr erforderlich sind oder die betroffene Person die Einwilligung widerrufen hat.[101]

8.3 Löschung von Bewerberdaten für das Richteramt

Die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung plante, die Aufbewahrungsdauer der Auswahlvermerke zu abgelehnten Bewerberinnen und Bewerbern um das Richteramt von ursprünglich zehn Jahren auf fünf Jahre zu begrenzen. Die immer noch sehr lange Aufbewahrungsdauer wurde mit den Besonderheiten des Berliner Verfahrens zur Auswahl und Einstellung von Richterinnen und Richtern begründet. Diesen komme als unabhängigen Organen der Rechtspflege eine herausragende Rolle zu, weshalb die Entscheidung für eine bestimmte Person in dem Auswahlverfahren auf einer möglichst vollständigen Tatsachengrundlage zu treffen sei. Insoweit hielt es die Senatsverwaltung für notwendig, bei einer Auswahlentscheidung, sofern sich Bewerberinnen und Bewerber schon einmal beworben hatten, vorangegangene Entscheidungen miteinzubeziehen. Damit könne festgestellt werden, ob früher erkannte Defizite einer positiven Auswahl weiterhin entgegenstünden. Angesichts der beschränkten Anzahl der in den Auswahlgesprächen erörterten Fallsituationen würde den abgelehnten Bewerberinnen und Bewerbern zudem durch Vorwissen aus früheren Bewerbungsgesprächen ein erheblicher Wettbewerbsvorteil gegenüber anderen Bewerberinnen und Bewerbern zukommen, der auch vor dem Hintergrund des Datenschutzes kaum in Einklang mit dem verfassungsrechtlich verbürgten Leistungsgrundsatz[102] zu bringen sei.

101 Siehe Art. 17 Abs. 1 lit. a und b DS-GVO

102 Siehe Art. 33 Abs. 2 Grundgesetz (GG)

Gemäß § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG)[103] dürfen Bewerbungsunterlagen nur so lange gespeichert werden, wie dies zur Entscheidung über die Begründung eines konkreten Beschäftigungsverhältnisses erforderlich ist. Vorliegend sollten die Daten hingegen für eine neue Einstellungsentscheidung im Anschluss an eine negative Entscheidung über die Begründung eines Beschäftigungsverhältnisses verwendet werden. Eine weitere Aufbewahrung von Daten der Betroffenen im Zusammenhang mit einer erfolglosen Bewerbung ist jedoch regelmäßig nur zur Begründung der Entscheidung über die Nichteinstellung, z.B. im Rahmen einer Klage auf der Grundlage des Allgemeines Gleichbehandlungsgesetzes (AGG), zulässig.[104]

Zudem wäre eine Aufbewahrungsfrist von fünf Jahren unverhältnismäßig. Fünf Jahre alte Bewerbungsunterlagen und Gesprächsprotokolle bzw. -einschätzungen haben keinen oder nur einen sehr begrenzten Aussagegehalt, denn schon nach einer kurzen Zeit ist eine persönliche Weiterentwicklung der Bewerberin oder des Bewerbers denkbar.

Aufgrund der Besonderheiten bei Bewerbungen für das Richteramt haben wir uns mit einer Aufbewahrung der Auswahlvermerke für einen auf das unbedingt erforderliche Maß gekürzten Zeitraum von maximal zwei Jahren einverstanden erklärt. Wir haben die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung gebeten, nach zwei Jahren eine Evaluierung vorzunehmen, ob diese Aufbewahrungsdauer tatsächlich erforderlich ist.

Daten von abgelehnten Bewerberinnen und Bewerbern sind grundsätzlich nach Beendigung des Auswahlverfahrens und nach Ablauf der Fristen für Klagen zu löschen. Besonderheiten in Einzelfällen sind jedoch stets zu würdigen und zu berücksichtigen.

103 Der deutsche Gesetzgeber hat insoweit von der Öffnungsklausel des Art. 88 DS-GVO Gebrauch gemacht und führt damit die spezialgesetzliche Regelung des § 32 BDSG alte Fassung fort.

104 Siehe Art. 17 Abs. 3 e) DS-GVO

8.4 Betriebsinterne WhatsApp-Gruppe

Das Arbeitsverhältnis eines Beschwerdeführers wurde fristlos gekündigt. Die Kündigung wurde öffentlich, weil das Kündigungsschreiben vom Geschäftsführer fotografiert und in einem WhatsApp-Gruppen-Chat des Unternehmens, der zur Koordination genutzt wird, für alle Beschäftigten sichtbar publiziert wurde. Dem Kündigungsschreiben war zu entnehmen, dass dem Beschwerdeführer ein Darlehen vom Unternehmen gewährt wurde, um private Zahlungsverpflichtungen auszugleichen. Das Unternehmen teilte uns auf Anfrage mit, der Geschäftsführer habe das Kündigungsschreiben versehentlich in die WhatsApp-Gruppe eingestellt.

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines solchen oder nach Begründung für dessen Durchführung oder Beendigung erforderlich ist.[105]

Die Einstellung bzw. die Weiterleitung eines Kündigungsschreibens an eine hausinterne WhatsApp-Gruppe kann kaum erforderlich sein und ist daher regelmäßig rechtswidrig. Daran änderte im vorliegenden Fall auch der Umstand nichts, dass es sich um ein Versehen des Geschäftsführers handelte.

Im Übrigen ist der Einsatz von WhatsApp im Beschäftigungsverhältnis auch für Koordinierungszwecke im Unternehmen mit Vorgaben zum Beschäftigtendatenschutz, wie z.B. zur Speicherbegrenzung und zur Integrität und Vertraulichkeit[106] kaum vereinbar und war hier unverzüglich abzustellen. Gegenüber dem Unternehmen haben wir deshalb eine Verwarnung[107] ausgesprochen.

Der Einsatz von WhatsApp im Beschäftigungsverhältnis birgt erhebliche Risiken für das Persönlichkeitsrecht der Beschäftigten und ist daher regelmäßig unzulässig.

105 § 26 Abs. 1 Satz 1 BDSG
106 Siehe § 26 Abs. 4 BDSG i. V. m. Art. 5 DS-GVO
107 Siehe Art. 58 Abs. 2 lit. b DS-GVO

8.5 Notizen zu Verfahren des betrieblichen Eingliederungsmanagements

Aus der Praxis

Im Rahmen eines Verfahrens zum betrieblichen Eingliederungsmanagement (BEM) wurde gemeinsam mit der Betriebsärztin ein Lösungsvorschlag für eine Beschäftigte erarbeitet, der später im Rahmen einer Fallbesprechung entsprechend der Betriebsvereinbarung erörtert wurde. Dieses Gespräch wurde protokolliert. Das entsprechende Protokoll fehlte jedoch bei der Akteneinsicht durch die Beschäftigte. Auf Nachfrage wurde ihr mitgeteilt, dass ein entsprechendes Protokoll nicht existiere bzw. noch nicht freigegeben sei und im Übrigen auch nicht Bestandteil der BEM-Akte wäre, da es sich um handschriftliche Notizen eines BEM-Beteiligten handele und damit eine Einsichtnahme nicht gewährt werden könne. Dagegen wandte sich die Betroffene mit ihrer Beschwerde.

Nach der DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden bzw. wurden.[108] Dabei hat der Verantwortliche insbesondere eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind bzw. waren, der oder dem Betroffenen zur Verfügung zu stellen oder, wie im vorliegenden Fall erwünscht, eine Einsichtnahme in die Daten zu gewähren.[109]

Nach einer Entscheidung des Bundesverwaltungsgerichts sind Notizhefte, Tagebuchkladden etc. keine Personalvorgänge, soweit sie durch individuelle Bestimmung der Besitzerin oder des Besitzers des Heftes für den ausschließlich persönlichen Gebrauch geführt werden, selbst wenn ihr Inhalt dienstliche Bezüge aufweist.[110] Als einzige Voraussetzung bzw. Bedingung für die Führung solcher Kladden oder Hefte mit persönlichen Notizen ist nach dieser Entscheidung eine sichere Aufbewahrung vor dem Zugriff von Dritten bzw. anderen Personen (z.B. Kolleginnen und Kollegen, Reinigungskräfte etc.).

108 Art. 15 Abs. 1 DS-GVO
109 Art. 15 Abs. 3 DS-GVO
110 Urteil des Bundesverwaltungsgerichts vom 19. Oktober 2005 – 1 D 14.04

Im vorliegenden Fall wurden handschriftliche Notizen eines Teilnehmers bei einem sog. Erörterungsgespräch angefertigt. Diese waren für den Dienstbetrieb erforderlich, da ohne schriftliche Fixierung bzw. ohne Protokolle Maßnahmen oder Hilfestellungen nicht konkret und korrekt umgesetzt und die Betroffene nicht umfassend über das Ergebnis der Fallbesprechung informiert werden konnte. Ein nur persönlicher Gebrauch scheidet somit aus. Die Verweigerung der Einsichtnahme durch die Beschwerdeführerin war daher rechtswidrig.

Nach kurzem Schriftwechsel teilte uns das Unternehmen mit, es habe nunmehr der Beschwerdeführerin vollumfänglich Einsicht in die Notizen zur Fallbesprechung gewährt. Wegen des Verstoßes haben wir eine Verwarnung ausgesprochen.[111]

Beschäftigte haben ein vollumfängliches Recht auf Kenntnis bzw. Einsichtnahme in Unterlagen und Dokumente, die personenbezogene Daten über sie enthalten – sowohl in elektronischer als auch in Papierform.

111 Siehe Art. 58 Abs. 2 lit. b DS-GVO

9 Wirtschaft

9.1 Die ewige Mieterakte

Aus der Praxis

Das erste deutsche Bußgeld nach der Datenschutz-Grundverordnung (DS-GVO) in Millionenhöhe verhängten wir im Oktober 2019 gegen die Deutsche Wohnen SE, das zweitgrößte deutsche Immobilienunternehmen. Grund war die fortdauernde Speicherung unzähliger Dokumente, die für die Durchführung von Mietverträgen überhaupt nicht oder nach dem Ablauf von buchhalterischen Aufbewahrungsfristen nicht mehr erforderlich waren.

Bei einer Prüfung vor Ort bei der Deutschen Wohnen SE im Juni 2017 war aufgefallen, dass das von diesem Unternehmen eingerichtete Archivsystem auch Unterlagen enthielt, die entweder von vornherein nicht hätten dort abgelegt werden dürfen oder deren Aufbewahrungsfrist bereits abgelaufen war. So ist z.B. die Aufbewahrung von Kopien von Ausweisdokumenten oder Arbeits- und Ausbildungsverträgen für die Durchführung eines laufenden Mietverhältnisses nicht erforderlich und damit auch nicht gestattet. Wir teilten dem Unternehmen im Anschluss an die damalige Prüfung mit, dass das vorgehaltene System nicht der geltenden Rechtslage entspricht und bereinigt werden muss. Die Deutsche Wohnen SE erklärte sich nach anfänglichem Zögern Ende 2017 bereit, rechtswidrig gespeicherte Dokumente zu entfernen und legte in der Folge ein Konzept hierfür vor, das sich maßgeblich auf eine Durchsicht der gespeicherten Unterlagen in einem automatisierten Verfahren stützte.

Im März 2019 unterzogen wir den Datenbestand vor Ort erneut einer eingehenden Prüfung, um uns von dem Erfolg des Ansatzes der Deutschen Wohnen SE zu überzeugen. Wir hatten dem Unternehmen unsere Zweifel, dass das geplante Verfahren zu einer vollständigen Bereinigung des Datenbestands führen würde, bereits ein Jahr zuvor mitgeteilt. Es stellte sich jedoch heraus, dass das Unternehmen zum Prüfzeitpunkt noch kein einziges Dokument gelöscht, sondern erst mit einigen vorbereitenden Arbeiten begonnen hatte. Frühestens zum Sommer 2019 sollte tatsächlich mit der Löschung der unrechtmäßig gespeicherten Daten begonnen werden.

Damit mussten wir feststellen, dass die Deutsche Wohnen SE mehr als anderthalb Jahre nach der ersten Prüfung und mehr als neun Monate nach Gültigkeit der DS-GVO weder die Löschung durchgeführt, noch die zu löschenden Daten bestimmt, noch auch nur die Voraussetzungen für die Erfüllung der Löschpflicht geschaffen hatte.

Zu diesen Voraussetzungen zählt insbesondere die Ablage der Daten in einem System, das über eine Funktion für die Löschung ausgewählter Unterlagen verfügt. Die Deutsche Wohnen SE hatte ihr Archivsystem ausdrücklich so konfigurieren lassen, dass die Löschung einzelner Dokumente nicht möglich war. Sie führte an, dass dies aus Gründen der Revisionssicherheit notwendig sei. Dies ist jedoch nicht der Fall. Handels- und steuerrechtlich ist lediglich geboten, dass bestimmte Unterlagen für eine gesetzlich fixierte Zeit unverändert aufbewahrt werden. Nach Ablauf dieser Aufbewahrungsfrist muss eine Löschung erfolgen, wenn nicht im Einzelfall besondere Gründe dagegensprechen. Ein Archivsystem muss daher so konstruiert sein, dass die rechtlich gebotenen Löschvorgänge die ebenfalls gebotene weitere Aufbewahrung jüngerer Dokumente nicht beeinflussen. Dies ist ohne Weiteres mit Systemen möglich, die seit Jahren am Markt verfügbar sind.

Darüber hinaus hatte die Deutsche Wohnen SE im Zuge des Ankaufs von Immobilien von den Voreigentümern übergebene Unterlagen jahrelang en bloc gescannt und sich die Mühe gespart, Dokumente auszusondern, für deren Aufbewahrung keine Rechtsgrundlage mehr bestand oder noch nie bestanden hatte. Diese Form der Datenübernahme war bereits nach alter Rechtslage unzulässig. Der Deutschen Wohnen SE war diese Unzulässigkeit durch unsere Hinweise spätestens seit dem Jahr 2017 bekannt. Umso mehr verwundert, dass wir diesen ungeordneten Zustand im Jahr 2019 noch immer vorfanden. Vorgestellt wurde uns lediglich die Softwarelösung, welche in der Zukunft die Aussonderung vornehmen sollte. Gleichzeitig wurde offenbar, dass – wie Tests des Unternehmens gezeigt hatten – diese Softwarelösung keineswegs alle auszusondernden Dokumente erkennen würde, eine manuelle Nachprüfung in Zweifelsfällen dessen ungeachtet jedoch nicht geplant war.

Die DS-GVO verlangt von den Verantwortlichen, dass sie – bei Festlegung der Mittel der Verarbeitung sowie zum Zeitpunkt ihrer Durchführung – technische und organisatorische Maßnahmen ergreifen, um die Einhaltung der Datenschutz-

grundsätze zu gewährleisten. Zu diesen Grundsätzen gehört, dass Daten nur rechtmäßig und in dem für die jeweiligen Zwecke notwendigen Umfang verarbeitet werden. Sind diese Zwecke und etwaige Aufbewahrungspflichten erfüllt, dann muss eine Löschung erfolgen. Da die Deutsche Wohnen SE über lange Zeit derart notwendige Maßnahmen nicht vorgenommen hat, haben wir diesen Verstoß gegen das Gebot des Datenschutzes durch Technikgestaltung geahndet.

Eine ausufernde Speicherpraxis kann nicht wegen vermeintlich bestehender Pflichten zur Aufbewahrung personenbezogener Daten gerechtfertigt werden. Auch große Unternehmen, die aufgrund ihres Geschäftsmodells eine Vielzahl von Daten verarbeiten, müssen den gegebenenfalls hohen Aufwand für die Kategorisierung dieser Daten, die Schaffung der technischen Voraussetzungen zur Ermöglichung der rechtlich geforderten Löschung und für die Umsetzung bestehender Löschpflichten in Kauf nehmen. Das Anlegen von „Datenfriedhöfen", wie im vorliegenden Fall, entspricht regelmäßig nicht den Anforderungen an technische und organisatorische Maßnahmen, deren Umsetzung die DS-GVO zum Schutz Betroffener vorsieht, und stellt auch im Einzelfall keine rechtmäßige Verarbeitung personenbezogener Daten dar.

9.2 Bitte lächeln! – Zutritt zu Coworking-Räumen nur nach Fotoaufnahmen

Gäste der Nutzenden von Coworking-Räumlichkeiten[112] erhielten nur Zutritt, wenn sie sich bei der Registrierung fotografieren ließen. Diese Fotos sollten der Besuchsanmeldung sowie der Gefahrenabwehr und Beweissicherung dienen. Die Aufnahmen wurden für 30 Tage gespeichert.

Gäste der Nutzenden von Coworking-Büroräumen mussten sich über eine auf einem fest installierten Tablet-Computer bereitgestellte Registrierungs-App als Besucherinnen und Besucher anmelden. Diese App fragte sowohl die Namen der

112 Der Begriff Coworking beschreibt das Teilen von Arbeitsräumen mit unternehmensfremden Personen. In den sog. Coworking Spaces mietet man zumeist einzelne Schreibtische für kurze Zeiträume an. Vor allem Freiberufler und Start-up-Unternehmen nutzen dieses Konzept.

Gäste als auch die Namen der Personen ab, bei denen sie angemeldet werden sollten. Anschließend startete die App die Frontkamera und machte ein Foto der jeweiligen Person. Erst nach Abschluss des Registrierungsprozesses konnten Gäste am Empfang abgeholt werden. Gespeichert wurden neben dem Namen des Gastes und der gastgebenden Person auch der Grund, das Datum und die Uhrzeit des Besuchs sowie das Foto des Gastes.

Eine Verarbeitung der personenbezogenen Daten von Besucherinnen und Besuchern ist nur rechtmäßig, soweit sie zur Wahrung der berechtigten Interessen der oder des Verantwortlichen oder eines Dritten erforderlich ist und sofern nicht Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen.[113] Als berechtigte Interessen kamen im vorliegenden Fall eine reibungslose Besuchsanmeldung, eine präventive Gefahrenabwehr und eine nachträgliche Beweissicherung in Betracht. Allerdings war die Anfertigung von Fotos der Besucherinnen und Besucher für diese Zwecke nicht erforderlich. Es gab gleich geeignete, aber weniger eingriffsintensive Maßnahmen, um das gewünschte Ergebnis zu erzielen.

Zum einen ist bereits durch die Übermittlung des Besuchernamens gewährleistet, dass es sich um die eingeladene Person handelt. Zum anderen werden die Gäste auch am Empfang abgeholt. Dadurch wird gewährleistet, dass Gastgeber nur Besucherinnen und Besucher hereinlassen, die sie persönlich kennen oder einer vorherigen Einladung zuordnen können. Im Übrigen kann durch die Vorlage eines Lichtbildausweises sichergestellt werden, dass es sich bei der anwesenden Person um die tatsächlich angemeldete Person handelt.

Auf unser Einschreiten hin hat der Verantwortliche der Büroraumvermietung das Vorgehen abgestellt.

Die Anfertigung und Speicherung von Fotografien bei einer Anmeldung von Besucherinnen und Besuchern ist rechtswidrig, da mildere, gleich geeignete Mittel zur Verfügung stehen, um eine reibungslose Anmeldung sicherzustellen.

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

9.3 Inkassounternehmen: Personenverwechslung nicht ausgeschlossen

Ein Inkassounternehmen verarbeitete nach einer Adressabfrage bei einer Auskunftei die Daten einer Beschwerdeführerin, obwohl weder deren aktuelle Anschrift noch deren Voranschrift mit der Rechnungs- und Lieferadresse der namensgleichen Schuldnerin übereinstimmten.

Das Inkassounternehmen war von einem Unternehmen mit der Einziehung einer offenen Forderung aus einem Warenkaufvertrag beauftragt worden. In diesem Zusammenhang hatte es u. a. Name, Vorname, Geburtsdatum, aktuelle Anschrift und Lieferadresse der Schuldnerin der Forderung erhalten. Diese wurde zunächst per E-Mail und nachfolgend postalisch unter der Lieferanschrift zur Begleichung der offenen Forderung aufgefordert, reagierte jedoch nicht. Zwei weitere an die Lieferanschrift gerichtete Briefe konnten von der Deutschen Post nicht zugestellt werden. Das Inkassounternehmen beantragte daher unter Angabe der bekannten Adressdaten eine Abfrage zur aktuellen Anschrift der Schuldnerin bei einer Auskunftei.

In der von der Auskunftei erteilten Antwort waren jedoch die Anschrift sowie die Voranschrift einer namensgleichen Person, nämlich die der Beschwerdeführerin enthalten – naturgemäß stimmten beide Angaben nicht mit den dem Inkassounternehmen bereits vorliegenden Adressinformationen überein. Die Auskunftei hatte die Auskunft allerdings ausdrücklich unter einen sog. Identitätsvorbehalt gestellt. Trotzdem und ohne weitere Prüfung forderte das Inkassounternehmen von der Beschwerdeführerin nunmehr die Begleichung der Forderung gegen die Schuldnerin.

Zwar können Unternehmen grundsätzlich Inkassounternehmen zur Geltendmachung von bestehenden Forderungen aus einem Vertragsverhältnis beauftragen und dürfen diesen nach Art. 6 Abs. 1 lit. f DS-GVO die dazu erforderlichen personenbezogenen Daten von Schuldnern übermitteln. Gestützt auf dieselbe Rechtsgrundlage können Inkassounternehmen die für die Erfüllung ihres Auftrags zusätzlich erforderlichen Daten, bspw. eine neue Anschrift, durch Anfrage bei einer Auskunftei erheben. Werden die Forderungen dagegen an ein Inkassounterneh-

men abgetreten (Factoring), wird dieses zum eigenen Vertragspartner gegenüber den jeweiligen Schuldnerinnen und Schuldnern und muss seine Datenverarbeitung auf eine andere Rechtsgrundlage stützen.[114]

Die Verwendung der Anschrift der Beschwerdeführerin verstieß im konkreten Fall allerdings dennoch gegen die gesetzlichen Vorgaben. Da die Beschwerdeführerin nicht Schuldnerin der Forderung war, konnte sich das Inkassounternahmen objektiv bereits hinsichtlich der Verarbeitung ihrer personenbezogenen Daten nicht auf eine wirksame Rechtsgrundlage stützen.

Personenbezogene Daten, die verarbeitet werden, müssen sachlich richtig sein.[115] Hieraus folgt die Verpflichtung jeder verantwortlichen Stelle, durch geeignete organisatorische und technische Verfahren sicherzustellen, dass Identitätsverwechslungen ausgeschlossen sind. Das Inkassounternehmen hatte vorliegend versäumt, entsprechende Prüfprozesse zu entwickeln und einzusetzen.

Das Inkassounternehmen hat uns mitgeteilt, dass es sein Verfahren zum Ausschluss einer Personenverwechslung zwischenzeitlich umgestellt habe. Seit der Umstellung könne eine neue Adresse aus einer Abfrage bei einer Auskunftei nur verwendet werden, wenn eine der Voranschriften aus der Adressabfrage mit der bereits bekannten Anschrift der Schuldnerin bzw. des Schuldners übereinstimmt.

Unternehmen dürfen nur sachlich richtige Daten verarbeiten und sind verpflichtet, durch geeignete technische und organisatorische Verfahren sicherzustellen, dass Identitätsverwechslungen ausgeschlossen sind. Informationen aus Auskünften mit einem Identitätsvorbehalt dürfen niemals ohne sorgfältige Prüfung im Einzelfall weiterverwendet werden.

114 Art. 6 Abs. 1 lit. b DS-GVO
115 Art. 5 Abs. 1 lit. d DS-GVO

9.4 „Topf Secret“ macht alles öffentlich

Aus der Praxis

Seit Januar 2019 können Bürgerinnen und Bürger auf der Plattform „Topf Secret“ die Protokolle behördlicher Hygienekontrollen von Gastronomiebetrieben wie Restaurants oder Bäckereien anfordern. Insgesamt wurden über die Plattform fast 50.000 Anträge gestellt. Das Projekt wurde von der Verbraucherorganisation Foodwatch e. V. und der Betreiberin der Internetplattform FragDenStaat gemeinsam initiiert.

Die Antragstellung erfolgt auf der Grundlage des Verbraucherinformationsgesetzes (VIG), auf dessen Basis jede Person auch eigenständig eine Anfrage an die zuständige Behörde richten kann.[116] Die Plattform möchte jedoch nicht nur die Antragstellung für einzelne Personen erleichtern, sondern die Korrespondenz und Hygieneberichte auch veröffentlichen, um Transparenz zu schaffen.

Wer über die Plattform einen Antrag stellen möchte, wählt über die eingebundene Karte von OpenStreetMap[117] einen Gastronomiebetrieb aus. Anschließend müssen der eigene Name und die eigene Adresse angegeben werden. Die Plattform generiert für jede Anfrage eine individuelle E-Mail-Adresse, an die die Antworten der Behörden gehen. Sollte eine angefragte Behörde per E-Mail antworten, werden diese Antworten ohne Anhänge automatisch veröffentlicht, einige Daten dabei ebenso automatisch geschwärzt. Alle weitere Korrespondenz müssen die Antragstellenden zunächst freischalten oder selbst hochladen. Sie werden in diesem Zusammenhang gebeten, personenbezogene Daten unkenntlich zu machen, was ihnen technisch auf der Plattform durch ein Anwendungsprogramm ermöglicht wird.

Auf der Plattform werden Daten von drei Personengruppen verarbeitet: Die erste sind die Antragstellenden selbst, die zweite die Inhaberinnen und Inhaber der häufig sehr kleinen Gastronomiebetriebe und die dritte Gruppe die Sachbearbeitenden in den Behörden, an die die Anfragen gerichtet werden.

116 § 1 VIG

117 OpenStreetMap ist ein online verfügbarer Stadtplan, der auch als Geoinformationssystem bezeichnet wird. In diesem sind auch die Adressen vieler Gastronomiebetriebe verzeichnet.

In unserer Prüfung ging es zunächst um das eingesetzte Schwärzungsprogramm: Dieses Programm ist in der Lage, eigenständig einige Formulierungen in den E-Mails zu erkennen, wie z.B. „Sehr geehrte …“, und in diesem Fall automatisch den sich daran anschließenden Namen zu schwärzen. Die Dokumente, die die Antragstellenden hochladen, sowie die E-Mail-Anhänge müssen diese hingegen selbst mit dem bereitgestellten Programm schwärzen. Die Plattform weist hierauf sehr deutlich hin. Trotzdem werden in einigen Fällen diese Dokumente nicht oder nicht ausreichend anonymisiert.

Da es sich bei der Plattform um einen Online-Dienst handelt, ist zunächst davon auszugehen, dass die Personen, die die Dokumente hochladen, für die Schwärzung verantwortlich sind. Die Anbieterinnen der Plattform sind erst dann für die Inhalte verantwortlich, wenn ihnen diese bekannt werden – bspw. indem sie darauf hingewiesen werden.[118] In diesem Fall müssen sie für eine umgehende Schwärzung sorgen. Einen systematischen Verstoß konnten wir hier nicht feststellen, da die Plattform, wenn sie auf ungenügend geschwärzte Dokumente aufmerksam gemacht wurde, dies in den uns bekannten Fällen innerhalb kürzester Zeit nachgeholt hat, teilweise innerhalb weniger Minuten.

Die Anfragen selbst können nicht anonym gestellt werden, da das VIG diese Angaben verlangt.[119] Auf der Plattform besteht nur die Möglichkeit, sich dagegen zu entscheiden, seinen Namen öffentlich anzeigen zu lassen, indem die Nutzenden ein Häkchen neben der Aussage „Ich möchte nicht, dass mein Name veröffentlicht wird“ (opt-out) setzen. Dies stellt keine Einwilligung im Sinne der DS-GVO dar. Denn eine Einwilligung liegt nur vor, wenn eine aktive Entscheidung für eine Datenverarbeitung getroffen wird. Dies wäre bspw. der Fall, wenn ein Häkchen vor dem Satz „Ja, ich möchte, dass mein Name veröffentlicht wird“ (opt-in) gesetzt werden kann. Allerdings hat die Plattform sich zum Ziel gesetzt, einen möglichst transparenten Dialog zwischen Bürgerinnen und Bürgern und den staatlichen Stellen zu fördern. Im Rahmen dieses Konzepts kann es noch als verhältnismäßig angesehen werden, auch die Namen der Antragstellenden zu veröffentlichen. Trotzdem fehlen hier eindeutige Informationen, wann und wo genau die Namen veröffentlicht werden. Derzeit wird zunächst nicht darauf hingewiesen, dass im

118 § 10 Telemediengesetz (TMG)

119 § 4 Abs. 1 Satz 3 VIG

Regelfall die Anfragenden auf der Webseite namentlich genannt werden. Wir haben die Plattform aufgefordert, einen solchen Hinweis einzufügen, denn Verantwortliche sind gesetzlich verpflichtet, personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise zu verarbeiten und hierüber transparent zu informieren[120], damit diese ihre Betroffenenrechte in umfassender Form wahrnehmen kann. Selbst wenn die Nutzenden sich entschieden haben, ihren Namen nicht zu veröffentlichen, kann es passieren, dass diese im Schriftverkehr mit einer Behörde versehentlich nicht unkenntlich gemacht werden, bevor die Dokumente durch die Antragstellenden oder die Plattform hochgeladen werden. Auch auf dieses Risiko muss die Plattform ausdrücklich hinweisen.

Im Übrigen war zu Beginn unserer Prüfung auf der Plattform keine aktuelle Datenschutzerklärung veröffentlicht. Auf unseren Hinweis hin wurde die Erklärung aktualisiert, insbesondere wird in ihr jetzt auf die Betroffenenrechte hingewiesen.

Beschwerden, die uns erreichten, weil die Ämter die Offenlegung der Kontrollberichte verweigerten, konnten wir allerdings nicht weiterverfolgen. Unsere Behörde kann in Angelegenheiten des VIG – anders als nach dem Berliner Informationsfreiheitsgesetz (IFG) – nicht vermitteln, weil das VIG eine Schiedsstelle nicht vorsieht und uns diese Funktion vom Landesgesetzgeber nur in Bezug auf das IFG übertragen wurde.[121] Allerdings haben wir die Behörden in den jeweiligen Fällen darauf hingewiesen, dass von Antragstellenden grundsätzlich keine Personalausweiskopie verlangt werden darf.

Die Plattform „Topf Secret“ hat einige Schritte unternommen, um einen Ausgleich zwischen Transparenz und Datenschutz zu finden. Was die Transparenz der Datenverarbeitung angeht, sind noch Nachbesserungen erforderlich.

120 Siehe Art. 5 Abs. 1 lit. a i. V. m. EG 39 DS-GVO und Art. 12 Abs. 1 i. V. m. EG 58 DS-GVO
121 § 18 IFG

9.5 HelloKoppelungsverbot

Das Unternehmen HelloFresh hat bei der Online-Anmeldung zu seinem Dienst verlangt, dass mit einem einzigen Häkchen der Datenschutzerklärung den allgemeinen Geschäftsbedingungen und der telefonischen Kontaktaufnahme zu Werbezwecken gleichzeitig zugestimmt wird.

Eine Einwilligung in dieser Form gebündelt einzuholen, ist rechtswidrig. Denn eine Einwilligung ist nur wirksam, wenn sie freiwillig erteilt wird. Freiwillig heißt, dass man sich für oder gegen etwas entscheiden kann, ohne Nachteile zu erleiden. Oder anders formuliert, die Einwilligung darf nicht zur Bedingung für etwas gemacht werden, was sich von anderen Vorgängen trennen lässt.[122] In diesem Fall muss es bspw. möglich sein, Lebensmittel zu bestellen, ohne zusätzlich sein Einverständnis in die Verwendung der persönlichen Telefonnummer zur Kontaktaufnahme zu erklären.

Dadurch wird sichergestellt, dass die Verarbeitung personenbezogener Daten, um deren Einwilligung ersucht wird, nicht direkt oder indirekt zur Gegenleistung für einen Vertrag werden kann. Bei der Einwilligung und dem Vertrag handelt es sich um zwei unterschiedliche Rechtsgrundlagen für die rechtmäßige Verarbeitung personenbezogener Daten. Diese beiden Rechtsgrundlagen dürfen nicht zusammengeführt werden, ihre Grenzen dürfen nicht verschwimmen.

Zur Bewertung, ob eine solche unzulässige Bündelung oder Verknüpfung vorliegt, muss festgestellt werden, welchen Umfang der Vertrag hat und welche Daten für die Erfüllung des Vertrags erforderlich sind. Die Einwilligung in die telefonische Kontaktaufnahme zum Zwecke der Werbung war hier für die Erbringung des Vertrags, die Lieferung der Lebensmittel, nicht erforderlich. Eine Lieferung kann auch an Menschen ohne Telefon erfolgen. Diese Einwilligung wurde deshalb unrechtmäßig mit der Erfüllung der Dienstleistung verknüpft.

122 Siehe Art. 7 Abs. 4 DS-GVO, EG. Nr. 42 und 43 DS-GVO

Wir konnten erwirken, dass die Zustimmung zur telefonischen Kontaktaufnahme aus dem Kästchentext entfernt wurde. Nunmehr wird eine Einwilligung in die telefonische Kontaktaufnahme zu Werbezwecken separat eingeholt.

Eine Einwilligung in eine für die Erfüllung eines Vertrags nicht erforderliche Datenverarbeitung darf nicht zur Bedingung des Vertrags gemacht werden.

9.6 Kundendaten beim Asset Deal

Die Veräußerung von einzelnen Geschäftszweigen, Vermögensgegenständen, Produktsparten oder Dienstleistungen eines Unternehmens an ein anderes Unternehmen (Asset Deal) zählt zum Tagesgeschäft im Bereich Wirtschaft. Wer im Wege eines Asset Deals nur einzelne Vermögensgegenstände eines Unternehmens kauft, hat in der Regel auch ein großes Interesse am Erwerb der zugehörigen Kundendaten, um Waren oder Dienstleistungen des übernommenen Geschäftszweigs den Kundinnen und Kunden weiter anbieten zu können.

Die Veräußerung von Kundendaten in solchen Fallkonstellationen ist eine Datenverarbeitung, deren Rechtmäßigkeit sich nach der DS-GVO bestimmt.[123]

Eine Weitergabe der Kundendaten darf erfolgen, wenn eine wirksame Einwilligung der Kundinnen und Kunden zur Übertragung der Daten auf das erwerbende Unternehmen vorliegt.[124]

Daneben kann eine Datenweitergabe aber auch berechtigt sein, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist.[125] Dabei ist zu prüfen, inwieweit schutzwürdige Interessen der Kundinnen und Kunden einer solchen Datenübertragung entgegenstehen.

123 Siehe Art. 4 Nr. 2 DS-GVO zur Definition personenbezogener Daten und Art. 6 Abs. 1 DS-GVO zur Rechtmäßigkeit der Datenverarbeitung

124 Art. 6 Abs. 1 lit. a DS-GVO, Art. 7 DS-GVO

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

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat Empfehlungen für eine einheitliche Verwaltungspraxis verabschiedet und sich auf einen Katalog von Fallgruppen verständigt, die im Rahmen der gesetzlich vorgegebenen Interessenabwägung bei einem Asset Deal herangezogen werden können.[126]

Es ist im jeweiligen Einzelfall zu untersuchen, ob eine Übertragung der Kundendaten mit dem Zweck der ursprünglichen Erhebung der Daten vereinbar ist. Besteht keine Vereinbarkeit oder handelt es sich um sensitive Daten[127], ist eine Weitergabe nur auf Grundlage einer informierten Einwilligung der Kundinnen und Kunden möglich.

In den anderen Fällen gilt: Eine Weitergabe von Kundendaten zum Zwecke der Fortführung laufender Verträge kann gerechtfertigt sein, wenn die Kundinnen und Kunden ihre zivilrechtliche Genehmigung zur Übernahme des Vertrags bzw. der Verpflichtungen aus dem Vertrag durch die erwerbende Stelle gemäß bzw. analog zu § 415 Bürgerliches Gesetzbuch (BGB) erteilt haben. Eine solche zivilrechtliche Genehmigung kann regelmäßig auch als datenschutzrechtliche Einwilligung zum Übergang der erforderlichen Daten[128] angesehen werden, aber auch als zur Vertragserfüllung erforderlich[129] oder auf Basis einer Interessenabwägung zulässig[130] sein.

Gleiches gilt für Fälle, in denen Kundendaten im Zusammenhang mit offenen Forderungen an eine Erwerberin oder einen Erwerber übertragen werden sollen. Auch hier richtet sich die Zulässigkeit zunächst nach den zivilrechtlichen Bestim-

126 Beschluss der DSK vom 24. Mai 2019: „Asset Deal – Katalog von Fallgruppen" (https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk/); Anmerkung: Der Beschluss wurde von der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) und dem Sächsischen Datenschutzbeauftragten abgelehnt. Die BlnBDI teilt die im Beschluss unter Ziffer 2 „Bestandskunden ohne laufende Verträge und letzter Vertragsbeziehung älter als 3 Jahre" enthaltene Auffassung, wonach eine Übermittlung und Nutzung dieser Daten für Zwecke gesetzlicher Aufbewahrungsfristen zulässig sein soll, nicht und vertritt die im Text enthaltene abweichende Rechtsposition.

127 Siehe Art. 9 DS-GVO

128 Art. 6 Abs. 1 lit. a DS-GVO, Art. 7 DS-GVO

129 Art. 6 Abs. 1 lit. b DS-GVO

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

mungen der Forderungsabtretung[131]. Sofern aus zivilrechtlicher Sicht eine Übertragung möglich und eine Forderungsabtretung nicht durch eine Vereinbarung ausgeschlossen ist,[132] kann eine Übertragung der mit der Forderung in Verbindung stehenden Kundendaten auch datenschutzrechtlich[133] zulässig sein.

Daten von Kundinnen und Kunden bei fortgeschrittener Vertragsanbahnung oder von Bestandskundinnen und -kunden ohne laufende Verträge, deren letzte aktive Vertragsbeziehung nicht länger als drei Jahre zurückliegt, können im Weg der Widerspruchslösung (sog. Opt-Out-Modell) übertragen werden. Dabei sind alle Betroffenen vorab über den geplanten Verkauf zu informieren und ihnen ist eine angemessene Widerspruchsfrist, die mindestens sechs Wochen betragen sollte, einzuräumen. Sofern kein Widerspruch erklärt wird, ist die Weitergabe der jeweiligen Daten an die Käuferin bzw. den Käufer zulässig.[134] Im Fall eines Widerspruchs dürfen die Daten nicht an die Erwerberin bzw. den Erwerber weitergegeben werden.

Eine Übermittlung der Daten von Bestandskundinnen und -kunden, bei denen die letzte aktive Vertragsbeziehung mehr als drei Jahre zurückliegt, an eine Erwerberin oder einen Erwerber ist jedoch grundsätzlich nicht zulässig. Für derartige Daten besteht schon gesetzlich eine antragsunabhängige Verpflichtung des ursprünglichen Unternehmens zur Löschung, sofern diese Daten für die Zwecke, für die sie erhoben bzw. verarbeitet wurden, nicht mehr notwendig sind.[135] Eine weitere Verarbeitung kann nur nach Maßgabe des Art. 17 Abs. 3 DS-GVO, wie bspw. auf der Grundlage von rechtlichen Verpflichtungen zur Erfüllung steuer- oder handelsrechtlicher Pflichten zulässig sein. Es handelt sich in allen Fällen jeweils um Verpflichtungen des ursprünglichen Unternehmens, welche nicht auf eine erwerbende Stelle übertragbar sind. Aus diesem Grund ist die Übertragung solcher Altdaten an Erwerberinnen und Erwerber datenschutzrechtlich unzulässig.

131 Siehe §§ 398 ff. BGB
132 Insbesondere nicht nach § 399 2. Alt. BGB
133 Auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO
134 Nach Art. 6 Abs. 1 lit. f DS-GVO
135 Siehe Art. 17 Abs. 1 lit. a 2. Alt. DS-GVO

Die Übertragung von Kundendaten auf die Erwerberin oder den Erwerber eines Unternehmens kann bei einem Asset Deal in bestimmten Fallkonstellationen auch ohne Einwilligung der Kundinnen und Kunden zulässig sein. Dabei ist jedoch stets sorgfältig zu prüfen, ob eine Übertragung mit dem Zweck der ursprünglichen Erhebung der Daten vereinbar ist und ob ihr schutzwürdige Interessen der Kundinnen und Kunden entgegenstehen.

9.7 Unternehmen: Bearbeitung von Anfragen Betroffener sicherstellen!

In Beschwerdeverfahren wird von verantwortlichen Stellen oft der Einwand vorgebracht, betroffene Personen hätten ihren Antrag auf Auskunft, Berichtigung, Löschung oder Geltendmachung eines Werbewiderspruchs oder ihren Widerruf einer Einwilligung nicht an die innerhalb eines Unternehmens jeweils zuständige Stelle gerichtet und aus diesem Grund habe eine fristgerechte Beantwortung ihrer Anliegen oder eine Umsetzung ihres Antrags nicht erfolgen können.

Adressat bei der Geltendmachung von Betroffenenrechten ist nach der DS-GVO der Verantwortliche als solcher[136]. Geht der oder dem Verantwortlichen ein solcher Antrag zu, ist er zu bearbeiten, auch wenn intern in der Einrichtung eine differenzierte Aufgabenverteilung bestimmt wurde. Auch E-Mails, die als vermeintlicher Spam zwar vom Mail-Server angenommen, aber in einen Spam-Ordner verschoben und nicht gelesen wurden, sind zugegangen.

Eine verantwortliche Stelle ist verpflichtet, durch geeignete technisch-organisatorische Maßnahmen die Erfüllung ihrer datenschutzrechtlichen Verpflichtungen sicherzustellen.[137] Durch passende innerorganisatorische Maßnahmen und Prozessabläufe ist jeweils eine Weiterleitung an die im Unternehmen hierfür zuständige Stelle und eine entsprechend fristgerechte Bearbeitung der Anfragen zu gewährleisten. Verantwortliche Stellen sollten deren Wirksamkeit regelmäßig

136 Siehe Definition in Art 4 Ziff. 7 DS-GVO: „...die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;..."

137 Art. 24 Abs. 1 DS-GVO

überprüfen und im Bedarfsfall eine Anpassung der Abläufe vornehmen, um die ihnen obliegenden Pflichten einzuhalten.

Unternehmen sind stets verpflichtet, durch geeignete Maßnahmen sicherzustellen, dass alle eingehenden datenschutzrechtlichen Anfragen auch die bei ihnen zuständigen Ansprechpartnerinnen und -partner erreichen, um ihre gesetzlichen Verpflichtungen einzuhalten.

9.8 Internet-Impressum: Keine Nutzung von Daten zu Werbezwecken!

Aus der Praxis

Immer wieder erreichen uns Beschwerden von Personen, die von Unternehmen, mit denen sie in keinerlei Beziehung stehen, Werbung in Form von Schreiben, E-Mails oder Anrufen erhalten. Im Rahmen der von uns durchgeführten Anhörung verweisen verantwortliche Stellen oft auf im Internet veröffentlichte Kontaktdaten der betroffenen Personen und vertreten die Auffassung, eine Zusendung von Werbung sei in solchen Fallkonstellationen zulässig, da ein Interesse dieser Personen an den angebotenen Waren und Dienstleistungen schließlich schon aufgrund des Inhalts der von der betroffenen Person ins Internet gestellten Webseite oder ihrer Berufsgruppe bzw. ihrer Tätigkeit vermutet werden könne.

Eine Verarbeitung von personenbezogenen Daten zu werblichen Zwecken kann rechtmäßig sein, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen der betroffenen Person überwiegen.[138] Dabei kann Direktwerbung grundsätzlich ein berechtigtes Interesse der verantwortlichen Stelle darstellen.[139]

Bei im Impressum angegebenen Daten handelt es sich zwar um allgemein zugängliche Informationen. Diese werden jedoch nicht freiwillig, sondern zweckgebunden zur Erfüllung der gesetzlichen Verpflichtung zur Anbieterkennzeichnung gemäß § 5 Telemediengesetz (TMG) veröffentlicht. Mangels Freiwilligkeit und an-

138 Art. 6 Abs. 1 Satz 1 lit. f DS-GVO
139 EG 47 DS-GVO

gesichts der Zweckgebundenheit der Veröffentlichung führt die gesetzlich erforderliche Interessenabwägung regelmäßig dazu, dass die werbliche Nutzung derart erhobener Daten unzulässig ist.[140]

Darüber hinaus ist die Verarbeitung personenbezogener Daten zu Werbezwecken auch dann unzulässig, wenn dem die Wertungen von § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) entgegenstehen. Nach dieser Norm ist insbesondere Werbung durch Fax, automatischen Anruf oder „elektronische Post" wie E-Mails, SMS oder Messenger nur mit vorheriger ausdrücklicher Einwilligung der angerufenen Person zulässig. Gleiches gilt für Telefonwerbung gegenüber Verbraucherinnen und Verbrauchern, wozu beispielsweise auch angestellte Rechtsanwältinnen und Rechtsanwälte gehören. Aber selbst personenbezogene Daten von Gewerbetreibenden dürfen nur ausnahmsweise für Telefonwerbung verwendet werden: Erforderlich ist ein konkretes Interesse der angerufenen Person, das die Annahme einer mutmaßlichen Einwilligung rechtfertigt. Der Umstand, dass ein bestimmter Typ Unternehmen stets Bedarf an bestimmten Leistungen – etwa Telekommunikation – hat, genügt nicht.

Bei bestehendem Geschäftskontakt kann ausnahmsweise Werbung per „elektronischer Post" ohne Einwilligung zulässig sein.[141] Werden Kontaktdaten jedoch nur einem Impressum entnommen, können diese Anforderungen nie erfüllt sein.

Eine Verarbeitung von personenbezogenen Daten aus einem Impressum zu Werbezwecken ist regelmäßig nicht zulässig.

140 Siehe auch Punkt 4.3 der Orientierungshilfe der DSK zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) (abrufbar unter: https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/orientierungshilfen/)

141 § 7 Abs. 3 UWG

9.9 Steuerberatertätigkeit in der Lohnbuchhaltung – Keine Auftragsverarbeitung!

Die Frage, ob Lohnbuchhaltung durch Steuerberaterinnen und Steuerberater Auftragsverarbeitung ist oder in eigener Verantwortlichkeit erfolgt, war bundesweit umstritten und wiederholt Diskussionsgegenstand im Arbeitskreis Wirtschaft der DSK. Mit der Neufassung von § 11 Steuerberatungsgesetz (StBerG) wurde die datenschutzrechtliche Einordnung der Tätigkeit von Steuerberaterinnen und Steuerberatern als datenschutzrechtlich Verantwortliche nunmehr durch den Gesetzgeber klargestellt.

In der Praxis kam es immer wieder zu Diskussionen darüber, ob Steuerberaterinnen und Steuerberater, die Aufgaben der externen Lohnbuchhaltung übernehmen, rechtlich als Auftragsverarbeitende oder als selbst datenschutzrechtlich Verantwortliche einzustufen seien.

Vor der gesetzlichen Neuregelung haben wir die Auffassung vertreten, dass für Steuerberaterinnen und Steuerberater, die sich selbst als Verantwortliche ansahen für die Verarbeitung der personenbezogenen Daten ihrer Mandantschaft und dementsprechende Verträge abschlossen, kein Auftragsverarbeitungsvertrag erforderlich sei. Sofern Steuerberaterinnen und Steuerberater sich dagegen so weit den Weisungen ihrer Mandantinnen und Mandanten unterwarfen, dass man von Auftragsverarbeitung ausgehen konnte, war nach unserer früheren Auffassung ein Auftragsverarbeitungsvertrag abzuschließen.

Mit der steuergesetzlichen Neuregelung hat der Gesetzgeber nunmehr klargestellt, dass Steuerberaterinnen und Steuerberater bzw. Steuerberatungsgesellschaften bei der Erbringung von Leistungen nach dem StBerG stets als datenschutzrechtlich Verantwortliche anzusehen sind und eine Auftragsverarbeitung nicht mehr in Betracht kommt.

§ 11 Abs. 2 Satz 1 und Satz 2 StBerG ist wie folgt neu gefasst:

„Die Verarbeitung personenbezogener Daten durch Personen und Gesellschaften nach § 3 erfolgt unter Beachtung der für sie geltenden Berufspflichten weisungsfrei. Die Per-

sonen und Gesellschaften nach § 3 sind bei Verarbeitung sämtlicher personenbezogener Daten ihrer Mandanten Verantwortliche gemäß Artikel 4 Nummer 7 der Datenschutz-Grundverordnung (EU) 2016/679."

Demnach erfolgt eine Verarbeitung personenbezogener Daten durch Steuerberaterinnen und Steuerberater bzw. Steuerberatungsgesellschaften unter Beachtung der für sie geltenden Berufspflichten weisungsfrei. Dies gilt auch dann, wenn sie im Rahmen ihrer gesetzlichen Pflichten geschäftsmäßig Hilfeleistung in Steuersachen erbringen und dabei personenbezogene Daten ihrer Mandantschaft verarbeiten.

Ausweislich der Gesetzesbegründung[142] sind davon auch das „Buchen laufender Geschäftsvorfälle", die „laufende Lohnabrechnung" und das „Fertigen der Lohnsteuer-Anmeldungen", umfasst, die als weisungsfreie Tätigkeiten angesehen werden. Die Hilfeleistungen der mit der Lohnbuchhaltung beauftragten Steuerberaterinnen und Steuerberater bzw. Steuerberatungsgesellschaften schließen nach Auffassung des Gesetzgebers auch eine jeweils eigenverantwortliche Prüfung und Anwendung der gesetzlichen Bestimmungen ein. Steuerberaterinnen und Steuerberater bzw. Steuerberatungsgesellschaften sind demnach bei der Erbringung von Leistungen nach dem StBerG künftig stets als datenschutzrechtlich Verantwortliche anzusehen.

Steuerberaterinnen und Steuerberater bzw. Steuerberatungsgesellschaften, die geschäftsmäßig Aufgaben der externen Lohnbuchhaltung erbringen, handeln weisungsfrei und sind nach der Neuregelung des § 11 StBerG stets als datenschutzrechtlich Verantwortliche anzusehen.

142 BT-Drs. 19/14909, S. 58

9.10 Speicherung von Kundendaten bei Abbruch eines Registrierungsprozesses

Aus der Praxis

Ein Unternehmen arbeitete mit einem mehrstufigen Registrierungsprozess auf seiner Online-Plattform, in dem zunächst E-Mail-Adresse und Passwort abgefragt wurden und anschließend in drei weiteren Schritten verschiedene zusätzliche Daten. Jeder Schritt wurde mit einem Button „Speichern und weiter" beendet. Dabei wurde darauf hingewiesen, dass die eingegebenen Daten gespeichert werden, damit die Registrierung auch zu einem späteren Zeitpunkt abgeschlossen werden kann. Der Beschwerdeführer hatte die Registrierung im Laufe der Dateneingabe abgebrochen. Später erhielt er trotzdem eine E-Mail von der Plattform.

Bricht jemand einen Registrierungsprozess ab, ist die fortgesetzte Speicherung der eingegebenen personenbezogenen Daten nicht ohne Weiteres zulässig. Zwar besteht ein berechtigtes Interesse von Plattformen, eine Unterbrechung und spätere Wiederaufnahme des Registrierungsprozesses zu ermöglichen. Allerdings ist es hierfür nicht erforderlich, die Daten aller Betroffenen, die den Registrierungsprozess abbrechen, zu speichern. Allein die Tatsache, dass ein Unternehmen über die Speicherung personenbezogener Daten informiert, führt noch nicht dazu, dass diese zulässig ist.[143]

Daher sollte im Registrierungsprozess ein ausdrücklicher Button wie „Abbrechen und Daten löschen" vorgesehen werden, damit der Wunsch auf Abbruch des Prozesses in einfacher und eindeutiger Weise zum Ausdruck gebracht werden kann. Ebenso sollte es einen ausdrücklichen Button wie „Daten speichern, um Registrierung später fortzusetzen" geben; die Speicherfrist ist in diesem Fall angemessen festzulegen. Wenn jemand die Registrierung einfach nur nicht fortsetzt, ohne einen dieser beiden Buttons anzuklicken, muss festgelegt werden, ab welcher Zeit der Untätigkeit ein Abbruch anzunehmen ist. Hierbei kommt es auch darauf an, wie lange das Ausfüllen des jeweiligen Formulars einschließlich der ggf. erforderlichen Zusammenstellung der abgefragten Informationen dauert. Hinzuzurechnen ist eine angemessene Zeitspanne, um etwa spontane Störungen abzudecken.

143 Siehe hierzu auch den Schwerpunktbericht zur Adressvermietung in 1.3

Wenn ein Registrierungsprozess technisch so gestaltet ist, dass eine Speicherung der Daten auf dem Server erst mit Abschluss des Registrierungsprozesses erfolgt, stellt sich das Problem der Löschung nicht. Die Server-Speicherung zur späteren Fortsetzung könnte dann optional angeboten werden.

Bei Registrierungsprozessen sollte es sowohl für die weitere Speicherung als auch für den Abbruch entsprechende Schaltflächen geben. Eine datenschutzfreundliche Alternative wäre eine Server-Speicherung erst am Ende des Registrierungsprozesses.

9.11 Verhaltensregeln nach Art. 40 DS-GVO – Ein Entwicklungsbericht

Viele Unternehmen beklagen sich, dass die Regelungen der DS-GVO sehr allgemein gehalten seien. Für sie ist es in der Praxis oft schwierig einzuschätzen, welche konkreten Datenverarbeitungen zulässig und welche Schutzmaßnahmen erforderlich sind.

Um Unternehmen eine Hilfestellung zu geben, sieht die DS-GVO vor, dass Branchenverbände sog. Verhaltensregeln erarbeiten können, die von der zuständigen Behörde genehmigt werden.[144] Derartige Verhaltensregeln können ausschließlich auf nationaler Ebene oder aber auf EU-Ebene mit daraus folgender EU-weiter Geltung vereinbart und genehmigt werden.

Ziel solcher Verhaltensregeln ist es, die Vorschriften der DS-GVO für einzelne Branchen und deren typische Fallkonstellationen zu konkretisieren und so die Einhaltung der DS-GVO für Unternehmen zu vereinfachen. Die Aufsichtsbehörden prüfen im Genehmigungsverfahren daher zum einen, ob die Verhaltensregeln mit der DS-GVO im Einklang stehen, zum anderen aber auch, ob sie tatsächlich eine Klarstellung oder Vereinfachung der DS-GVO-Vorgaben für die Unternehmen bewirken. Denn darin liegt der Mehrwert solcher Regeln.

144 = Codes of Conduct, siehe Art. 40, 41 DS-GVO

Die Möglichkeit solcher Verhaltensregeln begrüßen wir ausdrücklich. In der Praxis zeigt sich jedoch, dass ihre Schaffung und Implementierung sehr aufwendig sind. Nennenswerte Erleichterungen für Verantwortliche durch Verhaltensregeln werden sich daher erst mittelfristig ergeben. Wir unterstützen die Entwicklung von Verhaltensregeln aber nach Kräften.

Europäische Leitlinien

Der Europäische Datenschutzausschuss (EDSA) hat Anfang 2019 EU-weit geltende Leitlinien verabschiedet, die sowohl die inhaltlichen als auch die formalen Anforderungen an vorgenannte Verhaltensregeln näher definieren.[145] Dies stellt eine wichtige Hilfestellung für Verbände bei der Erarbeitung dar.

Nach diesen Leitlinien muss jeder Verband zwingend eine sog. Überwachungsstelle einrichten oder beauftragen. Solche Überwachungsstellen sind in der DS-GVO vorgesehen.[146] Neben der Kontrolle durch die Aufsichtsbehörden sollen sie sicherstellen, dass die Verhaltensregeln von den betroffenen Unternehmen auch eingehalten werden. Die Überwachungsstellen bedürfen einer Akkreditierung durch eine Aufsichtsbehörde.

Bis zur Verabschiedung der Leitlinien war umstritten, ob die DS-GVO die Einrichtung von Überwachungsstellen für Verhaltensregeln zwingend vorschreibt. Wir haben gemeinsam mit den anderen deutschen Aufsichtsbehörden die Auffassung vertreten, dass die Regelungen der DS-GVO auch die Genehmigung von Verhaltensregeln ohne Überwachungsstelle zulassen. Jedoch sind wir von der Mehrheit der europäischen Aufsichtsbehörden überstimmt worden. Daher können Verhaltensregeln nunmehr erst in Kraft treten, wenn auch eine entsprechend akkreditierte Überwachungsstelle hierfür besteht. Dies bedeutet einen erheblichen zeitlichen und finanziellen Zusatzaufwand für die jeweiligen Verbände. Allerdings besteht so die Möglichkeit, Beschwerden betroffener Personen bei der Überwachungsstelle zu kanalisieren.

145 Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679 (https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12019-codes-conduct-and-monitoring-bodies-under_de)

146 Art. 41 DS-GVO

Akkreditierungskriterien für Überwachungsstellen

Trotz europäischer Leitlinien ist jede Aufsichtsbehörde gesetzlich verpflichtet, Kriterien für die Akkreditierung von Überwachungsstellen aufzustellen und zu veröffentlichen.[147] Vor der Veröffentlichung müssen diese Kriterien jeweils vom EDSA gebilligt werden. Die Aufsichtsbehörden in Österreich und dem Vereinigten Königreich waren die ersten, die dieses Verfahren erfolgreich abgeschlossen haben.

In Deutschland hat der Arbeitskreis Wirtschaft der DSK eine Arbeitsgruppe eingesetzt, um solche Kriterien einheitlich für alle deutschen Aufsichtsbehörden auszuarbeiten. An dieser Arbeit waren wir maßgeblich beteiligt. Die ausgearbeiteten Kriterien wurden im November 2019 von der DSK beschlossen und an den EDSA zur Billigung weitergeleitetet. Wir hoffen, dass wir das Ergebnis bald veröffentlichen können.

Erste Verfahren

Mit ersten Verbänden haben wir intensive Beratungsgespräche geführt. Mittlerweile haben uns zwei dieser Verbände[148] Entwürfe für Verhaltensregeln in ihrer jeweiligen Branche vorgelegt und die Genehmigung beantragt. Dabei hat sich jedoch gezeigt, dass es eine große Herausforderung für die Verbände darstellt, die Regelungen so zu gestalten, dass sie für ihre Mitglieder eine konkrete Handlungserleichterung darstellen. Beide Genehmigungsverfahren konnten wir bisher noch nicht zum Abschluss bringen.

147 Art. 57 Abs. 1 lit. p 1. Alt. DS-GVO

148 ADM – Arbeitskreis Deutscher Markt- und Meinungsforschungsinstitute und Federation of European National Collection Associations. Bei letzterem handelt es sich um einen europäischen Dachverband für Branchenverbände der Kreditmanagement- und Inkasso-Branche. Der Bundesverband Deutscher Inkasso-Unternehmen e. V. ist einer der Mitgliedsverbände.

10 Finanzen

10.1 Einwilligungserklärung der Sparkassen

Der Deutsche Sparkassen- und Giroverband (DSGV) hat eine datenschutzrechtliche Einwilligungserklärung entworfen, die von allen Sparkassen in Deutschland verwendet wurde. Diese lautete:
„Ich möchte individuell und möglichst passgenau beraten, betreut und über Produkte und Aktionen informiert werden: Deshalb bin ich einverstanden, dass die Sparkasse folgende Daten über mich verknüpft, gemeinsam auswertet und verwendet:

1. Personendaten, wie Name, Geburtsdatum, Familienstand, Beruf
2. Kontaktdaten, wie Adresse, E-Mail und Telefonnummer
3. Daten zu meiner Bonität, meiner finanziellen Situation, meiner Risikobereitschaft und zu meinem Kreditrisiko
4. Girokonten-, Debit- und Kreditkartendaten, wie Karten-Nr., Saldo, Kreditrahmen, Zinsen, Umsätze (ohne Verwendungszwecke und Empfänger) oder vergleichbare Daten
5. Depot-, Kredit-, Leasing- und Einlagedaten, wie Produktart, Salden, Zinssätze, Wertpapierentwicklung, Laufzeiten und vergleichbare Daten
6. Daten aus Beratungs- und Servicegesprächen, Vertriebsaktivitäten, Dokumentationen und Erhebungsbögen, Sparkassen-Finanzkonzepten, Produktchecks, sowie vergleichbare Daten
7. Statistische Daten, welche mir mithilfe allgemeiner Kriterien zugeordnet werden können, beispielsweise für die Eignung bestimmter Finanzprodukte nach Altersgruppen
8. Daten aus für mich von der Sparkasse vermittelten Geschäften, wie Deka-Bank Depot, verschiedene Formen des Leasings und Mietkaufs, Bauspar- und Versicherungsverträge und ähnlichen Geschäften
9. Daten von den Verbundpartnern über von mir gehaltene Produkte, wie Versicherungen, Bausparverträge und Finanzdienstleistungen
10. Daten über meine Nutzung digitaler Angebote, die mir die Sparkassen und Verbundpartner jeweils anbieten, wie Aufrufzeiten von Webseiten, Apps oder Newslettern, angeklickte Seiten oder Einträge und vergleichbare Daten“

Außerdem wurde der folgende Hinweis gegeben:
„Wenn Sie nicht einwilligen oder eine Einwilligung zu einem späteren Zeitpunkt widerrufen, wirkt sich dies nicht auf unsere Geschäftsbeziehung aus. Wir können Ihre Daten dann im jeweils gesetzlich zulässigen Umfang verarbeiten (z.B. zur Vertragserfüllung). Auch anderweitige Einwilligungen und Vereinbarungen mit uns oder Dritten werden hiervon nicht berührt."
Mehrere Betroffene haben uns gebeten, die Rechtmäßigkeit der Einwilligungserklärung zu überprüfen. Bundesweit gab es auch Beschwerden, weil einzelne Sparkassen den Betroffenen vorangekreuzte Formulare vorgelegt hatten und einzelne Mitarbeiterinnen und Mitarbeiter im Gespräch behauptet hatten, die Einwilligung sei aufgrund des Geldwäschegesetzes (GwG) erforderlich oder die Sparkasse könne ohne eine entsprechende Erklärung die Geschäftsbeziehung nicht aufrechterhalten.

Da der DSGV seinen Sitz in Berlin hat, haben wir als zuständige Aufsichtsbehörde Verhandlungen mit dem Verband über die Formulierung der Einwilligungserklärung und die Art und Weise der Datenerhebung geführt. Dabei gelang es uns, zu einem tragfähigen Kompromiss zu gelangen. Dieser enthielt im Wesentlichen folgende Vereinbarungen:

- Der DSGV sensibilisiert die Regionalverbände und die Sparkassen dahingehend, dass die Kundinnen und Kunden auf die Freiwilligkeit der Einwilligung hingewiesen werden; die Mitarbeiterinnen und Mitarbeiter der Bank werden angewiesen, sich die Einwilligungserklärungen nicht durch Druck oder die falsche Darstellung von Tatsachen zu beschaffen.

- Die bisher verwendete Einwilligungserklärung wird möglichst zügig durch eine neue Einwilligungserklärung ersetzt.

- In der alten Einwilligungserklärung fehlte die Transparenz für die Kundinnen und Kunden, welche Finanzberatung allein auf gesetzlicher Grundlage beruht und welche nur mit ausdrücklicher Einwilligung erfolgen kann. Die neue Einwilligungserklärung wird nun so formuliert, dass für die Betroffenen transparent ist, wie weit die Datenverarbeitung aufgrund einer gesetzlichen Grundlage erfolgt und ab wann eine Datenverarbeitung nur noch auf eine Einwilligung gestützt werden kann.

- Es wird auf eine gemeinsame Einwilligung zu allen zehn Punkten des Einwilligungskatalogs verzichtet, Betroffene werden zukünftig um eine zusammengefasste Einwilligung zu den Punkten 1 bis 9 gebeten, zu Punkt 10 soll eine eigenständige Einwilligung eingeholt werden. Dies entspricht den Vorgaben des EG[149] 43 Satz 2 DS-GVO, der bei verschiedenen Datenverarbeitungsvorgängen gesonderte Einwilligungen fordert. Die Einwilligung in die Auswertung der individuellen Nutzung digitaler Angebote ist von den anderen Tatbeständen zu trennen, weil es sich insoweit um einen separaten Sachverhalt handelt.

- Bei der Analyse der individuellen Internetnutzung können auch Gesundheitsdaten (Schlafstörungen, Legasthenie etc.) ermittelt werden. Die neue Einwilligung stellt sicher, dass keine sensitiven Daten ohne ausdrücklich erklärten Willen der Kundin oder des Kunden verarbeitet werden.

Die Einigung wurde bereits umgesetzt bis auf die Abtrennung der separaten Einwilligung zu Punkt 10 der Einwilligungserklärung. Dies soll bis Mai 2020 erfolgen.

Unsere Verhandlungen mit dem DSGV haben zu einer deutlichen Verbesserung der von den Sparkassen verwendeten Einwilligungserklärung geführt.

10.2 Hypothekenkredit nur bei Information über Familienplanung?

Aus der Praxis

Kundinnen und Kunden einer Hessischen Volksbank, die sich für einen Hypothekenkredit interessieren, müssen einen Fragebogen ausfüllen, in dem auch Angaben zur Familienplanung zu machen sind. Diese Angabe ist nicht freiwillig, jedenfalls fehlt ein entsprechender Hinweis. Die Bank begründete ihr Vorgehen u. a. damit, dass die Frage nach der Familienplanung auf Empfehlung des Bundesverbands der Deutschen Volksbanken und Raiffeisenbanken e. V. (BVR) erfolge. Wir haben dies zum Anlass genommen, mit dem in Berlin ansässigen Verband ein Gespräch zu führen.

149 Erwägungsgrund

Der Bankenverband trug vor, die Frage zur Familienplanung sei aufgrund von § 511 Bürgerliches Gesetzbuch (BGB), nach dem sich die Bank vor Erbringung der Beratungsleistung u. a. über die „persönliche Situation" der Kundin oder des Kunden zu informieren habe, verpflichtend. Bei der anschließenden Kreditvergabe werde das Beratungsprotokoll zwar berücksichtigt. Die Beantwortung der Frage nach der Familienplanung sei jedoch weder für die Vergabe eines konkreten Kredits noch für dessen Konditionen ein entscheidendes Kriterium.

Eine Rechtsgrundlage für die Frage nach der Familienplanung gibt es vorliegend nicht, die Vorgehensweise der Bank ist deshalb rechtswidrig. Im Rahmen des freiwilligen Beratungsgesprächs hängt es maßgeblich von den Kundinnen und Kunden ab, welche Beratung sie wünschen. Die Frage zur Familienplanung ist deshalb nur dann zulässig, wenn die Betreffenden ausdrücklich auf die Freiwilligkeit der Angabe hingewiesen werden. Eine gesetzliche Verpflichtung zur Abfrage der Familienplanung ergibt sich auch nicht aus § 511 BGB. Die „persönliche Situation" umfasst nur solche Ereignisse, für deren Eintritt zumindest schon konkrete Anhaltspunkte vorliegen. Ansonsten müssten auch andere potenziell eintretende Ereignisse (bspw. pflegebedürftige Verwandte, Krankheit) abgefragt werden. Da die Beantwortung der Frage nach der Familienplanung weder für die Vergabe eines konkreten Kredits noch für dessen Konditionen entscheidend ist, sind die Daten auch nicht zur Durchführung des Kreditvertrags erforderlich.

Eine Einigung mit dem Verband kam nicht zustande. Banken, die das Merkmal Familienplanung abfragen, müssen mit aufsichtsrechtlichen Schritten rechnen.

Die Frage nach der Familienplanung im Rahmen eines Beratungsgesprächs zur Kreditvergabe ist – ohne Hinweis auf die Freiwilligkeit der Angabe – rechtswidrig.

10.3 Wie viele Personalausweise braucht ein Verein für eine Kontoeröffnung?

Aus der Praxis

Ein Verein, der sich für die Interessen der Berliner Polizei einsetzt, wollte ein Bankkonto eröffnen. Der erste Vorsitzende und der Kassenwart des Vereins sollten eine Bankvollmacht erhalten, nicht jedoch die weiteren Vorstandsmitglieder. Der Verein übergab der Bank Personalausweiskopien der Bevollmächtigten, die Steueridentitätsnummer sowie das Vereinsregister. Der Bank wurde außerdem mitgeteilt, dass Rechtsverkehr mit dem Ausland nicht geplant sei.
Die Bank teilte dem Verein mit, dass eine Kontoeröffnung erst erfolgen könne, wenn sie eine Personalausweiskopie von allen Vorstandsmitgliedern erhalte. Hierzu sei die Bank aufgrund des Geldwäschegesetzes (GwG) und der Abgabenordnung (AO) verpflichtet. Der Verein bat uns zu prüfen, ob die Aussage der Bank so zutreffend ist.

Banken sind nach dem GwG verpflichtet, bei der Eröffnung eines Kontos für einen Verein die wirtschaftlich Berechtigten zu identifizieren.[150] Bei gemeinnützigen Vereinen „gilt als wirtschaftlich Berechtigter der gesetzliche Vertreter, geschäftsführende Gesellschafter oder Partner des Vertragspartners“[151] – danach musste die Bank also auch die nicht kontobevollmächtigten Vorstandsmitglieder identifizieren.

Durch den Vereinsregisterauszug verfügte die Bank vorliegend aber schon über den Namen, den Wohnort und das Geburtsdatum der Vorstandsmitglieder. Eine generelle Identifizierung von wirtschaftlich Berechtigten mithilfe von Ausweispapieren sieht das Gesetz nicht vor. Die Identifizierungsmaßnahmen haben sich nach der offenen Formulierung der Risikoabschätzung im Geldwäschegesetz[152] stets am Einzelfall zu orientieren. Die Angemessenheit der Maßnahme richtet sich dabei zunächst nach dem Geldwäsche- und Terrorismusfinanzierungsrisiko der Geschäftsbeziehung.[153] Da im vorliegenden Fall kein besonderes Risiko vor-

150 Siehe § 11 Abs. 1 Satz 1 i. V. m. § 3 Abs. 2 Satz 5 GwG
151 Siehe § 3 Abs. 2 Satz 5 GwG
152 § 11 Abs. 5 Satz 4 GwG
153 Gesetzesbegründung zu § 11 Abs. 5 GwG (BT-Drs. 16/9038, Seite 38)

lag – dieses wurde von der Bank auch nicht vorgetragen – reichte nach dem Geldwäschegesetz die Vorlage des Vereinsregisters aus. Zu derselben Interessenabwägung kommt man bei der Anwendung der Regelungen der AO.

Die Bank war somit nicht berechtigt, von den nicht kontobevollmächtigten Vorstandsmitgliedern Personalausweiskopien zu fordern. Die Bank hat uns zugesagt, künftig entsprechend unserer Rechtsauffassung zu verfahren.

Bei der Eröffnung eines Kontos durch einen Verein dürfen Banken in der Regel nicht die Personalausweiskopien der nicht kontobevollmächtigten Vorstandsmitglieder anfordern.

10.4 Ein gesprächiger Bankmitarbeiter

Ein Bankmitarbeiter empfahl seiner Kundin, die gerade Witwe geworden war, ihre Immobilie zu verkaufen und nannte ihr einen ihm bekannten Makler. Die Kundin hatte jedoch kein Interesse an einem Kontakt. Trotzdem informierte der Bankangestellte den offenbar mit ihm befreundeten Makler darüber, dass in einer bestimmten Straße ein Hauseigentümer verstorben sei und die Witwe mit ziemlicher Sicherheit das Haus verkaufen müsse. Dem Makler gelang es, mit dieser Information die Witwe zu ermitteln und ihr ein Angebot zu unterbreiten. Diese beschwerte sich daraufhin bei uns.

Da der Makler mit der erhaltenen Information in der Lage war, die Betroffene problemlos zu ermitteln, handelt es sich bei dem Hinweis des Bankmitarbeiters um eine Übermittlung personenbezogener Daten der Betroffenen. Diese erfolgte ohne Rechtsgrundlage[154] und war somit rechtswidrig. Die Bank hat dies eingeräumt und den Vorfall gemeldet[155] sowie arbeitsrechtliche Schritte gegen ihren Mitarbeiter eingeleitet. Wir haben gegenüber der Bank eine Verwarnung ausgesprochen.

154 Siehe Art. 6 Abs. 1 DS-GVO
155 Siehe Art. 33 DS-GVO

Banken dürfen nur mit Willen der Betroffenen einen Kontakt zu Maklerinnen oder Maklern herstellen.

10.5 Nachweis der Betreuereigenschaft gegenüber einer Bank

Aus der Praxis

Eine Bank forderte von einem Betreuungsbüro, welches Bankgeschäfte für eine betreute Person durchführen wollte, neben dem Betreuerausweis auch den gerichtlichen Beschluss mit der Begründung für die Anordnung der Betreuung.[156]

Betreuerinnen und Betreuer haben sich im Zusammenhang mit der Betreuung gegenüber Dritten, also etwa Behörden, Ärzten, Kreditinstituten etc. zu legitimieren, um die Interessen der Betroffenen wahrnehmen zu können. Zu diesem Zweck erstellen die Betreuungsgerichte Ausweise. Solche Ausweise enthalten neben der Betreuereigenschaft auch Angaben zu den Aufgabenkreisen der Betreuerin bzw. des Betreuers. Im konkreten Fall war der Betreuer für die Vermögenssorge zuständig.

Während der Betreuungsausweis keine Informationen über die Gründe für die Anordnung der Betreuung enthält, ist in dem Betreuungsbeschluss genau dargestellt, welche körperlichen und/oder psychischen Erkrankungen eine Betreuung erforderlich machen. Diese weitergehenden Informationen benötigt die Bank jedoch nicht, um zu überprüfen, ob die Betreuerin bzw. der Betreuer die betroffene Person bei der Vermögenssorge vertreten kann. Die Anforderung dieser Unterlagen war somit rechtswidrig. Die Bank hat den Fehler eingeräumt und sagte zu, sich künftig nur noch Betreuungsausweise vorgelegen zu lassen.

Die Betreuerin bzw. der Betreuer legitimiert sich gegenüber Dritten ausschließlich durch die Vorlage des Betreuungsausweises.

156 Siehe § 1896 BGB

11 Videoüberwachung

11.1 Südkreuz bleibt Versuchslabor für „intelligente“ Videoüberwachung

Nachdem bereits im Jahr 2018 die S-Bahn-Fahrgäste bei einem Test der Bundespolizei als Versuchskaninchen in Sachen „intelligenter“ Videoüberwachung herhalten mussten,[157] nutzt nun auch die Deutsche Bahn den Bahnhof als Versuchslabor. Seit dem 18. Juni 2019 testet die Deutsche Bahn am Bahnhof Berlin-Südkreuz sog. „intelligente“ Videoanalysesysteme von drei verschiedenen Anbietern.

Ziel der Deutschen Bahn ist es bei dieser zweiten Versuchsreihe, mit der neuen Videotechnologie die Zuverlässigkeit und Pünktlichkeit des Bahnbetriebs zu verbessern und Beeinträchtigungen zu Lasten der Bahnkundinnen und -kunden zu reduzieren. Zur Durchführung von Testszenarien im Bahnhofsbereich spielten bis Ende 2019 Freiwillige rund 1.600 Szenen nach einem festgelegten Drehbuch. Dabei sollte geprüft werden, ob die eingesetzte Bildanalyse-Software in der Lage ist, zweifelsfrei Situationen zu erkennen, die die Qualität, Zuverlässigkeit und Sicherheit des Bahnbetriebs beeinträchtigen könnten.

Für den Test wurden folgende Szenen ausgewählt: Liegende Personen auf dem Bahnsteig, unbefugtes Betreten definierter Bereiche (z.B. Gleisbett), Ansammlung von Personen (z.B. vor Rolltreppen), Bewegung von Personengruppen, Personenzählung und abgestellte Gegenstände. Bei der Auswahl der Testszenarien hat sich die Deutsche Bahn an typischen Situationen orientiert, die in der Vergangenheit zu Störungen im Bahnbetrieb geführt haben. Erkennt die Technik solche Szenen, schaltet sich das jeweilige Kamerabild mit einem Hinweiston auf die für den Test eingerichteten Monitore auf. Soweit eine anlassbezogene Aufschaltung nicht erfolgt, werden die von der jeweiligen Kamera erfassten Bilder dauerhaft in wechselnder zufälliger Folge übertragen. Die Testbereiche im Bahnhof sind durch

157 JB 2018, 4.4

blaue Markierungen gekennzeichnet und werden durch Verantwortliche vor Ort betreut.

Wir haben als zuständige Aufsichtsbehörde für die DB Station&Service AG, die für die Videoüberwachung auf den Bahnhöfen der Deutschen Bahn zuständig ist, dieses Projekt bereits während der Vorbereitung in der Planungsphase eng begleitet und auf die erheblichen Risiken hingewiesen, die bei einer möglichen Erhebung und Verarbeitung biometrischer Daten bestehen.[158]

Die Deutsche Bahn hat uns zugesagt, dass durch die in diesem Versuchsdurchlauf eingesetzte Videotechnik keinerlei biometrische Merkmale betroffener Personen zur Beurteilung der Testszenarien erhoben würden. Um die Datenerhebung und -verarbeitung nachvollziehen und bewerten zu können, haben wir die Deutsche Bahn aufgefordert, uns eine Liste derjenigen Merkmale zuzusenden, die von den Anbietern verarbeitet werden sollten. Dieser Liste war zu entnehmen, dass einige der verwendeten Merkmale nur dazu dienen sollten, festzustellen, ob es sich um einen Menschen handelt oder z.B. um größere Gegenstände, Schatten oder Tiere. Unter diesen Voraussetzungen soll es jedoch nicht zu einer Identifizierung bestimmter natürlicher Personen kommen.

Da der Test mit Freiwilligen durchgeführt wurde, war er datenschutzrechtlich grundsätzlich unbedenklich. Für die Beurteilung, ob eine solche Anwendung nach Beendigung des Tests in den Regelbetrieb übergehen kann, ist ganz entscheidend, inwieweit die Anwendung zur Sicherheit am Bahnhof beitragen kann und wie hoch die Eingriffsintensität in die Persönlichkeitsrechte der Fahrgäste ist.

Auch während der Durchführung des Testbetriebs war die Deutsche Bahn verpflichtet, die Datenschutzgrundsätze einzuhalten. Dies bedeutete zum einen die Sicherstellung eines für die Betroffenen transparenten Verfahrens sowie die fristgemäße Löschung erzeugter Aufzeichnungen. Darüber hinaus waren von den Anbietern der Videotechnologie technische und organisatorische Maßnahmen zur Senkung von Datenschutz-Risiken vorzusehen. Die Deutsche Bahn musste die Umsetzung dieser Anforderungen als Auftraggeberin kontrollieren.

158 JB 2018, 4.4

Während der gesamten Testphase hatte die Deutsche Bahn darauf zu achten, dass keine biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen erhoben und verarbeitet werden, weil dies für die durchgeführten Tests nicht erforderlich war. Bereits bei der Durchführung der Tests mussten die mit der Umsetzung beauftragten Anbieter kontrolliert werden. Die Deutsche Bahn musste sicherstellen, dass die beauftragten Unternehmen die Datenschutzgrundsätze einhalten und überprüfen, ob sie vereinbarte technische und organisatorische Maßnahmen zur Senkung von Datenschutz-Risiken für Betroffene umsetzen. Diese Anforderungen würden erst recht für einen möglichen Regelbetrieb gelten. Auf der Grundlage der Testergebnisse werden wir entscheiden, ob ein datenschutzkonformer Regelbetrieb möglich ist. Bei einer eventuellen Ausschreibung sollte die Wahrung des Datenschutzes Teil der Auswahlkriterien für die Anbieter sein.

11.2 Biometrische Zugangskontrolle bei einem großen Verlagshaus

Ein großes Verlagshaus testet seit August 2019 eine biometrische Zugangskontrolle (Gesichtserkennung) im Rahmen eines Pilotprojekts. Damit soll für Beschäftigte des Unternehmens der Zugang zum Gebäude erleichtert werden. In diesem Zusammenhang werden biometrische Merkmale von solchen Personen erfasst, die einen markierten Teil des Eingangsbereichs betreten. Personen, die zuvor eine Einwilligung erteilt haben, werden von dem Kontrollsystem als zutrittsberechtigt erkannt, und der Zugang wird gewährt.

Grundsätzlich ist eine Einwilligung im Arbeitsverhältnis nur unter sehr engen Bedingungen zulässig, da es durch das bestehende Abhängigkeitsverhältnis regelmäßig an der Freiwilligkeit einer Einwilligung fehlt. Diese Frage drängt sich geradezu auf, wenn eine biometrische Zugangskontrolle flächendeckend für alle Beschäftigten eingeführt werden soll. Im vorliegenden Fall hatten die Beschäftigten zunächst jedoch die Möglichkeit, sich freiwillig für das Pilotprojekt anzumelden. Ein Zugang zum Arbeitsplatz ohne biometrische Kontrolle ist den Beschäftigten weiterhin ohne Einschränkungen möglich. Somit kann zumindest während der Testphase des Pilotprojektes die Freiwilligkeit angenommen werden.

Die Verarbeitung biometrischer Daten derjenigen Personen, die keine Einwilligung erteilt haben, ist hingegen unzulässig.[159] Auch die biometrischen Charakteristika dieser Personen werden jedoch durch das System zunächst auf Basis optischer Sensoren abgebildet, wodurch auch für sie biometrische Merkmale erzeugt werden.[160] Diese Personen werden dann als nicht zutrittsberechtigt identifiziert. Die Bilder werden zwar nach diesem Vorgang automatisch verpixelt, die biometrischen Daten der Betroffenen werden aber zum Zweck des Datenabgleichs dennoch erhoben und verarbeitet.

Um den Test in zulässiger Weise durchzuführen, muss deshalb gewährleistet werden, dass nur Daten derjenigen Personen erfasst werden, die wirksam in die Verarbeitung biometrischer Daten eingewilligt haben. Dies kann z.B. dadurch erreicht werden, dass die Kamera nur auf Knopfdruck einer zugangsberechtigten Person eingeschaltet wird.[161] Vorliegend hatte das Unternehmen zwar bestimmte Randbereiche des Kamerabildes verpixelt. Dennoch konnte nicht gänzlich ausgeschlossen werden, dass Personen, die zufällig den markierten Zugangsbereich durchqueren, ebenfalls biometrisch erfasst werden. Auf unseren Hinweis hin wurden zusätzliche Stellwände um den Bereich der gesichtserkennenden Kameras aufgebaut, um ein zufälliges Erfassen Unbeteiligter zu verhindern.

Wir haben das Unternehmen gebeten, uns nach Abschluss der Testphase über die Ergebnisse zu informieren. Sollte anschließend ein Regelbetrieb angestrebt werden, müsste insbesondere sichergestellt werden, dass die Teilnahme an der biometrischen Zugangskontrolle durch die Möglichkeit einer alternativen Zugangskontrolle freiwillig bleibt, damit entsprechende Einwilligungen wirksam erteilt werden können.

159 Siehe Art. 9 DS-GVO

160 Zu den Einzelheiten und Komponenten biometrischer Erfassung siehe auch das Positionspapier zur biometrischen Analyse der DSK vom 3. April 2019 (insb. S. 11 f.)

161 EDPB, Guidelines 3/2019 on processing of personal data through video devices, Version for public consultation, adopted on 10 July 2019

11.3 Zur Zulässigkeit von Dashcams

Ein in Berlin ansässiges Unternehmen, das seine Dienste zur privaten Personenbeförderung bundesweit anbietet, beabsichtigt, seine Fahrzeugflotte mit sog. Dashcams auszustatten. Im vorliegenden Fall sollen die Kameras innen an der Windschutzscheibe hinter dem Innenspiegel angebracht werden, um das Verkehrsgeschehen vor dem Fahrzeug und somit weiträumig öffentliches Straßenland zu beobachten. Die Aufnahmen sollen einerseits zur Beweissicherung bei Unfällen dienen, andererseits präventiv wirken, indem die Fahrzeugführenden zu vorausschauendem und vorsichtigem Fahren angehalten werden. Inwieweit Letzteres erreicht werden kann, ist allerdings sehr zweifelhaft.

Der Einsatz von Dashcams in Fahrzeugen, die eine anlasslose Daueraufzeichnung ermöglichen, ist im Straßenverkehr in der Regel unzulässig.[162] Der Bundesgerichtshof (BGH) hat aber bereits angedeutet, dass ein datenschutzkonformer Einsatz von Dashcams im Einzelfall möglich sein kann, wenn durch ein technisches System eine automatische periodische Löschung der Aufnahmen nach kurzer Zeit und anlassbezogen realisiert wird.[163]

Vor diesem Hintergrund wurde unter den Aufsichtsbehörden diskutiert, unter welchen Voraussetzungen der Einsatz von Dashcams datenschutzrechtlich zulässig sein könnte.

Letztendlich müssen die mit einer Dashcam aufgezeichneten Daten stets unmittelbar überschrieben werden und eine Speicherung immer mit einem konkreten Aufzeichnungsanlass verbunden sein. Erkennen (Unfall-)Sensoren wie z.B. ein Beschleunigungssensor eine Kollision oder eine starke Verzögerung des Fahrzeugs, dann ist eine Sicherung des letzten Aufzeichnungsintervalls anlassbezogen zulässig. Die Speicherung über einen Zeitraum von 30 Sekunden vor und 30 Sekunden nach einem erkannten Anlass reicht aus, um einen Unfallhergang

162 Positionspapier der DSK vom 21. Januar 2019; BGH, Urteil vom 15. Mai 2018 – VI ZR 233/17

163 Siehe BGH, Urteil vom 15. Mai 2018 – VI ZR 233/17

zu dokumentieren. Nach einer Gesamtvideolänge von 60 Sekunden sind Dashcam-Aufzeichnungen automatisch zu löschen.

Ein bislang noch nicht gelöstes Problem ist die Einhaltung der Transparenzpflichten beim Betrieb einer Dashcam. Für den Fall, dass es aufgrund eines Unfalls zu einer längerfristigen Speicherung personenbezogener Daten kommt, müssen die Unfallbeteiligten hierüber informiert werden. Dies gilt grundsätzlich auch in Bezug auf Personen, die nur flüchtig erfasst werden.

Die Erhebung und Speicherung von Bilddaten beim Einsatz von Dashcams im Straßenverkehr ist nur zulässig, wenn dies ausschließlich anlassbezogen und für einen kurzen Zeitraum von maximal 60 Sekunden geschieht; eine dauerhafte, anlasslose Erhebung und Speicherung ist hingegen nicht zulässig. Die Transparenz der Datenverarbeitung muss gewährleistet werden.

12 Sanktionen

Nach dem Inkrafttreten der neuen datenschutzrechtlichen Regelungen der EU bearbeiteten wir nun die überwiegende Anzahl der Fälle in unserer Sanktionspraxis nach den neuen Bußgeldvorschriften. Regelmäßig betrafen die Fälle die unrechtmäßige Verarbeitung von personenbezogenen Daten.

Wir haben 56 Bußgelder in Höhe von insgesamt 14.808.400 Euro festgesetzt. 16 Zwangsgeldbescheide wurden von uns erlassen. In vier Fällen haben wir einen Strafantrag gestellt.

Bei den Entscheidungen über die Verhängung von Geldbußen und deren Höhe werden von uns in jedem Einzelfall die Ermessenskriterien des Art. 83 Abs. 2 DS-GVO geprüft. Insbesondere sind die konkreten Umstände zu Art, Schwere und Dauer des jeweiligen Verstoßes von Bedeutung. Daneben werden u. a. auch die Folgen des jeweiligen Verstoßes und die Maßnahmen, die von den Verantwortlichen ergriffen worden sind, um die Folgen des Verstoßes abzuwenden oder abzumildern, berücksichtigt. Hilfreiche Orientierung bietet das von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beschlossene Bußgeldkonzept[164].

12.1 N26 Bank GmbH

Die Online-Bank der N26 Bank GmbH führte unrechtmäßig eine sog. „schwarze Liste" ehemaliger Kundinnen und Kunden, weswegen wir ein Bußgeld in Höhe von 50.000 Euro verhängt haben.

Das junge Unternehmen hatte zu Zwecken der Geldwäscheprävention die Vor- und Nachnamen ehemaliger Kundinnen und Kunden auf eine „schwarze Liste" gesetzt, unabhängig davon, ob diese tatsächlich der Geldwäsche verdächtig waren. Die Betroffenen konnten dadurch keine neuen Konten bei der Bank eröffnen.

164 Siehe 1.4

Die N26 Bank GmbH hat die Geldbuße akzeptiert und unserer Behörde gegenüber eine Reihe von Maßnahmen angekündigt, um bisherige organisatorische Mängel zu beseitigen und dadurch den Schutz der Daten ihrer Kundinnen und Kunden zu verbessern. Insbesondere sagte das Unternehmen in diesem Zusammenhang zu, sein Personal im Bereich Datenschutz umfassend aufzustocken und zu schulen.

Unternehmen müssen bei der Umsetzung gesetzlicher Vorgaben zur Datenverarbeitung, wie z.B. vorliegend zur Geldwäscheprävention, strikt auf deren Reichweite achten und dürfen die Datenverarbeitung nur im erlaubten Umfang vornehmen. Anderenfalls drohen empfindliche Bußgelder.

12.2 Delivery Hero Germany GmbH

Die Daten von Kundinnen und Kunden des Lieferdienstes der Delivery Hero Germany GmbH wurden über viele Jahre gespeichert, selbst wenn diese jahrelang nichts mehr bestellt hatten. Dies verstieß gegen die DS-GVO und wurde mit Bußgeldern geahndet.

Die Bußgelder wurden in zwei Bescheiden verhängt. In einem Bußgeldbescheid haben wir 18 Bußgelder wegen Verstoßes gegen die DS-GVO in Höhe von insgesamt 120.000 Euro verhängt. In einem weiteren Bescheid gegen den Lieferservice haben wir zehn Bußgelder nach den alten datenschutzrechtlichen Regelungen in Höhe von zusammen 58.000 Euro festgesetzt. Inklusive der Gebühren betrugen die Bußgelder insgesamt 195.307 Euro. Die Geldbußen ergingen in zwei Bescheiden, da ein Teil der Verstöße noch nach dem vor Wirksamwerden der DS-GVO geltenden Datenschutzrecht zu beurteilen war. Maßgeblich für die Frage, ob ein Verstoß nach alter oder neuer Rechtslage zu bewerten ist, ist der Tatzeitpunkt.

Mit den Geldbußen haben wir diverse datenschutzrechtliche Einzelverstöße des Unternehmens geahndet. Die Mehrzahl der Fälle betraf die Nichtbeachtung der Betroffenenrechte wie das Recht auf Auskunft über die Verarbeitung der eigenen Daten, das Recht auf Löschung der Daten sowie das Recht auf Widerspruch. Nach unseren Feststellungen hatte die Delivery Hero Germany GmbH in mehreren Fällen Konten ehemaliger Kundinnen und Kunden nicht gelöscht, obwohl die Betroffenen längst – in einem Fall seit 2008 – nicht mehr auf der Lieferdienst-Plattform

des Unternehmens aktiv gewesen waren. Auch hatten sich ehemalige Nutzende über unerwünschte Werbe-E-Mails des Unternehmens beschwert. In weiteren Fällen erteilte das Unternehmen gegenüber den beschwerdeführenden Personen die geforderten Selbstauskünfte nicht oder erst, nachdem wir als Aufsichtsbehörde eingeschritten waren.

Die Delivery Hero Germany GmbH hatte uns gegenüber einige der Verstöße mit technischen Fehlern bzw. Mitarbeiterversehen erklärt. Aufgrund der hohen Anzahl an wiederholten Verstößen gingen wir jedoch von grundsätzlichen strukturellen Organisationsproblemen aus. Obwohl wir dem Unternehmen vielfache Hinweise erteilt hatten, waren über einen langen Zeitraum keine ausreichenden Maßnahmen umgesetzt worden, die die pflichtgemäße Erfüllung der Rechte der Betroffenen sicherstellen konnten. Wir haben die Maßnahmen, die von dem Unternehmen ergriffen worden sind, um die Folgen des Verstoßes abzuwenden oder abzumildern, in unseren Bußgeldbescheiden entsprechend berücksichtigt.

Die Delivery Hero-Marken Lieferheld, Pizza.de und foodora wurden am 1. April 2019 von dem niederländischen Konzern Takeway.com übernommen. Die dem Verfahren zugrundeliegenden Verstöße wurden allesamt vor dieser Übernahme begangen. Der neue Eigner hat die Bußgeldbescheide akzeptiert und keine Rechtsmittel eingelegt.

Wer als Digitalunternehmen mit personenbezogenen Daten arbeitet, braucht ein funktionierendes Datenschutzmanagement. Daten von Kundinnen und Kunden sollten nur so lange gespeichert werden, wie diese das Online-Angebot auch regelmäßig in Anspruch nehmen. Das hilft nicht nur, Bußgelder zu vermeiden, sondern stärkt auch das Vertrauen und die Zufriedenheit der Kundschaft.

12.3 Deutsche Wohnen SE

Die von der Deutschen Wohnen SE begangenen Ordnungswidrigkeiten[165] wurden von unserer Behörde mit Bußgeldern in Millionenhöhe sanktioniert.

Die Verhängung von Bußgeldern in dieser Höhe für die Verstöße im Zeitraum zwischen Mai 2018 und März 2019 war zwingend, denn die DS-GVO verpflichtet die Aufsichtsbehörden, sicherzustellen, dass Bußgelder in jedem Einzelfall nicht nur verhältnismäßig, sondern auch wirksam und abschreckend sind.

Anknüpfungspunkt für die Bemessung der Geldbußen war u. a. der weltweit erzielte Vorjahresumsatz des Unternehmens. Für die konkrete Bestimmung der Bußgeldhöhe haben wir sodann unter Berücksichtigung aller be- und entlastenden Aspekte die gesetzlichen Kriterien[166] herangezogen:

Belastend wirkte sich vor allem aus, dass die Deutsche Wohnen SE die beanstandete Archivstruktur bewusst angelegt hatte und die betroffenen Daten über einen langen Zeitraum in unzulässiger Weise verarbeitet wurden.

Bußgeldmildernd haben wir hingegen berücksichtigt, dass das Unternehmen durchaus erste Maßnahmen mit dem Ziel der Bereinigung des rechtswidrigen Zustandes ergriffen und formal gut mit uns zusammengearbeitet hat. Auch dass dem Unternehmen keine missbräuchlichen Zugriffe auf die unzulässig gespeicherten Daten nachgewiesen werden konnten, berücksichtigten wir bußgeldmindernd.

Neben der Sanktionierung des strukturellen Verstoßes verhängten wir gegen die Deutsche Wohnen SE Bußgelder wegen der unzulässigen Speicherung personenbezogener Daten von Mieterinnen und Mietern in 15 konkreten Einzelfällen.

Die Bußgeldentscheidung ist bisher nicht rechtskräftig, da die Deutsche Wohnen SE Einspruch gegen den Bußgeldbescheid eingelegt hat.

165 Siehe auch 9.1

166 Art. 83 Abs. 2 DS-GVO

Datenfriedhöfe sind nicht nur unzulässig und bußgeldbewehrt, sondern erhöhen auch das Risiko missbräuchlicher Zugriffe. Unternehmen sollten daher dringend ihre Datenarchivierung auf Vereinbarkeit mit der DS-GVO überprüfen.

12.4 NPD-Landesverband Berlin

Gegen den Berliner Landesverband der NPD haben wir ein Bußgeld in Höhe von 6.000 Euro wegen rechtswidriger Veröffentlichung personenbezogener Daten festgesetzt.

Der Landesverband veröffentlichte bereits im Februar 2018 auf seiner Internetseite eine mit Google Maps erstellte Karte von Einrichtungen für Asylsuchende in Berlin mit dem Titel: „Eine Übersicht der Überfremdungsschwerpunkte in unserer Stadt". Jedem Standort waren Namen, Telefon- und Handynummern sowie E-Mail-Adressen dort tätiger Personen beigefügt.

Ein 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. Jedoch war es weiterhin leicht möglich, den Quellcode auszulesen und so die in der Karte hinterlegten personenbezogenen Daten weiterhin sichtbar zu machen. Dadurch dauerte der rechtswidrige Zustand an.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit dies durch Gesetz erlaubt ist oder die Betroffenen eingewilligt haben. Eine Einwilligung der betroffenen Personen lag hier nicht vor. Die Verwendung war auch gesetzlich nicht erlaubt.[167] Danach wäre die Verarbeitung von Daten nur dann rechtmäßig, sofern die verantwortliche Stelle dadurch berechtigte Interes-

167 Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO

sen verfolgte und eine Interessenabwägung ergäbe, dass keine schutzwürdigen Interessen der betroffenen Personen überwiegen. 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 Daten der betroffenen Personen wurden gezielt für Flüchtlingsgegnerinnen und -gegner zusammengefasst und sichtbar gemacht. Die schutzwürdigen Belange der betroffenen Personen überwiegen hier eindeutig gegenüber etwaigen Interessen der NPD an der Veröffentlichung dieser Daten.

Der Berliner Landesverband der NPD hat gegen unseren Bescheid Einspruch eingelegt, sodass nun das zuständige Gericht die endgültige Entscheidung hierüber treffen wird.

Unter den Begriff des „Verarbeitens" im Sinne der DS-GVO fällt jede Verwendung von personenbezogenen Daten, so auch das Sammeln, Zusammenfassen und Veröffentlichen von allgemein zugänglichen Daten.

13 Telekommunikation und Medien

13.1 Von der einmaligen Datenübermittlung zum regelmäßigen Datenabgleich – 23. Rundfunkänderungsstaatsvertrag

Mit dem 23. Rundfunkänderungsstaatsvertrag soll der ursprünglich als einmalige Übermittlung geplante vollständige Melderegisterdatenabgleich ab 2022 alle vier Jahre durchgeführt werden. Außerdem sind Beschränkungen der Rechte der betroffenen Personen auf Information[168] und Auskunft[169] vorgesehen.

Bereits der im Jahr 2013 durchgeführte erste vollständige Abgleich der Melderegisterdaten mit den Daten der Rundfunkbeitragszahlenden war auf erhebliche datenschutzrechtliche Bedenken gestoßen.[170] Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte ihre Bedenken damals nur teilweise und auch nur deshalb zurückgestellt, weil lediglich ein einmaliger Meldedatenabgleich vorgenommen werden sollte, um die Umstellung des Gebührenmodells auf einen wohnungsbezogenen Rundfunkbeitrag zu erleichtern. Bereits zu diesem Zeitpunkt bestanden jedoch Zweifel an der Zusicherung des Gesetzgebers, dass es sich dabei um einen einmaligen Vorgang handeln würde. Diese Zweifel wurden bereits im Jahr 2015 bestätigt, als der Gesetzgeber einen erneuten „einmaligen" Meldedatenabgleich beschloss.[171]

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

169 Siehe Art. 15 DS-GVO

170 Siehe die Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) vom 11. Oktober 2010 (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2010/2010-DSK-Systemwechsel_Rundfunkfinanzierung.pdf) und JB 2010, 13.4

171 JB 2015, 15.4

Der jetzt vorgelegte Entwurf für den 23. Rundfunkänderungsstaatsvertrag sieht sogar eine regelmäßige Wiederholung des vollständigen Meldedatenabgleichs in einem vierjährigen Turnus vor. Dieses Vorhaben stellt einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung dar und steht im Konflikt mit den Grundsätzen der Datenminimierung und der Erforderlichkeit.[172]

Bei einem vollständigen Meldedatenabgleich werden im großen Umfang personenbezogene Daten von Personen an die Rundfunkanstalten übermittelt, die überhaupt nicht beitragspflichtig sind, weil sie entweder in einer Wohnung leben, für die bereits durch andere Personen ein Rundfunkbeitrag gezahlt wird, oder weil sie von der Beitragspflicht befreit sind. Zudem werden auch Daten von all denjenigen Einwohnerinnen und Einwohnern erhoben und verarbeitet, die bereits bei der Landesrundfunkanstalt angemeldet sind und regelmäßig ihre Beiträge zahlen. Gerade in diesen Fällen ist von besonderer Relevanz, dass der geplante Meldedatenabgleich sogar mehr personenbezogene Daten abfragt, als die Beitragszahlerinnen und -zahler der Rundfunkanstalt bei der Anmeldung dort mitteilen müssen (z.B. Doktorgrad und Familienstand).[173] Es sollen also flächendeckend personenbezogene Daten an die Rundfunkanstalten übermittelt werden, die zur Beitragserhebung gar nicht notwendig sind.

Die Rundfunkanstalten begründen die Erforderlichkeit eines regelmäßigen Meldedatenabgleichs damit, dass es ohne diese regelmäßige Maßnahme zu einer „Erosion" des Bestands an Beitragszahlenden kommen würde. Vor allem, wenn aus einer gemeinschaftlich genutzten Wohnung diejenige Person, die den Rundfunkbeitrag für diese Wohnung zahlt, auszieht oder verstirbt und sich die übrigen Bewohnerinnen und Bewohner der Wohnung nicht wie vorgeschrieben bei der entsprechenden Rundfunkanstalt anmelden, fielen Beiträge für diese Wohnungen weg.

Die Rundfunkanstalten gehen selbst davon aus, dass ein vollständiger Meldeabgleich letztlich in weniger als einem Prozent der Fälle zu einer zusätzlichen,

172 Art. 5 Abs. 1 lit. a und c, Art. 6 Abs. 1 DS-GVO

173 Siehe § 8 Abs. 4 des Rundfunkbeitragsstaatsvertrages (RBStV) zur Liste der erforderlichen Anmeldedaten

dauerhaften Anmeldung von Beitragspflichtigen führt.[174] Bei einem regelmäßigen vollständigen Meldedatenabgleich würde damit in unverhältnismäßiger Weise in das informationelle Selbstbestimmungsrecht der betroffenen Personen eingegriffen. Dem steht auch nicht entgegen, dass die Landesrundfunkanstalten nach eigenen Angaben durch den zweiten vollständigen Meldedatenabgleich im Jahr 2018 ein zusätzliches Beitragsaufkommen im oberen zweistelligen Millionenbereich erzielt haben.

Zwar ist es zutreffend, dass es in den von den Landesrundfunkanstalten dargestellten Fällen tatsächlich unter bestimmten Umständen zum Wegfall von Einnahmen kommen kann. Diesem Problem sollte jedoch mit spezifisch auf diese Fälle zugeschnittenen Maßnahmen begegnet werden (zu denen grundsätzlich auch die Schaffung neuer Auskunfts- und Verarbeitungsbefugnisse gehören kann), anstatt einfach eine Übermittlung des kompletten Datenbestands der Einwohnermeldeämter in Bezug auf sämtliche volljährigen Bürgerinnen und Bürger an die Landesrundfunkanstalten zu verstetigen.

Die geplanten Regelungen berücksichtigen darüber hinaus auch die Maßstäbe der Datenschutz-Grundverordnung (DS-GVO) nicht in ausreichender Weise: Aufgrund des Anwendungsvorrangs europäischer Verordnungen müssen nationale Datenschutzvorschriften auf eine Öffnungsklausel der DS-GVO gestützt werden können. Das Medienprivileg aus Art. 85 Abs. 2 DS-GVO kommt hier nicht in Betracht, da die Datenverarbeitung zum Zweck des Einzugs von Rundfunkbeiträgen nicht in den Anwendungsbereich dieser Norm fällt.

Bei Regelungen, die auf die Öffnungsklausel nach Art. 6 Abs. 2 und Abs. 3 i. V. m. Art. 6 Abs. 1 lit. e DS-GVO gestützt werden, sind u. a. die Grundsätze der Datenminimierung und Erforderlichkeit zu beachten. Danach dürfen mitgliedsstaatliche Regelungen für die Erfüllung von Aufgaben eingeführt werden, die im öffentlichen Interesse liegen, wenn sie die DS-GVO zwar präzisieren, nicht aber deren Grenzen überschreiten. Regelungen, die sich auf diese Öffnungsklausel beziehen, müssen sich folglich in dem Rahmen halten, den die DS-GVO vorgibt. Bei der vorgeschlagenen Regelung bestehen in dieser Hinsicht erhebliche Bedenken im Hinblick auf die Grundsätze der Datenminimierung und der Erforderlichkeit. Die DSK hat da-

174 Evaluierungsbericht der Länder gem. § 14 Abs. 9a RBStV vom 20. März 2019

her den Gesetzgeber in einem Beschluss aufgefordert, den geplanten regelmäßigen vollständigen Meldedatenabgleich nicht einzuführen.[175]

Der Vorsitzende der DSK 2019 hat zudem die Bedenken der Aufsichtsbehörden in der nicht öffentlichen mündlichen Anhörung der Rundfunkkommission der Länder vorgetragen.

Dessen ungeachtet haben die Regierungschefinnen und Regierungschefs der Länder auf ihrer Konferenz am 6. Juni 2019 einen Entwurf des 23. Rundfunkänderungsstaatsvertrags beschlossen, in dem der vollständige regelmäßige Meldedatenabgleich nach wie vor enthalten ist. Ergänzt wurde allerdings eine Regelung, nach der „zur Wahrung der Verhältnismäßigkeit zwischen Beitragsgerechtigkeit und dem Schutz persönlicher Daten" ein Meldedatenabgleich nicht erfolgen soll, wenn die Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten (KEF) feststellt, dass „der Datenbestand hinreichend aktuell ist". Diese Beurteilung soll die KEF „unter Berücksichtigung der Entwicklung des Beitragsaufkommens und sonstiger Faktoren" vornehmen. Damit wird den o. g. verfassungs- und datenschutzrechtlichen Bedenken jedoch nicht ausreichend Rechnung getragen. Die Ergänzung schafft vielmehr ein zusätzliches verfassungsrechtliches Problem, indem die Entscheidung über die Durchführung eines vollständigen Meldedatenabgleichs an die KEF delegiert wird, ohne dieser irgendwelche Kriterien – abgesehen von der Entwicklung des Beitragsaufkommens – für diese Entscheidung an die Hand zu geben. Solche wesentlichen Entscheidungen in Bezug auf die Verarbeitung personenbezogener Daten aller volljährigen Einwohnerinnen und Einwohner Deutschlands muss jedoch der Gesetzgeber selbst treffen (Gesetzesvorbehalt).

Gleichzeitig sieht der vorgenannte Entwurf auch in anderen Bereichen Einschränkungen der Rechte betroffener Personen nach der DS-GVO vor. Insbesondere sollen die Auskunftsrechte der betroffenen Personen[176] beschränkt werden. Anstatt wie bisher mit einzeln definierten Ausnahmen generell zur Auskunft verpflichtet

175 Beschluss der DSK vom 26. April 2019: „Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen" (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2019/2019-DSK-Beschluss-Meldedatenabgleich_Rundfunkbeitrag.pdf)

176 Siehe Art. 15 DS-GVO

zu sein, soll das Regel-Ausnahme-Verhältnis künftig umgekehrt werden und die Landesrundfunkanstalten nach den neuen Regelungen nur noch hinsichtlich bestimmter und in dem Entwurf abschließend aufgezählter Daten[177] Auskunft erteilen müssen. Diese geplante Beschränkung des Auskunftsrechts ist mit den Bestimmungen der DS-GVO nicht vereinbar: Art. 23 Abs. 1 DS-GVO enthält eine abschließende Aufzählung der Gründe, aus denen der nationale Gesetzgeber Betroffenenrechte über das in der DS-GVO selbst vorgesehene Maß hinaus einschränken kann. Dazu zählt auch der „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedsstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedsstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit".[178] Auf diese Ausnahme will der Gesetzgeber die beabsichtigten Beschränkungen stützen. Die amtliche Begründung zu dem Entwurf vermerkt dazu: „Die vorgenommenen Regelungen stellen sicher, dass die Auskunftspflichten der Landesrundfunkanstalten das Ziel der Datenverarbeitung bzw. die Erfüllung des damit verfolgten öffentlichen Interesses nicht gefährden."[179] Wäre dies eine realistische Gefahr, müssten sich entsprechende Erfahrungswerte aus der Anwendung der derzeit bestehenden Auskunftsverpflichtungen der Landesrundfunkanstalten ergeben. Dies ist jedoch nicht der Fall – es gibt keinerlei Anhaltspunkte dafür, dass diese Auskunftspflichten den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedsstaats gefährdet hätten, wie es Voraussetzung für eine Einschränkung nach Art. 23 Abs. 1 lit. e DS-GVO ist. Insoweit bestehen erhebliche Zweifel, dass die vorgesehene Beschränkung „den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt", wie es in Art. 23 Abs. 1 DS-GVO gefordert wird, und damit an der Vereinbarkeit der vorgesehenen Beschränkung des Auskunftsrechts der betroffenen Personen mit dem Europarecht.

177 Das sind die von den Beitragsschuldnerinnen und Beitragsschuldnern selbst an die Landesrundfunkanstalten gemeldeten Daten, Angaben zu einer etwaigen Befreiung von der Beitragspflicht bzw. zur Ermäßigung des Rundfunkbeitrags, außerdem die Bankverbindung und die Stelle, die die jeweiligen Daten übermittelt hat.

178 Art. 23 Abs. 1 lit e DS-GVO

179 Amtliche Begründung zu Nr. 6 des Entwurfs, S. 7

Zusätzlich von der Auskunft ausgenommen werden sollen zukünftig Daten, „die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen". Das Berliner Datenschutzgesetz (BlnDSG) enthält eine ähnliche Regelung[180]; schon deren Vereinbarkeit mit den Bestimmungen der DS-GVO ist zweifelhaft. Allerdings ist die Regelung dort an weitere Voraussetzungen geknüpft: Danach muss die Auskunftserteilung zusätzlich einen unverhältnismäßigen Aufwand erfordern und eine Verarbeitung der betreffenden Daten durch geeignete technische und organisatorische Maßnahmen muss ausgeschlossen sein. Derartige zusätzliche Voraussetzungen enthält der Entwurf des 23. Rundfunkänderungsstaatsvertrags nicht. Durch die jetzt dort vorgesehene Regelung würden damit die Auskunftsrechte der betroffenen Personen über das sonst für öffentliche Stellen des Landes Berlin geltende Maß hinaus weiter beschränkt, ohne dass dafür eine Notwendigkeit ersichtlich ist. Diese Regelung des Entwurfs sollte daher ersatzlos gestrichen werden. Sie wäre als europarechtswidrige Vorschrift ohnehin nicht anwendbar.

Positiv hervorzuheben ist, dass die bisherige „Vermieterauskunft" für Mietwohnungen[181] gestrichen und der Ankauf von Adressdaten von Privatpersonen im Adresshandel zukünftig ausdrücklich ausgeschlossen werden soll. Diese Befugnisse waren aus Sicht des Datenschutzes von jeher kritisch zu sehen und ihre Streichung ist zu begrüßen. Dabei darf jedoch nicht übersehen werden, dass mit dem geplanten regelmäßigen vollständigen Meldedatenabgleich ein weitaus umfassenderes, datenschutzrechtlich sehr bedenkliches Instrument der Datenerhebung geschaffen werden soll, das das praktische Bedürfnis nach einer Vermieterauskunft und dem Ankauf privater Adressen ohnehin entfallen lässt.

Der Gesetzgeber sollte davon absehen, einen regelmäßigen vollständigen Meldedatenabgleich einzuführen, da gegen die vorgesehenen Regelungen grundsätzliche verfassungsrechtliche Bedenken bestehen und die Maßstäbe der DS-GVO nicht ausreichend berücksichtigt würden. Beschränkungen der Rechte der betroffenen Personen, wie des Informations- und Auskunftsrechts, dürfen nur

180 Siehe § 24 Abs. 1 Satz 3 BlnDSG

181 Siehe § 9 Abs. 2 und 3 RBStV

in dem in Art. 23 DS-GVO vorgesehenen Rahmen erfolgen. Die geplante europarechtswidrige Einschränkung des Auskunftsrechts sollte daher aus dem Entwurf des Rundfunkbeitragsstaatsvertrags gestrichen werden.

13.2 Entscheidung des Europäischen Gerichtshofs zu „Planet 49“

Bereits seit mehreren Jahren verhandeln Gerichte über eine Klage des Bundesverbands der Verbraucherzentralen und Verbraucherverbände (vzbv) gegen den Gewinnspielanbieter „Planet 49“. Dieser hatte in einem Gewinnspiel-Angebot im Internet ein Zustimmungskästchen für Tracking-Cookies eingebunden, das bereits angekreuzt war. Außerdem ließ er sich in den Nutzungsbedingungen für das Gewinnspiel zwangsweise das Recht zur Weitergabe von Daten betroffener Personen an eine große Anzahl von Drittunternehmen einräumen. Der Europäische Gerichtshof (EuGH) hat jetzt entschieden, dass diese Praxis gegen geltendes Datenschutzrecht verstößt.[182]

Der EuGH stellte zunächst klar, dass sowohl unter den Bedingungen der Datenschutzrichtlinie für elektronische Kommunikation (kurz E-Privacy-Richtlinie)[183] als auch nach der DS-GVO eine wirksame Einwilligung in eine Datenverarbeitung dann nicht vorliegt, wenn die Einwilligung durch ein voreingestelltes Ankreuzkästchen erklärt wird, das die Nutzenden zur Verweigerung ihrer Einwilligung abwählen müssen (sog. Opt-out).

Die rechtlichen Anforderungen für das Setzen von Cookies und ähnliche Technologien[184] gelten dabei unabhängig davon, ob es sich bei den im Endgerät gespeicherten oder daraus abgerufenen Informationen um personenbezogene Daten handelt oder nicht.

182 EuGH, Entscheidung vom 1. Oktober 2019 – C-673/17

183 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates

184 Art. 5 Abs. 3, Art. 2 Satz 2 lit. f der Richtlinie 2002/58/EG i. V. m. Art. 2 lit. h der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates bzw. mit Art. 6 Abs. 1 lit. a, Art. 4 Nr. 11 der DS-GVO

Schließlich stellt das Gericht fest, dass Art. 5 Abs. 3 der Richtlinie 2002/58/EG dahingehend auszulegen ist, dass zu den Informationen, die ein Dienste-Anbieter den Nutzenden einer Webseite zu geben hat, auch Angaben zur Funktionsdauer der Cookies zählen sowie die Angabe, welche Empfänger oder Kategorien von Empfängern Zugriff auf die Cookies erhalten.

Die Entscheidung des EuGH hat über den Einzelfall hinaus große Bedeutung: So präzisiert das Gericht in seiner Entscheidung auch die Anforderungen, die an eine Einwilligung zu stellen sind, und stellt klar, dass jede Einwilligung ein aktives Verhalten der Nutzerinnen und Nutzer voraussetzt, das ohne jeden Zweifel eine Zustimmung signalisiert und freiwillig erfolgt. Damit ist (endlich) höchstrichterlich festgestellt, dass die häufig anzutreffende Ausgestaltung von Angeboten im Internet, wonach bereits die reine Weiternutzung des Angebots eine Einwilligung im datenschutzrechtlichen Sinne darstellen soll, rechtswidrig ist.

Ebenfalls rechtswidrig sind damit die ebenfalls weit verbreiteten Ausgestaltungen in Internet-Angeboten, bei denen Einwilligungen durch bereits im Voraus angekreuzte Kästchen eingeholt werden sollen.

Mit der Entscheidung des EuGH könnte auch Bewegung in die bereits seit 2009 durch das Bundesministerium für Wirtschaft und Energie (BMWi) verschleppte Umsetzung der Vorschriften aus Art. 5 Abs. 3 der bisher geltenden E-Privacy-Richtlinie[185] kommen: So hat ein Pressesprecher des Ministeriums bereits nach der Veröffentlichung der Schlussanträge des Generalanwalts in dem Verfahren vor dem EuGH im September angekündigt, dass man nach der Entscheidung des EuGH auch die Rechtslage in Deutschland „unmissverständlich klären" wolle und dass dazu schon entsprechende Änderungen des Telemediengesetzes (TMG)

185 Eine EU-Richtlinie muss in nationales Recht umgesetzt werden; eine EU-Verordnung gilt unmittelbar ohne nationale Umsetzung. Daher waren die Regelungen der bisherigen E-Privacy-Richtlinie durch ein nationales Gesetz umzusetzen. Die derzeit auf europäischer Ebene in der Verhandlung befindliche neue E-Privacy-Verordnung würde hingegen im Falle ihrer Verabschiedung unmittelbar in allen EU-Mitgliedsstaaten gelten.

in Vorbereitung seien. Noch im Herbst 2019 solle dazu ein Gesetzentwurf vorgelegt werden.[186] Dies ist unserer Kenntnis nach bisher nicht erfolgt.

Das Vorhaben des BMWi ist zu begrüßen. Die DSK hatte bereits im April 2018 in ihrer Positionsbestimmung zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018 (Wirksamwerden der DS-GVO) darauf hingewiesen, dass in Bezug auf das TMG ein dringender Novellierungsbedarf besteht und die Regelungen des 4. Abschnitts des TMG nach Inkrafttreten der DS-GVO nicht mehr anwendbar sind.[187]

Das Setzen und Abrufen von Cookies oder anderer Informationen, die in einem Endgerät einer betroffenen Person gespeichert sind, ist in vielen Fällen einwilligungsbedürftig. Das in vielen Internet-Angeboten bisher praktizierte Widerspruchsverfahren reicht nicht aus. Eine datenschutzrechtliche Einwilligung setzt ein aktives Verhalten der Nutzerin oder des Nutzers voraus, das ohne jeden Zweifel eine Zustimmung signalisiert und tatsächlich freiwillig sein muss. Vorab ausgefüllte Ankreuzfelder oder eine reine Weiternutzung eines Angebots stellen keine Einwilligung dar. Zu den Pflicht-Informationen, die Webseitenbetreibende etwa in ihrer Datenschutzerklärung geben müssen, gehören auch die Funktionsdauer von Cookies und die Angabe, ob Dritte Zugriff auf diese Cookies erhalten können. Verantwortliche für Internet-Angebote in Berlin sind aufgerufen, diese Anforderungen in ihren Angeboten unverzüglich umzusetzen, soweit dies nicht schon geschehen ist.

186 Siehe Bericht des netzpolitik.org e.V. vom 11. September 2019: „Wirtschaftsministerium will im Herbst neue Regeln für Online Tracking vorschlagen", https://netzpolitik.org/2019/wirtschaftsministerium-will-im-herbst-neue-regeln-fuer-online-tracking-vorschlagen/

187 Positionsbestimmung der DSK vom 26. April 2018 „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018 (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2018/2018-DSK-Positionsbestimmung_TMG.pdf); vgl. auch die Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien vom März 2019 (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2019-OH-Anbieter_Telemedien.pdf)

13.3 Orientierungshilfe der Aufsichtsbehörden für Telemedien-Angebote

Welche Dritt-Inhalte auf Webseiten unter welchen Bedingungen eingebunden werden dürfen, welche Reichweitenmessungs- und Tracking-Maßnahmen wann zulässig sind, war in der Praxis bisher schwer zu bewerten. Zur Konkretisierung der Positionsbestimmung der DSK vom April 2018[188] zur Verarbeitung personenbezogener Daten durch Telemedien-Anbietende nach Inkrafttreten der DS-GVO hat die DSK im März 2019 eine detaillierte Orientierungshilfe für Telemedien-Angebote (beschränkt auf nicht-öffentliche Stellen) verabschiedet.[189]

Die nach Konsultation betroffener Wirtschaftsverbände und -unternehmen beschlossene Orientierungshilfe stellt zunächst klar, dass mit Inkrafttreten der DS-GVO die datenschutzrechtlichen Vorschriften des TMG im nicht-öffentlichen Bereich wegen des Anwendungsvorrangs der DS-GVO keine Anwendung mehr finden.

Sie enthält darüber hinaus umfangreiche konkretisierende Erläuterungen zur Rechtmäßigkeit der Verarbeitung personenbezogener Nutzungsdaten nach der DS-GVO durch Anbieterinnen und Anbieter von Telemedien. Denn diese verarbeiten Nutzungsdaten für eine Vielzahl von über die reine Vertragserfüllung hinausgehenden Zwecken[190], u. a. um das Angebot nutzungsfreundlich zu gestalten und anzuzeigen, um weitere individuelle Funktionalitäten (z. B. die Warenkorbfunktion) bereitzustellen, um Inhalte von Dritt-Anbietenden einzubinden (z. B. ein Video oder einen Kartendienst), für IT-Sicherheitsmaßnahmen, für Reichweitenmessung und

188 Siehe Fn. 187 und JB 2018, 12.3

189 Siehe Fn. 187

190 Soweit die Verarbeitung von Nutzungsdaten für die Erfüllung des jeweiligen (Nutzungs-)Vertrages zwingend erforderlich ist, ist sie nach Art. 6 Abs. lit. b DS-GVO zulässig. Dieser Erlaubnistatbestand wurde im Hinblick auf die Diskussionen auf europäischer Ebene zur Frage der Anwendbarkeit des Art. 6 Abs. 1 lit. b DS-GVO im Zusammenhang mit der Bereitstellung von Online-Services in der Orientierungshilfe jedoch nicht thematisiert. Mittlerweile hat der Europäische Datenschutzausschuss hierzu Richtlinien verabschiedet, die unter https://edpb.europa.eu/our-work-tools/our-documents/smernice/guidelines-22019-processing-personal-data-under-article-61b_en abgerufen werden können.

statistische Analysen, zu Werbezwecken u. v. m. Abhängig von dem Zweck und der technischen Ausgestaltung werden dabei teilweise auch personenbezogene Daten an Dritte weitergegeben. Für jede einzelne dieser Verarbeitungen muss die Anbieterin oder der Anbieter sicherstellen, dass dafür eine rechtliche Grundlage existiert.

In der Orientierungshilfe werden die Voraussetzungen der praktisch relevanten Erlaubnistatbestände der Interessenabwägung[191] und der Einwilligung[192] ausdifferenziert:

Viele Anbietende stützen die Verarbeitung von Nutzungsdaten auf ihr berechtigtes Interesse gemäß Art. 6 Abs. 1 lit. f DS-GVO. Dabei ist jedoch zu beachten, dass die Vorschrift neben einem berechtigten Interesse der Anbieterin oder des Anbieters voraussetzt, dass „nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person (also der Nutzerinnen und Nutzer, Anm. d. Verf.), die den Schutz personenbezogener Daten erfordern, überwiegen".

Die Orientierungshilfe enthält daher Hinweise für die Ausgestaltung dieser Interessenabwägung, d.h., welche Interessen der Verantwortlichen als berechtigte Interessen i. S. d. Vorschrift anzusehen sind, wie die Erforderlichkeit der Datenverarbeitung zur Wahrung der berechtigten Interessen geprüft wird und was bei der Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Personen im konkreten Einzelfall berücksichtigt werden muss.

Soweit diese Interessenabwägung für eine bestimmte Nutzungsdatenverarbeitung zugunsten der betroffenen Nutzerinnen und Nutzer ausfällt, muss die Anbieterin oder der Anbieter des Telemedienangebots regelmäßig vor der Verarbeitung eine selbstbestimmte und informierte Einwilligung[193] von den jeweiligen Nutzenden einholen oder auf die betreffende Nutzungsdatenverarbeitung verzichten.

Auch die Voraussetzungen der selbstbestimmten und informierten Einwilligung werden in der Orientierungshilfe näher erläutert:

191 Art. 6 Abs. 1 lit. f DS-GVO
192 Art. 6 Abs. 1 lit. a DS-GVO
193 Siehe Art. 7, Art. 4 Nr. 11 DS-GVO

Eine selbstbestimmte und informierte Einwilligung setzt insbesondere voraus, dass die Nutzenden eine echte Wahl haben, ob sie die Einwilligung auf der Grundlage einer nachvollziehbaren und transparenten Information über die beabsichtigten Datenverarbeitungen erteilen oder nicht. Zudem muss die Einwilligung von ihnen durch eine eindeutige bestätigende Handlung erklärt werden. Stillschweigen, vorangekreuzte Kästchen oder Untätigkeit (und Weiternutzung) reichen hierfür nicht aus.[194] Viele sog. Cookie-Banner, die im Internet zu finden sind, geben zwar vor, eine Einwilligung darzustellen. Häufig genügen sie den Anforderungen der DS-GVO jedoch leider nicht.

Wird eine erforderliche Einwilligung nicht ordnungsgemäß erteilt, darf die jeweilige Datenverarbeitung nicht erfolgen. Eine Einwilligung ist bspw. dann erforderlich, wenn das Verhalten der Webseiten-Besucherinnen und -Besucher im Detail nachvollzogen und aufgezeichnet wird, etwa wenn Tastatureingaben, Maus- oder Wischbewegungen erfasst und analysiert werden. Als zulässig eingeordnet werden kann es demgegenüber, wenn eine Webseiten-Betreiberin eine Reichweitenerfassung durchführt und dafür die Zahl der Besucherinnen und Besucher pro Seite, die Gerätetypen und die Spracheinstellungen erhebt.

Uns erreichen immer wieder Beschwerden und Hinweise betroffener Personen auf die unzulässige Nutzungsdatenverarbeitung durch Berliner Anbieterinnen und Anbieter von Telemedien. Wir prüfen diese und haben bereits Verfahren gegen Verantwortliche eingeleitet.

Insbesondere: Einbindung von Dritt-Inhalten

Viele Anbieterinnen und Anbieter von Telemedien binden in ihren Angeboten Inhalte von Dritten für verschiedenste Zwecke ein. Dazu gehören, um nur einige besonders prominente Beispiele zu nennen:

- Werbenetzwerke,
- Schriftarten,
- Videos,
- Kartendienste,

194 Siehe EG 32 zur DS-GVO und 13.2

- Social Plugins wie der „Gefällt mir"-Knopf von Facebook und vergleichbare Schaltflächen anderer Unternehmen sowie
- Nachrichtendienste wie z.B. Twitter.

Diese Einbindung von Dritt-Inhalten ist regelmäßig mit der Übermittlung personenbezogener Nutzungsdaten der Nutzenden an diese Dritten verbunden. Auch dafür bedarf es einer Rechtsgrundlage. Vielfach gehen die Anbietenden in ihren Datenschutzerklärungen davon aus, dass diese Übermittlung ohne Weiteres auf die Bestimmungen des Art. 6 Abs. 1 lit. f DS-GVO gestützt werden kann.

In vielen Fällen kann zwar davon ausgegangen werden, dass die Verantwortlichen ein berechtigtes Interesse – wozu auch kommerzielle Interessen zählen – an der Übermittlung der personenbezogenen Daten der betroffenen Personen haben. Verantwortliche für Telemedien sollten sich jedoch darüber im Klaren sein, dass dies nur der erste Teil der Rechtmäßigkeitsprüfung ist und das Ergebnis der ebenfalls erforderlichen Interessenabwägung bei einer Übermittlung von Nutzungsdaten an Dritte in vielen Fällen zu ihren Ungunsten ausfallen wird, sodass damit für die entsprechende Datenverarbeitung in aller Regel eine Einwilligung der Betroffenen erforderlich ist. Im Hinblick auf ihre Rechenschaftspflicht[195] sollten Anbieterinnen und Anbieter Dritt-Inhalte daher nur dann in ihre Webseite einbinden, wenn sie vorab geprüft und dokumentiert haben, dass die durch die Einbindung ausgelöste Datenverarbeitung vollständig rechtmäßig ist.

Betreiberinnen und Betreiber von Internet-Angeboten, die unzulässig Dritt-Inhalte einbinden, müssen nicht nur mit datenschutzrechtlichen Anordnungen rechnen, sie sollten auch berücksichtigen, dass die DS-GVO für derartige Verstöße hohe Geldbußen androht.

Anbieterinnen und Anbieter von Telemedien sollten ihre Nutzungsdatenverarbeitung umgehend überprüfen. Wer Funktionen nutzt, die eine Einwilligung erfordern, muss entweder diese Einwilligung rechtskonform einholen oder die jeweilige Funktion entfernen. Die rechtswidrige Übermittlung von Nutzungsdaten an Dritte kann u. a. die Verhängung eines Bußgelds nach sich ziehen.

195 Siehe Art. 5 Abs. 2 DS-GVO

13.4 Einsatz von Google Analytics & Co. zur Reichweitenmessung

Viele Betreiberinnen und Betreiber von Webseiten setzen Werkzeuge zur Reichweitenmessung ein. Zu den besonders populären Anwendungen für die Reichweitenmessung zählt das Werkzeug „Google Analytics". Dieses Werkzeug kann jedoch nur noch mit Einwilligung der betroffenen Nutzerinnen und Nutzer rechtskonform eingesetzt werden. Die Einräumung eines Widerspruchsrechts reicht für einen rechtskonformen Einsatz nicht mehr aus.

Der Einsatz von Google Analytics hat die Aufsichtsbehörden für den Datenschutz bereits in der Vergangenheit beschäftigt.[196] Er war unter den damals gegebenen Bedingungen in vielen Fällen ohne Einwilligung insbesondere deswegen möglich, weil er auf die Regelungen zur Auftragsdatenverarbeitung aus dem damaligen Bundesdatenschutzgesetz (BDSG) gestützt werden konnte und damit für die Weitergabe der Daten an Google Inc. keine Rechtsgrundlage erforderlich war.

Eine Auftragsverarbeitung scheidet jedoch dann aus, wenn der Auftragnehmer oder die Auftragnehmerin die Daten auch zu eigenen Zwecken verwendet.

Genau dies ist jedoch bei den jetzt von Google Inc. verwendeten Nutzungsbedingungen der Fall: Dort wird klargestellt, dass Google Inc. die Daten auch für eigene Zwecke verarbeiten darf.[197] Gemäß Art. 28 Abs. 10 DS-GVO handelt es sich beim Anbieter von Google Analytics somit nicht (mehr) um einen Auftragsverarbeiter, auch wenn dieser weiterhin den Vertrag als Auftragsverarbeitung bezeichnet.

Unter diesen veränderten Bedingungen stellt die Einbindung von Google Analytics durch den Webseiten-Betreiber im datenschutzrechtlichen Sinne eine Übermittlung an den Betreiber von Google Analytics dar, die einer Rechtsgrundlage bedarf. Nach den Bestimmungen der DS-GVO und deren Auslegung durch die DSK in der

196 Siehe JB 2011, 12.2, S. 170 ff.

197 Nutzungsbedingungen für Google Analytics (https://marketingplatform.google.com/about/analytics/terms/de/, Stand 17. Juni 2019, Ziffer 6) i. V. m. Google-Datenschutzerklärung (https://policies.google.com/privacy, Stand 15. Oktober 2019, Punkt „Messung der Leistung")

Orientierungshilfe für Anbieter von Telemedien[198] kommt für diese Übermittlung von Nutzungsdaten nur die Einwilligung der betroffenen Personen in Betracht.

Wie bereits in anderem Zusammenhang erwähnt[199], ist eine Einwilligung unabhängig von der Einbeziehung von Auftragsverarbeitenden oder Dritten immer auch dann erforderlich, wenn das Verhalten der Webseiten-Besucherinnen und -Besucher bei einer Reichweitenmessung im Detail nachvollzogen und aufgezeichnet werden kann, etwa wenn Tastatureingaben, Maus- oder Wischbewegungen erfasst werden.

Als ohne Einwilligung zulässig angesehen werden kann es demgegenüber, wenn eine Webseiten-Betreiberin eine Reichweitenerfassung durchführt und dafür die Zahl der Besucherinnen und Besucher pro Seite, die Geräte und die Spracheinstellungen erhebt, auch wenn ein Auftragsverarbeiter dies erledigt.

Die Einwilligung muss in einer Art und Weise erteilt werden, mit der die betroffene Person eindeutig zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Sie muss also wirklich freiwillig und unmissverständlich als Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung erteilt werden und zwar für den konkreten Fall und in informierter Weise.[200] Ergänzend hierzu stellt die DS-GVO klar, dass Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person keine Einwilligung sind.[201] Diese klare Wertung des Gesetzgebers hat auch der EuGH in der Streitsache „Planet49" ausdrücklich bestätigt.[202]

Der Einsatz von Google Analytics kann insbesondere auch nicht mehr auf die vom damaligen Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) im März 2013 veröffentlichten „Hinweise für Webseiten-Betreiber mit Sitz in Berlin, die Google Analytics einsetzen" gestützt werden. Auf diese verän-

198 Siehe 13.3
199 Siehe 13.3
200 Art. 4 Nr. 11 DS-GVO
201 EG 32 DS-GVO
202 Siehe 13.2

derte Situation haben wir bereits im November 2019 in einer Presseerklärung hingewiesen.[203]

Trotzdem stellen wir bei Überprüfungen von Internet-Angeboten immer wieder fest, dass dort Google Analytics und andere Dienste eingesetzt werden, ohne dass die dafür erforderlichen Einwilligungen der Nutzenden eingeholt werden. Uns liegen dementsprechend auch eine Vielzahl von Beschwerden Betroffener und von Hinweisen über die unzulässige Einbindung von Google Analytics und ähnlichen Diensten vor.

Betreiberinnen und Betreiber von Webseiten, die Google Analytics und ähnliche Dienste einsetzen, sollten ihre Angebote umgehend daraufhin überprüfen, ob die gesetzlichen Anforderungen für den rechtskonformen Einsatz erfüllt sind. Wer Funktionen nutzt, die eine Einwilligung erfordern, muss entweder eine Einwilligung einholen oder die Funktion entfernen.

Für den rechtskonformen Einsatz von Google Analytics ist die Einwilligung der Besucherinnen und Besucher der Webseite erforderlich. Betreiberinnen und Betreiber von Webseiten, die Google Analytics weiterhin ohne rechtskonforme Einwilligung einsetzen, setzen sich der Gefahr aufsichtsbehördlicher Maßnahmen aus, wozu auch die Verhängung von Bußgeldern zählen kann.

13.5 „Facebook Custom Audience“-Listenverfahren – Kein Einsatz ohne Einwilligung!

Das sog. „Listenverfahren“ für „Facebook Custom Audience“ ermöglicht es Unternehmen (vor allem Betreiberinnen und Betreibern von Online-Shops), ihre Kundinnen und Kunden bei Facebook gezielt bewerben zu lassen, soweit diese gleichzeitig auch Facebook nutzen.

203 Pressemitteilung der BlnBDI vom 14. November 2019 (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191114-PM-Analyse_Trackingtools.pdf)

Dazu erstellt das werbende Unternehmen eine Liste mit Daten seiner Kundinnen und Kunden, wie z.B. der E-Mail-Adresse und/oder der Telefonnummer. Diese Daten werden „gehasht" (d.h. Einweg-verschlüsselt, wobei die Anwendung der Funktion auf ein bestimmtes Datum oder eine Serie von Daten immer dasselbe Ergebnis ergibt) und danach in das Facebook-Konto des Unternehmens übertragen. Dort werden die Daten durch Facebook mit den ebenfalls gehashten Daten seiner eigenen Kundinnen und Kunden verglichen. Gleichartige Ergebnisse bei der Anwendung der Funktion zeigen dann, dass die jeweilige Person sowohl Kundin oder Kunde des „einmeldenden" Unternehmens als auch von Facebook ist. Auf dieser Grundlage kann das einmeldende Unternehmen dann seinen Kundinnen und Kunden auf Facebook Werbung für seine Produkte oder Dienstleistungen anzeigen oder seine Bestandskundinnen und -kunden von Werbekampagnen für seine Produkte oder Dienstleistungen auf Facebook ausnehmen lassen. Dies kann u. U. für sehr spezifische Zielgruppen erfolgen, die auf der Grundlage der bei Facebook über die jeweiligen Personen bekannten Merkmale herausgefiltert werden können.

Nach den Bestimmungen der DS-GVO ist die Nutzung des Listenverfahrens nur auf Basis einer wirksamen Einwilligung der betroffenen Personen möglich.

Dies hat bereits im Jahr 2018 und vor Inkrafttreten der DS-GVO der bayerische Verwaltungsgerichtshof festgestellt.[204] In diesem Beschluss bestätigt das Gericht eine Entscheidung des Verwaltungsgerichts Bayreuth[205], in der dieses u. a. folgende Feststellungen zum datenschutzkonformen Einsatz des „Facebook Custom Audience"-Listenverfahrens trifft:

- „Gehashte" E-Mail-Adressen sind personenbezogene Daten, da das „Hashen" keine Anonymisierung darstellt.

- Die Weitergabe der „gehashten" E-Mail-Adressen an Facebook für das „Facebook Custom Audience"-Listenverfahren ist eine Übermittlung an Dritte und keine Auftragsdatenverarbeitung.

204 VGH München, Beschluss vom 26. September 2018 – 5 CS 18.1157
205 VG Bayreuth, Beschluss vom 8. Mai 2018 – B 1 S 18.105

- Auch eine Interessenabwägung[206] kann die Übermittlung der „gehashten" E-Mail-Adressen nicht rechtfertigen. Das berechtigte Interesse der verantwortlichen Stelle an der Übermittlung „gehashter" E-Mail-Adressdaten kann auch ohne unverhältnismäßigen Aufwand gewahrt werden, wenn im Einzelfall eine Einwilligung der Betroffenen z. B. im Rahmen eines Bestellvorgangs eingeholt wird. Dem Interesse an der Übermittlung der Daten zu Werbezwecken stehen die überwiegenden schutzwürdigen Persönlichkeitsrechte der Betroffenen gegenüber.

Die Ausführungen der beiden Gerichte beziehen sich zwar auf die Rechtslage vor Inkrafttreten der DS-GVO. Jedoch können die Grundzüge der o. g. Entscheidungen auch auf die Rechtslage in der nachfolgenden Zeit übertragen werden.

Im Ergebnis ist damit eine Verwendung des „Facebook Custom Audience"-Listenverfahrens nur mit vorheriger wirksamer Einwilligung der betroffenen Personen zulässig.

Uns liegen Beschwerden betroffener Personen gegen verschiedene Unternehmen vor, die in der Vergangenheit das „Facebook Custom Audience"-Listenverfahren ohne Einwilligung der betroffenen Personen eingesetzt haben oder dies sogar weiterhin tun. Wir sind dabei, diese Einzelfälle zu untersuchen. Dabei werden wir auch die Einleitung von aufsichtsbehördlichen Maßnahmen einschließlich der Verhängung von Bußgeldern in Erwägung ziehen, insbesondere wenn die betroffenen Unternehmen nach Hinweis auf die Rechtslage den Einsatz des „Facebook Custom Audience"-Listenverfahrens ohne Einwilligung der betroffenen Personen fortführen.

Der Einsatz des „Facebook Custom Audience"-Listenverfahrens ist nur auf Basis einer vorherigen rechtswirksamen Einwilligung der betroffenen Personen zulässig. Die Einräumung eines Widerspruchsrechts reicht nicht aus. Anbieterinnen und Anbieter, die das „Facebook Custom Audience"-Listenverfahren ohne die erforderliche Einwilligung einsetzen, müssen mit aufsichtsbehördlichen Maßnahmen rechnen.

206 Siehe § 28 Abs. 1 Satz 1 Nr. 2 BDSG a. F.

13.6 Facebook-Fanpages: Prüfungen und Entwicklungen

Wer eine Facebook-Fanpage betreibt, verarbeitet personenbezogene Daten in gemeinsamer Verantwortlichkeit mit Facebook[207] Um zu prüfen, ob die daraus folgenden Rechtspflichten eingehalten werden, hatten wir Ende 2018 verschiedene Prüfverfahren gegen Fanpage-Betreibende eingeleitet. Zwischenzeitlich hat das Bundesverwaltungsgericht (BVerwG) entschieden, dass eine Aufsichtsbehörde den Betrieb einer Facebook-Fanpage untersagen darf, insbesondere ohne zunächst gegen Facebook vorzugehen.[208] Auch hat der EuGH seine Rechtsprechung zur gemeinsamen Verantwortlichkeit fortentwickelt. Es ist nun höchstrichterlich bestätigt, dass auch beim Einsatz von Social PlugIns wie Facebooks Like-Button eine gemeinsame Verantwortlichkeit besteht.[209]

In der Folge des EuGH-Urteils zur gemeinsamen Verantwortlichkeit von Facebook und Facebook-Fanpage-Betreibenden haben wir eine Reihe von Prüfverfahren gegenüber Stellen der Landesverwaltung, politischen Parteien sowie Unternehmen und Organisationen eingeleitet, in der es uns zunächst um die Feststellung der Sachlage ging.[210] Die DSK bestätigte in ihrer Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit[211] unsere Bedenken.

Drei der von uns angeschriebenen politischen Parteien verweigerten die Auskunft unter Verweis auf unsere angebliche Unzuständigkeit: Sie hätten mit Facebook vereinbart, dass die irische Datenschutz-Aufsichtsbehörde die federführende Behörde sei und damit die alleinige Ansprechpartnerin auch für Fanpage-Betreibende. Diese Ansicht geht jedoch bereits im Ansatz fehl, weil die DS-GVO das

207 EuGH, Urteil vom 5. Juni 2018 – C-210/16 (Wirtschaftsakademie Schleswig-Holstein)

208 BVerwG, Urteil vom 11. September 2019 – 6 C 15.18 (Wirtschaftsakademie Schleswig-Holstein). Die Entscheidung erging zur alten Rechtslage unter der Datenschutzrichtlinie (Richtlinie 95/46/EG), wesentliche Aussagen sind allerdings auf die neue Rechtslage übertragbar.

209 EuGH, Urteil vom 29. Juli 2019 – C-40/17 (Fashion ID)

210 JB 2018, 1.7

211 https://www.datenschutzkonferenz-online.de/media/dskb/20190405_positionierung_facebook_fanpages.pdf

Konzept der federführenden Aufsichtsbehörde nur dann vorsieht, wenn die Hauptniederlassung eines Verantwortlichen Entscheidungs- und Durchsetzungsbefugnisse gegenüber den anderen Niederlassungen hinsichtlich der Verarbeitung personenbezogener Daten hat.[212] Der Gedanke der federführenden Aufsichtsbehörde bedeutet dabei, dass es eine Ansprechpartnerin auf Seiten der beteiligten Aufsichtsbehörden gibt – nämlich die federführende Aufsichtsbehörde –, die für alle Aufsichtsbehörden bindend handelt. Ebenso gehört dazu aber, dass es auf Seiten der Verantwortlichen nur eine Ansprechpartnerin gibt – nämlich die Hauptniederlassung –, die die Entscheidung der Aufsichtsbehörden in allen Niederlassungen umsetzen kann. Dieses vom Gesetz zwingend vorausgesetzte 1:1-Verhältnis besteht im Fall von Facebook-Fanpages nicht.

Die Artikel-29-Datenschutzgruppe, d.h. die unabhängige europäische Arbeitsgruppe, die sich vor Inkrafttreten der DS-GVO auf europäischer Ebene mit dem Schutz der Privatsphäre und der personenbezogenen Daten beschäftigt hat, hatte die Auffassung vertreten, unter bestimmten Bedingungen könnten gemeinsam Verantwortliche die federführende Aufsichtsbehörde auch vertraglich festlegen.[213] Wir halten die dortige Formulierung für irreführend und setzen uns auf europäischer Ebene im nunmehr neu eingesetzten Europäischen Datenschutzausschuss (EDSA) für eine Korrektur ein.

Für unsere Prüfverfahren in Sachen Facebook-Fanpages ist diese Frage allerdings nicht entscheidend, denn die aufgestellten Bedingungen für eine Festlegung einer federführenden Aufsichtsbehörde durch gemeinsam Verantwortliche sind vorliegend ohnehin nicht gegeben. Hierfür wäre es erforderlich, dass die als Hauptniederlassung im Sinne der Vorschriften über die federführende Aufsichtsbehörde geltende Niederlassung eines gemeinsam Verantwortlichen (hier: Facebook) die Befugnis hätte, für alle gemeinsam Verantwortlichen (alle) Entscheidungen über die Datenverarbeitung zu treffen und umzusetzen. Facebook ist allerdings weder berechtigt zu entscheiden, ob die Fanpage-Betreibenden ihre Fanpage überhaupt betreiben, noch, ob sie die (nach kürzlich durchgeführten Änderungen durch Facebook nur noch geringfügigen) Konfigurationsmöglichkeiten oder die sog. Seiten-Insights-Statistiken nutzen, die nähere statistische Informa-

212 Siehe Art. 55, Art. 56 Abs. 1, Art. 4 Nr. 16 lit. b, Art. 60 Abs. 10 DS-GVO

213 Artikel-29-Datenschutzgruppe, Working Paper 244, S. 8 f.

tionen über die Besucherinnen und Besucher der Fanpage liefern, und auf welche Rechtsgrundlage sie ihr Handeln gründen. Ebenso kann Facebook nicht einseitig über den Umfang der Verarbeitung in gemeinsamer Verantwortlichkeit entscheiden. Alle von uns angeschriebenen Fanpage-Betreibenden bleiben daher in jedem Fall verpflichtet, die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sicherzustellen und uns als zuständiger Aufsichtsbehörde bei Bedarf auch nachzuweisen.[214]

Mit den meisten Fanpage-Betreibenden sind wir allerdings in einen konstruktiven Dialog eingetreten. Zwar konnten sie ihren gesetzlichen Verpflichtungen letztlich durchgängig nicht nachkommen und insbesondere die Rechtmäßigkeit der Verarbeitung nicht nachweisen, vor allem, weil die von Facebook bereitgestellte Vereinbarung über die gemeinsame Verantwortlichkeit nicht ausreichend war. Allerdings hat Facebook Ende Oktober 2019 eine wesentlich überarbeitete Fassung der „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen"[215] bereitgestellt. Diese geht auf eine Vielzahl der Kritikpunkte ein, die die DSK und wir geäußert haben, sodass einige unserer Fragen sich dadurch erledigt haben. In ganz entscheidenden Punkten bleibt diese Ergänzung jedoch ungenügend: Insbesondere sind die Datenverarbeitungen unter gemeinsamer Verantwortlichkeit nicht abschließend, sondern nur beispielhaft beschrieben. Damit Fanpage-Betreibende die Rechtmäßigkeit der Verarbeitung prüfen und ihrer Rechenschaftspflicht nachkommen können, ist es aber zwingend nötig, dass sie den Umfang der Verarbeitung abschließend kennen und sichergestellt ist, dass es keine ihnen unbekannten Verarbeitungen in gemeinsamer Verantwortlichkeit gibt. Zudem bestehen Zweifel, ob die Vereinbarung tatsächlich alle Verarbeitungen in gemeinsamer Verantwortlichkeit abdeckt, und es gibt weitere Mängel im Bereich der Information der betroffenen Personen. Letztere dürften sich allerdings ohne weitere Schwierigkeiten beheben lassen.

Nach wie vor bleiben erhebliche Vorbehalte gegen die Datenverarbeitung im Rahmen von Facebook-Fanpages bestehen, einschließlich Zweifeln daran, ob die von Facebook bereitgestellte Vereinbarung alle Verarbeitungsschritte in gemeinsa-

214 Art. 5 Abs. 2 DS-GVO

215 Informationen der Facebook zu Seiten-Insights (https://de-de.facebook.com/legal/terms/page_controller_addendum)

mer Verantwortlichkeit abdeckt. Darüber hinaus ist denkbar, dass Fanpage-Betreibende auch sanktionsrechtlich für einen eventuellen Datenschutzverstoß von Facebook mit verantwortlich sind. Es ist davon auszugehen, dass uns diese Fragen noch eine Weile beschäftigen werden und zu weiteren Prüfungen und Maßnahmen führen können.

Derzeit können Fanpage-Betreibende ihren gesetzlichen Pflichten zum Nachweis der Rechtmäßigkeit der Verarbeitung nicht nachkommen. Ein legaler Betrieb einer Facebook-Fanpage ist damit momentan kaum möglich. Fanpage-Betreibende, die die damit verbundenen rechtlichen Risiken nicht in Kauf nehmen wollen, sollten Facebook zur Abstellung der Mängel auffordern.

13.7 Social PlugIns und gemeinsame Verantwortlichkeit

Aus der Praxis

Mit Urteil vom 29. Juli 2019 hat der EuGH festgestellt, dass auch beim Einsatz von Social PlugIns wie Facebooks Like-Button eine gemeinsame Verantwortlichkeit der Webseiten-Betreibenden und der Social-Media-Dienste besteht.[216] Im grundlegenden EuGH-Urteil zu den Facebook-Fanpages[217] war der Umstand, dass Fanpage-Betreibende durch den Betrieb ihrer Fanpage Facebook die Verarbeitung der Daten von Fanpage-Besuchenden überhaupt erst ermöglichen, nur eine von mehreren Begründungen für die gemeinsame Verantwortlichkeit von Facebook und Fanpage-Betreibenden. Mit dem Urteil zum Like-Button hat der EuGH nun unmissverständlich festgehalten, dass es für die gemeinsame Verantwortlichkeit genügt, wenn Webseiten-Betreibende Dritt-Inhalte wie Social PlugIns in ihre Webseite integrieren und dadurch die Verarbeitung personenbezogener Daten durch diese Dritten erst ermöglichen.

Dies betrifft neben dem in der EuGH-Entscheidung streitgegenständlichen Like-Button von Facebook nahezu jede Art von fremden Inhalten, die auf einer Webseite eingebunden werden können. Zu denken wäre etwa an Skripte, Schriftarten,

216 EuGH, Urteil vom 29. Juli 2019 – C-40/17; insbesondere Rn. 75 f. (Fashion ID)
217 EuGH, Urteil vom 5. Juni 2018 – C-210/16 (Wirtschaftsakademie Schleswig-Holstein)

Videos, Stadtpläne, Reichweitenmessung und Werbung. Wichtigste Ausnahme ist das Vorliegen einer Auftragsverarbeitung – eine solche ist aber nicht anzunehmen, wenn die Dritten die vermeintlichen Auftragsdaten auch zu eigenen Zwecken verarbeiten dürfen, wie dies etwa bei Google Analytics der Fall ist.[218]

In diesem Fall müssen die gemeinsam Verantwortlichen nicht nur eine Vereinbarung nach Art. 26 DS-GVO abschließen, sondern benötigen auch jeweils eine Rechtsgrundlage für die Verarbeitung der Daten. Als Rechtsgrundlage für die Offenlegung der personenbezogenen Daten der Besucherinnen und Besucher der Webseite gegenüber Dritten kommt in aller Regel nur eine Einwilligung in Betracht.[219]

In der Praxis binden Webseiten-Betreibende in vielen Fällen unzulässig Dritt-Inhalte ein, besonders bei Tracking-Diensten und Werbenetzwerken. Oftmals werden aber auch gedankenlos Standard-Funktionen genutzt, die unzulässig und auch meist unnötig Dritt-Inhalte einbinden, ohne dass dies den Nutzenden zwangsläufig bewusst ist. Verantwortliche müssen jedoch die Rechtmäßigkeit ihrer Datenverarbeitung nachweisen können.[220] Dies setzt die genaue Kenntnis voraus, welche Daten zu welchem Zweck verarbeitet werden, und die Prüfung der Rechtmäßigkeit der Verarbeitung. Immer wieder stellen wir fest, dass Webseiten-Betreibende keinerlei Auskünfte geben können, welche Daten durch den Einsatz von Dritt-Inhalten zu welchem Zweck verarbeitet werden. Es ist deutlich darauf hinzuweisen, dass Nichtwissen nicht vor der Verantwortlichkeit schützt.[221]

Uns liegt eine Vielzahl von Beschwerden über unzulässige Dritt-Inhalte vor, zudem prüfen wir in einigen Fällen von Amts wegen. Die Verfahren sind wegen der oftmals großen Zahl von Dritt-Inhalten sehr aufwendig. Vor dem Hintergrund der damit verbundenen groben Verletzungen des Persönlichkeitsrechts der Besucherinnen und Besucher der Webseiten sind in diesem Bereich sicher Bußgeldverfahren zu erwarten.

218 Siehe dazu 13.4

219 Siehe dazu 13.3 und 13.4

220 Art. 5 Abs. 2 DS-GVO

221 EuGH, Urteil vom 5. Juni 2018 – C-210/16 (Wirtschaftsakademie Schleswig-Holstein) Rn. 40

Wer Dritt-Inhalte auf der eigenen Webseite einbindet, verarbeitet in den meisten Fällen personenbezogene Daten in gemeinsamer Verantwortlichkeit mit der Anbieterin oder dem Anbieter dieser Dritt-Inhalte und muss mit dieser oder diesem eine Vereinbarung nach Art. 26 DS-GVO abschließen. Außerdem ist für die Einbindung von Dritt-Inhalten in den meisten Fällen eine Einwilligung der Besucherinnen und Besucher der Webseiten erforderlich. Webseiten-Betreibende in Berlin sollten ihre Webseiten mit geeigneten Tools auf eingebundene Dritt-Inhalte überprüfen. Dritt-Inhalte müssen entweder entfernt oder rechtskonform gestaltet werden.

13.8 Berlin.de – Serviceportal mit Problemen

Aus der Praxis

Das Stadtportal Berlin.de wird als Public-Private-Partnership zwischen dem Land Berlin und einem privaten Anbieter betrieben; die Werbeschaltungen sind auf einen weiteren Anbieter ausgelagert. Die Verantwortlichkeiten sind intransparent. Umso transparenter sind allerdings die Besucherinnen und Besucher der Webseite: Berlin.de bindet in großem Maßstab Dritt-Inhalte ein, womit notwendig die Übermittlung personenbezogener Daten an die Anbieter der Dritt-Inhalte verbunden ist. Das intensive Tracking jedenfalls auf den inhaltlich nicht durch das Land verantworteten Seiten führt dazu, dass auch sensitive Daten der sich über die Berliner Angebote informierenden Menschen an diverse Dritte weitergegeben werden.

Bereits wer die Startseite von Berlin.de auch nur aufruft, wird automatisch an eine enorme Zahl Dritter gemeldet: Unsere Tests ergaben, dass über 400 Elemente von bis zu 149 unterschiedlichen Servern geladen wurden. Auch wenn unsere Prüfung noch nicht abgeschlossen ist, scheint es sich dabei zum größten Teil um Dienste zu handeln, die Nutzungs-Profile zu Werbezwecken erstellen. Für die Einbindung derartiger Dienste ist zwingend eine Einwilligung der Webseiten-Besuchenden erforderlich, wie die DSK in der Orientierungshilfe für Anbieter von Telemedien detailliert herausgearbeitet haben.[222] Darüber hinaus liegt nach der Rechtsprechung des EuGH eine gemeinsame Verantwortlichkeit von Webseiten-Betreiben-

222 Siehe dazu 13.3

den und Werbeunternehmen vor, die u. a. eine Vereinbarung nach Art. 26 DS-GVO erfordert.[223]

Auf den inhaltlich vom Land Berlin verantworteten Seiten sieht es besser aus, weil dort keine Werbung eingebunden wird. Aber selbst wer etwa über eine Suchmaschine den direkten Weg auf das Serviceportal des Landes (service.berlin.de) gefunden hat, darf sich vor Überwachung nicht sicher fühlen: Auch hier gibt es Nutzungs-Tracking – und wegen der intransparenten Verknüpfung der Verantwortungsbereiche von Land und Privatanbieter kann es schnell passieren, dass der „öffentliche" Teil des Angebots unbemerkt verlassen wird.

Sucht man etwa im Serviceportal des Landes in der Rubrik „Sicherheit und Notlagen" nach dem Begriff „Aidstest", gibt es keine Ergebnisse, obwohl es diverse Informationen des Landes zu diesem Thema gibt – allerdings nicht im Serviceportal. Stattdessen wird angeboten, die Suche auf Berlin.de insgesamt auszuweiten – was, wer einen Aidstest braucht, sicher gerne machen wird. Ohne Hinweis auf die Konsequenzen für den Datenschutz erfolgt die weitere Suche dann im privaten Verantwortungsbereich. Der Suchbegriff – eine sensitive Information, die dem besonderen gesetzlichen Schutz der DS-GVO unterfällt[224] – wird ohne Zustimmung der Suchenden an eine große Zahl Dritter weitergegeben (in unserem Test: 73 Dritt-Server). Das erfolgt teilweise sehr gezielt, teilweise durch die technische Gestaltung. Dies ist ohne ausdrückliche und auf die spezifisch sensitiven Daten bezogene Einwilligung der Webseiten-Besuchenden unzulässig.

Wir führen zu Berlin.de ein Prüfverfahren von Amts wegen durch. Ferner liegen uns diverse Hinweise und Beschwerden zu unzulässigem Tracking und unzulässiger Einbindung von Dritt-Inhalten vor. Die Prüfung wird wegen des großen Aufwands für derartige Prüfungen noch einige Zeit in Anspruch nehmen. Es ist jedoch bereits jetzt festzustellen, dass das Thema Datenschutz bei Berlin.de stiefmütterlich behandelt wird und nicht einmal auf unsere Anfrage intern herauszufinden war, welche personenbezogenen Nutzungsdaten durch wen und zu welchen Zwecken verarbeitet werden. Auch die Rechtsprechung des EuGH zur Frage gemeinsamer Verantwortlichkeit scheint trotz aller Informationen durch uns oder

223 Siehe dazu 13.7

224 Siehe Art. 9 DS-GVO

die diversen Presseveröffentlichungen zum Thema an den Verantwortlichen vorbeigegangen zu sein. Obwohl wir den Senat im hier vorliegenden Fall über unsere Zwischenerkenntnisse informiert haben, hat sich die Situation bisher nicht merkbar verbessert.

Der Fall Berlin.de sollte für Webseite-Betreibende mahnendes Beispiel und Anlass dafür sein, ihre Webseiten kritisch zu überprüfen. Wer Dritt-Inhalte auf der eigenen Webseite einbindet, benötigt meist eine Einwilligung der die Webseite Besuchenden. Besonders kritisch sind Dritt-Inhalte, wenn die Dritten Eingaben wie etwa Suchbegriffe erfahren, die für die Webseiten-Betreibenden unkontrollierbar sensitive Daten im Sinne von Art. 9 DS-GVO enthalten können, oder wenn aus den Inhalten der Webseite auf sensitive Informationen etwa zu Gesundheit oder politischen Einstellungen geschlossen werden kann. Die in solchen Fällen erforderliche ausdrückliche und spezifische Einwilligung wird in der Praxis kaum einholbar sein. Dritt-Inhalte müssen entweder entfernt oder rechtskonform gestaltet werden.

13.9 Löschroutine bei Kundenkonten

Ein Bürger beschwerte sich über die E-Mail einer Kontaktbörse, in der ihm mitgeteilt wurde, dass sein Profil von einer anderen Person angesehen worden war. Der Beschwerdeführer hatte sich sechs Jahre zuvor bei der Plattform zunächst kostenlos registriert und ein Profil angelegt. Kurz darauf hatte er auch eine kostenpflichtige Mitgliedschaft beantragt, die ihm die Kontaktaufnahme zu anderen Mitgliedern ermöglichte. Diese hatte er jedoch kurz darauf wieder beendet. Danach war der Beschwerdeführer auf der Plattform nicht mehr aktiv. Sein Kundenkonto und sein Profil blieben jedoch gespeichert. Der Beschwerdeführer realisierte dies erst, als er sechs Jahre später eine E-Mail mit der Nachricht erhielt, jemand habe sein Profil angesehen.

Die Speicherung von personenbezogenen Daten in kostenlosen Kundenkonten, die über längere Zeit nicht genutzt werden, ist nicht unbegrenzt zulässig.

Unternehmen sind zur Datenminimierung verpflichtet. Sie dürfen personenbezogene Daten nur verarbeiten, soweit dies dem Zweck angemessen und auf das not-

wendige Maß beschränkt ist. Sobald die Verarbeitung nicht mehr erforderlich ist, müssen personenbezogene Daten auch ohne Aufforderung der betroffenen Person gelöscht werden. Dafür müssen Unternehmen, die personenbezogene Daten verarbeiten, entsprechende interne Regelungen und Maßnahmen vorsehen. Sie müssen in regelmäßigen Abständen überprüfen, welche personenbezogenen Daten nicht mehr notwendig sind und gelöscht werden müssen. Hierfür ist es erforderlich, ein Löschkonzept zu erstellen, welche Daten nach welcher Frist gelöscht werden und wann die Fristberechnung beginnt – Informationen, die übrigens auch in der Datenschutzerklärung anzugeben sind.[225]

Wie lange Daten in inaktiven Kundenkonten noch gespeichert werden dürfen, kann nicht pauschal beantwortet werden. Dies hängt von vielen Faktoren des Einzelfalls ab, z.B. davon, welchem Zweck das Kundenkonto dient, wie sensibel die Daten sind, ob Dritte Zugriff darauf haben u. v. m. Hier muss jedes Unternehmen zunächst für sich eine Abwägung und Regelung treffen, die dann von uns überprüft werden kann.

In unserem Fall waren in dem Profil hochsensible Daten gespeichert, z.B. Fotos und Informationen über sexuelle Orientierung und Vorlieben. Außerdem war das Profil für andere Mitglieder der Plattform auch sichtbar. Die Daten wurden also einer Vielzahl von Menschen zugänglich gemacht. Dies stellt einen besonderen Eingriff in die Privatsphäre des Beschwerdeführers dar.

Nach sechs Jahren, in denen der Beschwerdeführer sein Kundenkonto nicht genutzt hatte, konnte das Unternehmen jedenfalls nicht mehr ohne Weiteres davon ausgehen, dass er noch ein Interesse an der Speicherung und Offenlegung derartiger Informationen über ihn haben würde. Das Unternehmen hätte sich zumindest regelmäßig vergewissern müssen, dass eine Aufrechterhaltung des Profils noch gewünscht ist.

Unternehmen, die ihren Kundinnen und Kunden (kostenlos) die Anlage eines Kundenkontos anbieten, müssen insbesondere bei inaktiven Konten regelmäßig überprüfen, ob die Kundinnen und Kunden noch ein Interesse an der Aufrechterhaltung dieser Konten haben und diese Konten andernfalls löschen.

225 Siehe Art. 13 Abs. 2 lit. a bzw. Art. 14 Abs. 2 lit. a DS-GVO

14 Europa

14.1 Anpassung des Berliner Landesrechts an die Datenschutz-Grundverordnung

Aus der Praxis

Die Datenschutz-Grundverordnung (DS-GVO) ist wie jede andere EU-Verordnung unmittelbar anwendbar, sodass es grundsätzlich keines Umsetzungsaktes durch den Berliner Gesetzgeber bedürfte. Gleichwohl enthält die DS-GVO in bestimmten Teilen Ausnahmebereiche, in denen der Landesgesetzgeber berechtigt und verpflichtet ist, ausfüllende Regelungen zu erlassen. Dies betrifft insbesondere die Schaffung von Rechtsgrundlagen für die Datenverarbeitung öffentlicher Stellen. Auch kann der Gesetzgeber unter bestimmten Voraussetzungen die Betroffenenrechte beschränken. Eigentlich hätten diese Anpassungen des Landesrechts an die DS-GVO spätestens bis zum 25. Mai 2018 erfolgen müssen. Der aktuelle Zeitplan sieht vor, dass das Gesetzgebungsvorhaben bis Mitte des Jahres 2020 abgeschlossen ist.

Fast zwei Jahre nach Ablauf der Frist ist der Gesetzgeber endlich auf der Zielgeraden. Der Senat hat einen Entwurf für ein Artikelgesetz erstellt, der die notwendigen Änderungen im Berliner Landesrecht zusammenfassen und dem Abgeordnetenhaus von Berlin zur Beschlussfassung vorgelegt werden soll. Federführend zuständig für die Erstellung eines Referentenentwurfs ist die Senatsverwaltung für Inneres und Sport. Die jeweils inhaltlich zuständigen Senatsverwaltungen arbeiten der Senatsverwaltung für Inneres und Sport also zu.

Der Referentenentwurf sieht vor, dass insgesamt ca. 80 Berliner Gesetze und Verordnungen geändert werden. Unsere Behörde war bei der Erstellung des Gesetzentwurfs zumindest ansatzweise beteiligt und hat sowohl die Senatsverwaltung für Inneres und Sport als auch einzelne andere Senatsverwaltungen bei spezifischen Fragen beraten.

In unseren Stellungnahmen haben wir insbesondere moniert, dass der Referentenentwurf an verschiedenen Stellen über das Ziel hinausgeschossen ist und der Verwaltung mehr Verarbeitungsbefugnisse einräumt, als zur Aufgabenerfüllung

erforderlich wären.[226] Außerdem haben wir uns gegen Einschränkungen der Betroffenenrechte der Bürgerinnen und Bürger gewandt, die ebenfalls nur in sehr engen Grenzen zulässig sind, die teilweise überschritten wurden.[227] Leider wurden in der Referentenfassung des Gesetzentwurfs nicht alle unsere Vorschläge berücksichtigt. Dies ist nicht nur ein datenschutzpolitisches Problem, sondern verstößt auch gegen höherrangiges Europarecht, da die Öffnungsklauseln der DS-GVO in unzulässiger Weise überdehnt werden. In besonderer Weise gilt dies auch in Bezug auf sensitive Daten, an deren Verarbeitung die DS-GVO besonders hohe Anforderungen stellt, da sie mit einem besonders tiefen Eingriff in das Persönlichkeitsrecht von Menschen verbunden ist.[228]

Positiv ist demgegenüber, dass in dem Gesetzentwurf ein Anhörungsrecht unserer Behörde vor dem Abgeordnetenhaus wieder vorgesehen ist, das in den ersten Gesetzgebungsvorgängen nach Wirksamwerden der DS-GVO entfallen war. Allerdings gilt dies nur in unserer Eigenschaft als Beauftragte für den Datenschutz. Im Bereich der Informationsfreiheit fehlt ein solches Recht ebenso wie z.B. ein Beanstandungsrecht[229]. Hier sollte auch die Unterstützungspflicht der öffentlichen Stellen entsprechend normiert werden. Ohne diese Befugnisse ist eine sachgerechte Erfüllung der Aufgaben nach dem Informationsfreiheitsgesetz nicht möglich.

Ein anderer wichtiger Bereich, der in dem aktuellen Gesetzgebungsvorhaben völlig außen vor gelassen wird, ist der Bereich Polizei und Justiz. Bereichsspezifische Regelungen zur Umsetzung der sog. JI-Richtlinie[230] fehlen. Auch diese bereichsspezifischen Regelungen – insbesondere das Allgemeine Sicherheits- und Ordnungsgesetz (ASOG) – müssen dringend an den europäischen Rechtsrahmen angepasst werden.

226 Siehe Art. 6 Abs. 1 lit. c, e Abs. 2, Abs. 3 DS-GVO

227 Siehe Art. 23 DS-GVO

228 Art. 9 DS-GVO

229 Siehe § 13 Abs. 2 Satz 1-3 BlnDSG

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

Der Senat von Berlin hat einen Gesetzentwurf auf den Weg gebracht. Wir werden uns im Gesetzgebungsprozess weiter dafür einsetzen, dass die Datenschutzrechte der Bürgerinnen und Bürger auch bei der Datenverarbeitung durch die öffentliche Verwaltung des Landes Berlin gewahrt bleiben. Es ist zu hoffen, dass der Entwurf entsprechend überarbeitet und dann möglichst bald verabschiedet wird, da er wichtige Regelungen zur Anpassung des Berliner Landesrecht an die DS-GVO enthält. Das gilt auch für den Bereich der Polizei und Justiz sowie der Informationsfreiheit.

14.2 Wie entsteht eine Leitlinie des Europäischen Datenschutzausschusses?

Mit Wirksamwerden der DS-GVO hat auch der sog. Europäische Datenschutzausschuss (EDSA) seine Arbeit aufgenommen. In diesem Gremium sind Datenschutzaufsichtsbehörden aller europäischen Mitgliedsstaaten sowie der Europäische Datenschutzbeauftragte vertreten.[231] Eine wichtige Aufgabe besteht darin, allgemeine Leitlinien zur Interpretation der DS-GVO herauszugeben. Damit soll Klarheit hinsichtlich der einheitlichen Auslegung unbestimmter Rechtsbegriffe in den Datenschutzgesetzen der EU-Mitgliedsstaaten geschaffen werden. Eine solche Leitlinie, die unsere Behörde federführend betreut hat, ist die Leitlinie zur Videoüberwachung.

Wer viel in Europa verreist und darauf achtet, stellt schnell fest, dass – obwohl wir mit der DS-GVO jetzt ein unmittelbar geltendes einheitliches Datenschutzrecht haben – die Videoüberwachung vielerorts ganz unterschiedlich gehandhabt wird. An manchen Orten scheinen uns Kameras auf Schritt und Tritt zu verfolgen und in anderen EU-Mitgliedsstaaten kann man sich weitgehend frei und unbeobachtet bewegen. Auch die Maßnahmen, wie eine Videoüberwachung transparent gemacht wird, scheinen stark zu variieren.

Dies liegt weniger an den Kosten für solche Kameras, die mittlerweile überall günstig zu haben sind, sondern vielmehr daran, dass Datenschutzgesetze sehr

231 Siehe 14.3

unterschiedlich ausgelegt werden. Zunächst ist festzustellen, dass die DS-GVO keine speziellen Regeln zur Videoüberwachung enthält. Vielmehr muss die Videoüberwachung an der Generalklausel des Art. 6 Abs. 1 lit. f DS-GVO gemessen werden. Diese Vorschrift sieht eine Abwägung zwischen den Interessen der für die Überwachung Verantwortlichen und den Interessen und Grundrechten der Beobachteten vor. Diese Interessensabwägung wird von den jeweils zuständigen Aufsichtsbehörden unterschiedlich durchgeführt. Um eine einheitliche Handhabung im Bereich der Videoüberwachung zu fördern, hat der EDSA beschlossen, eine diesbezügliche Leitlinie zu erlassen.

Da wir die Freiheit, sich in der Öffentlichkeit auch unbeobachtet bewegen zu können, für ein besonderes hohes und schützenswertes Gut halten, hat unsere Behörde sich in dieser Angelegenheit als Hauptberichterstatterin gemeldet. Unser Ziel war es dabei, ein möglichst hohes Datenschutzniveau für Betroffene zu erreichen bzw. zu erhalten und gleichzeitig für die Unternehmen klare Vorgaben zu machen, damit diese sich besser auf die neue Rechtslage einstellen können.

Als Hauptberichterstatterin hatten wir zunächst die Aufgabe, ein Konzept zu entwickeln und in einer Arbeitsgruppe des Ausschusses vorzustellen. Danach haben wir gemeinsam mit den Co-Berichterstattern aus Frankreich, Schweden, Tschechien, Polen und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen ersten Entwurf erstellt, der mit den übrigen europäischen Datenschutzaufsichtsbehörden in besagter Arbeitsgruppe diskutiert wurde. Nach vielen Sitzungen und mühseligen Verhandlungen hat sich die Arbeitsgruppe schließlich auf einen Entwurf geeinigt, der am 9. Juli 2019 im Plenum des EDSA angenommen wurde.

Unterstützt wurden wir während des gesamten Prozesses immer wieder auch von Aufsichtsbehörden anderer Bundesländer. Die Einbindung der anderen deutschen Aufsichtsbehörden ist nicht nur aus Gründen der Arbeitsteilung wichtig. Da die deutschen Aufsichtsbehörden im EDSA – wie alle anderen Mitgliedsstaaten – nur eine Stimme haben, muss eine entsprechende Meinungsbildung vorab auf nationaler Ebene erfolgen. Hilfreich war in diesem Fall die Existenz eines eigenen Arbeitskreises zu Fragen der Videoüberwachung auf der Ebene der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). In diesem Arbeitskreis wurden immer wieder Zwischenergebnisse präsentiert, sodass die Ex-

pertise der Mitglieder aus Bund und Ländern optimal abgerufen werden konnte und eine enge Rückkopplung zwischen europäischer und nationaler Ebene problemlos möglich war.

Nach der Annahme durch den EDSA war der Prozess der Erstellung der Leitlinie zur Videoüberwachung aber noch nicht beendet. Im Anschluss wurde eine sog. Public Consultation durchgeführt. Bei dieser Form der Öffentlichkeitsbeteiligung haben Interessenvertreterinnen und -vertreter aus Wirtschaft, Politik und Zivilgesellschaft, aber auch interessierte Privatpersonen die Gelegenheit, ihre Ansichten und Anliegen schriftlich vorzutragen und Änderungsvorschläge zu machen. Zu dieser Leitlinie haben uns ca. 100 Stellungnahmen erreicht. Die meisten kamen von Unternehmen und Unternehmensverbänden aus ganz Europa, aber auch aus Asien. Diese Stellungnahmen haben wir gemeinsam mit den Co-Berichterstattern ausgewertet und die Ergebnisse den anderen europäischen Aufsichtsbehörden in der Arbeitsgruppe des EDSA vorgestellt und diskutiert. Am Ende dieses aufwendigen Prozesses steht die Billigung der Änderungsvorschläge durch den EDSA und die endgültige Verabschiedung der Leitlinien, die kurz nach Ende des Berichtszeitraums Ende Januar 2020 erfolgt ist.

Die Erarbeitung von Leitlinien auf europäischer Ebene ist in jedem Einzelfall ein langer und mühsamer Prozess, der viel Abstimmung und Koordination auf nationaler und EU-Ebene bedarf. Gleichwohl ist er alternativlos, da die DS-GVO viele auslegungsbedürftige Generalklauseln enthält. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit setzt sich dabei aktiv für ein hohes Datenschutzniveau für die Bürgerinnen und Bürger und gleichzeitig für klare und handhabbare Regeln für die Betreiberinnen und Betreiber von Videokameras ein.

14.3 Neues aus Europa – Überblick über die Arbeit des Europäischen Datenschutzausschusses

Spätestens seitdem die DS-GVO wirksam wurde, ist das Datenschutzrecht ein europäisches Gemeinschaftsprojekt von allen EU-Mitgliedsstaaten. Das erfordert eine größere Bereitschaft zur Kommunikation und Kooperation über die Anwendung der Datenschutzvorschriften unter den deutschen Aufsichtsbehörden einerseits und unter den europäischen Aufsichtsbehörden andererseits.

Eine besondere Bedeutung kommt bei den vielfältigen Abstimmungsnotwendigkeiten dem EDSA zu, der eine unabhängige europäische Institution ist und seinen Sitz in Brüssel hat. Der EDSA stellt die einheitliche Anwendung der DS-GVO in der Europäischen Union sicher und fördert die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden untereinander. Er besteht aus dem Europäischen Datenschutzbeauftragten sowie den Leiterinnen und Leitern der EU-Aufsichtsbehörden bzw. deren Vertreterinnen und Vertretern. Die deutsche Datenschutzaufsicht hat nach dem Willen des deutschen Gesetzgebers im EDSA nur einen stimmberechtigten Vertreter bzw. eine Vertreterin sowie einen Stellvertreter bzw. eine Stellvertreterin, obwohl es in Deutschland aufgrund unseres föderalen Systems mehrere Datenschutzaufsichtsbehörden gibt.[232] Stimmberechtigter Vertreter im EDSA ist der Bundesbeauftragte für Datenschutz und Informationsfreiheit, die Stellvertretung steht einer oder einem Landesdatenschutzbeauftragten zu, um so die Landessicht auch unmittelbar auf der europäischen Ebene einbringen zu können. Dies ist von besonderer Bedeutung vor allem deswegen, weil die Zuständigkeiten zwischen Bund und Ländern klar getrennt sind und gerade der Bereich der Wirtschaft, der einen Großteil der vom EDSA beratenen Fälle ausmacht, Ländersache ist. Leider hat der Bundesrat auch über zwei Jahre nach Inkrafttreten dieser gesetzlichen Regelung noch keine Person aus den Reihen der Landesdatenschutzbehörden nominiert. Kommissarisch nimmt derzeit der Hamburger Datenschutzbeauftragte weiterhin diese Funktion wahr.

232 § 17 Bundesdatenschutzgesetz (BDSG)

Zu den Aufgaben des EDSA gehört es, allgemeine Anleitungen im Sinne von Stellungnahmen, Leitlinien, Empfehlungen oder auch konkrete Handreichungen wie z.B. zu sog. „bewährten Verfahren“[233] herauszugeben, in denen datenschutzrechtliche Begriffe geklärt werden. Der EDSA berät außerdem die Europäische Kommission in allen Fragen, die mit dem Schutz personenbezogener Daten und der Änderung der Datenschutzvorschriften im Zusammenhang stehen. Weiterhin fördert der EDSA die Zusammenarbeit sowie den wirksamen Austausch von Informationen und Erfahrungen zu bewährten Verfahren zwischen den Aufsichtsbehörden. Auch in Streitfällen zwischen den europäischen Aufsichtsbehörden kann der EDSA tätig werden und einen verbindlichen Beschluss erlassen. In Fällen, in denen es um eine Angelegenheit mit allgemeiner Geltung geht, kann er eine Stellungnahme veröffentlichen. In einem Jahresbericht berichtet der EDSA jedes Jahr über seine Aktivitäten.

Der Ausschuss hat mehrere Unterarbeitsgruppen, in denen sich Mitarbeiterinnen und Mitarbeiter der Aufsichtsbehörden der EU-Mitgliedsstaaten sowie des Europäischen Datenschutzbeauftragten in Brüssel regelmäßig treffen, um gemeinsame Leitlinien und andere Dokumente zu erarbeiten. In den Arbeitsgruppen zu Themengebieten wie bspw. Vollstreckungsverfahren, Zusammenarbeit, Technologie, Soziale Medien oder Bußgeldverfahren findet die inhaltliche Arbeit auf der Grundlage von Problemfällen und Leitfragen statt. In diesen Arbeitsgruppen wird kompromissorientiert diskutiert und produktiv gestritten, um Antworten zu konkreten und anwendungsorientierten Fragen im Zusammenhang mit der Umsetzung des Datenschutzes in der EU zu finden. Die Ergebnisse der Fachberatungen werden anschließend im Plenum des EDSA diskutiert und verabschiedet.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit vertritt die Aufsichtsbehörden der Länder in einer ganzen Reihe von EU-Arbeitsgruppen und hat so an zahlreichen Leitlinien mitgewirkt. Da unsere Behörde jedoch nicht in allen Arbeitsgruppen vertreten sein kann, arbeiten wir eng mit den Aufsichtsbehörden anderer Bundesländer und des Bundes zusammen. Das bedeutet, dass wir unsere Positionen über die jeweiligen Vertreterinnen und Vertreter in den Arbeitsgruppen einbringen, wenn wir nicht selbst dort vertreten sind.

233 Engl. „Best practice“. Der Begriff bezeichnet bewährte, optimale bzw. vorbildliche Methoden, Praktiken oder Vorgehensweisen.

Zu den wichtigsten Leitlinien, die in Arbeitsgruppen des EDSA erarbeitet und im Plenum verabschiedet wurden, zählt eine Leitlinie, die sich mit Verträgen über Online-Dienste befasst.[234] Außerdem wurde eine Leitlinie über sog. Verhaltensregeln (Codes of Conduct) und Überwachungsstellen gemäß der Verordnung 2016/679 verabschiedet, die eine praktische Orientierungshilfe in der Auslegung und in der Anwendung der Art. 40 und 41 DS-GVO darstellt.[235] Diese Leitlinie zielt darauf ab, Verfahren und Regeln für die Einreichung, Genehmigung und Veröffentlichung von Verhaltensregeln für bestimmte Wirtschaftszweige auf nationaler und europäischer Ebene zu erläutern. Bereits angenommen – aber noch Gegenstand einer Öffentlichkeitsbeteiligung – sind die Leitlinien zur Videoüberwachung[236], zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie zum „Recht auf Vergessenwerden" im Zusammenhang mit Internetsuchmaschinen.[237]

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit wirkt an den Leitlinien, Empfehlungen und sonstigen Dokumenten des Europäischen Datenschutzausschusses mit. Durch unsere Mitarbeit in vielen der Arbeitsgruppen des Ausschusses setzen wir uns für ein hohes Datenschutzniveau EU-weit ein.

234 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects vom 8. Oktober 2019

235 Leitlinien 1/2009 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679 vom 4. Juni 2019, S. 6

236 Siehe 14.2. Hinweis: Diese Leitlinie wurde nach Abschluss der Öffentlichkeitsbeteiligung unmittelbar nach Ende des Berichtszeitraums am 29. Januar 2020 im EDSA verabschiedet.

237 Alle Leitlinien können Sie abrufen unter: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de und – soweit in deutscher Sprache verfügbar – auch unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitlinien/

14.4 Datenschutz-Grundverordnung vs. Berliner Verfassung

Mit Wirksamwerden der DS-GVO wurde europarechtlich verbindlich die völlige Unabhängigkeit der Datenschutzaufsichtsbehörden festgelegt. Die Verfassung von Berlin (VvB) hat diese Entwicklung noch nicht nachvollzogen.

Derzeit lautet Art. 47 Abs. 1 Verfassung von Berlin (VvB) wie folgt:

„Zur Wahrung des Rechts der informationellen Selbstbestimmung wählt das Abgeordnetenhaus einen Datenschutzbeauftragten. Er wird vom Präsidenten des Abgeordnetenhauses ernannt und unterliegt dessen Dienstaufsicht."

Demgegenüber regelt Art. 52 Abs. 1 DS-GVO, dass jede Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig handelt. Dieses wird durch Art. 52 Abs. 2 DS-GVO, der die Weisungsfreiheit ausdrücklich und umfassend konstituiert, konkretisiert.

Das Erfordernis der Unabhängigkeit der Datenschutzbehörden aus Art. 52 Abs. 1 DS-GVO findet seine primärrechtliche[238] Verankerung im Vertrag über die Arbeitsweise der Europäischen Union (AEUV)[239] und in der Charta der Grundrechte der Europäischen Union (GRCh)[240], die vorsehen, dass die Einhaltung des Datenschutzes von unabhängigen Behörden bzw. Stellen überwacht werden soll.

In seinem Urteil gegen Deutschland[241] präzisierte der EuGH die Anforderungen an die „völlige Unabhängigkeit", indem er klarstellte, dass die Entscheidungsgewalt der Datenschutz-Aufsichtsbehörden jeglicher äußeren Einflussnahme, sei sie unmittelbar oder mittelbar, entzogen sein müsse, „durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins

238 Primärrecht ist das ranghöchste Recht der EU.
239 Art. 16 Abs. 2 Satz 2 AEUV
240 Art. 8 Abs. 3 GRCh
241 EuGH, Urteil vom 9. März 2010 – C-518/07

Gleichgewicht zu bringen, erfüllen".[242] Eine staatliche Aufsicht „gleich welcher Art" ermögliche jedoch eine solche Einflussnahme. Selbst wenn die Aufsicht einer übergeordneten Stelle in der Praxis regelmäßig nicht zu konkreten Weisungen an die Aufsichtsbehörden führe, reiche die bloße Gefahr einer politischen Einflussnahme, um deren unabhängige Aufgabenwahrnehmung zu beeinträchtigen.[243]

Die in der Berliner Verfassung noch immer geregelte Dienstaufsicht der Berliner Beauftragten für Datenschutz und Informationsfreiheit durch den Präsidenten des Abgeordnetenhauses verstößt gegen Art. 52 Abs. 1 und 2 DS-GVO. Eine andere Auslegung lässt die Entscheidung des EuGH in seinem Urteil gegen Österreich[244] nicht zu.

In diesem bewertete er die beamtenrechtliche Dienstaufsicht über das geschäftsführende Mitglied der österreichischen Datenschutzkommission trotz der ausdrücklich gesicherten Weisungsfreiheit und funktionellen Unabhängigkeit der Kommission als einen Verstoß gegen Art. 28 Abs. 1 Unterabs. 2 Datenschutz-RL (alt)[245]. Insoweit genüge der Hinweis, dass nicht ausgeschlossen werden könne, dass die Beurteilung des geschäftsführenden Mitglieds der Datenschutzkommission durch den Vorgesetzten, mit der das dienstliche Fortkommen dieses Beamten gefördert werden soll, bei diesem zu einer Form von „vorauseilendem Gehorsam" führen könne.[246] Die Datenschutzkommission sei so aufgrund der Bindungen ihres geschäftsführenden Mitglieds an das ihrer Kontrolle unterliegende politische Organ nicht über jeden Verdacht der Parteilichkeit erhaben.[247] Vor diesem Hintergrund geht auch die Mehrheit der Literatur davon aus, dass eine Dienstaufsicht

242 EuGH, Urteil vom 9. März 2010 – C-518/07, Rn. 30

243 EuGH, Urteil vom 9. März 2010 – C-518/07, Rn. 32-36

244 EuGH, Urteil vom 16. Oktober 2012 – C-614/10

245 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, außer Kraft seit Geltungsbeginn der DS-GVO

246 EuGH, Urteil vom 16. Oktober 2012 – C-614/10, Rn. 51

247 EuGH, Urteil vom 16. Oktober 2012 – C-614/10, Rn. 52, ZD 2012, 563

über Mitglieder der Aufsichtsbehörde nicht mit dem Erfordernis „völliger Unabhängigkeit" aus Art. 52 Abs. 1 DS-GVO zu vereinbaren ist.[248]

Für diese Auslegung spricht zudem die Stellungnahme der Kommission im Vertragsverletzungsverfahren gegen Deutschland (Nr. 2003/4820).[249] Demnach stehe die in den Verwaltungen bestehende Dienstaufsicht zum Erfordernis einer „völligen Unabhängigkeit" im Widerspruch, da nicht mit an Sicherheit grenzender Wahrscheinlichkeit auszuschließen sei, dass der jeweilige Dienstherr auf diesem Weg versuchen könnte, unbilligen Einfluss auf die Entscheidungen der Kontrollstelle zu nehmen. Ähnliche Erwägungen stellte der deutsche Gesetzgeber in seiner Gesetzesbegründung zur Zweiten Änderung des damaligen Bundesdatenschutzgesetzes an, mit welchem von einer Dienstaufsicht für die Bundesbeauftragte bzw. den Bundesbeauftragen für den Datenschutz und die Informationsfreiheit abgesehen wurde. Ein Verzicht auf die Dienstaufsicht sei demnach notwendig, „um den formalen Anschein einer mittelbaren Einflussnahme auf die Amtsausführung von vornherein zu unterbinden", auch wenn eine Dienstaufsicht weder die Möglichkeit eröffnet, unmittelbaren Einfluss auf Entscheidungen der Datenschutzbehörde auszuüben, noch die Möglichkeit, diese Entscheidungen aufzuheben oder zu ersetzen.[250] Etwas anderes kann demnach auch nicht für die Datenschutzbeauftragten auf Landesebene gelten.

Art. 52 DS-GVO eröffnet nur geringe Gestaltungsspielräume für die Mitgliedsstaaten. Insbesondere die Abs. 1 bis 3 sind auf nationaler Ebene unmittelbar anwendbares Unionsrecht[251] und somit dem nationalen Recht vorrangig.[252] Im Fall von Verstößen der Mitgliedsstaaten gegen Art. 52 DS-GVO können sich die Aufsichtsbehörden unmittelbar auf die DS-GVO berufen und gerichtlichen Rechtsschutz

248 Gola DS-GVO/Nguyen, 2. Aufl. 2018, DS-GVO Art. 52, Rn. 12, 13; Ehmann/Selmayr/Selmayr, 2. Aufl. 2018, DS-GVO Art. 52, Rn. 17; Kühling/Buchner/Boehm, 2. Aufl. 2018, DS-GVO Art. 52, Rn. 25; Taeger/Gabel/Grittmann, 3. Aufl. 2019, DS-GVO Art. 52, Rn. 15; Paal/Pauly/Körffer, 2. Aufl. 2018, DS-GVO Art. 52, Rn. 3; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 52, Rn. 8

249 Stellungnahme KOM Vertragsverletzungsverfahren gg. Deutschland Nr. 2003/4820, S. 5

250 Gesetzentwurf zum Zweiten Gesetz zur Änderung des Bundesdatenschutzgesetzes - Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund durch Errichtung einer obersten Bundesbehörde, BT-Drs. 18/2848, S. 13

251 Paal/Pauly/Körffer, 2. Aufl. 2018, DS-GVO Art. 52, Rn. 2; BeckOK DatenschutzR/Schneider, 29. Ed. 1. August 2019, DS-GVO Art. 52, Rn. 1

252 EuGH Urteil vom 15. Juli 1964, Rs. 6/64, Costa/ENEL

suchen.[253] Sollte Art. 47 VvB nicht den datenschutzrechtlichen Anforderungen entsprechend geändert werden, könnte zudem ein erneutes Vertragsverletzungsverfahren gegen Deutschland drohen.

Eine europarechtskonforme Formulierung von Art. 47 Abs. 1 VvB könnte etwa wie folgt lauten:

„Zur Wahrung des Rechts auf informationelle Selbstbestimmung wählt das Berliner Abgeordnetenhaus eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten. Sie oder er wird von der Präsidentin oder dem Präsidenten des Abgeordnetenhauses ernannt. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit handelt bei der Erfüllung ihrer oder seiner Aufgaben oder bei der Ausübung ihrer oder seiner Befugnisse völlig unabhängig und weisungsfrei."

Art. 47 Abs. 1 VvB ist europarechtswidrig und sollte geändert werden.

253 BeckOK DatenschutzR/Schneider, 29. Ed. 1. August 2019, DS-GVO Art. 52 Rn. 1

15 Informationspflicht bei Datenpannen

15.1 Allgemeine Entwicklungen

Im letzten Jahr haben wir über die neuen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO) in Bezug auf Melde- und Informationspflichten der Verantwortlichen bei Datenpannen[254] berichtet.[255] Gab es im Jahr 2018 insgesamt 357 Meldungen, was bereits eine sprunghafte Zunahme im Vergleich zum Vorjahr bedeutete[256], so war im Berichtszeitraum ein weiterer drastischer Anstieg der Meldungen auf 1017 zu verzeichnen.[257]

Häufig fragten uns Verantwortliche, die eine Datenpanne gemeldet und die Betroffenen (ggf. vorsorglich) benachrichtigt hatten, ob sie aufgrund der Meldung eine Sanktion zu erwarten hätten. Gemäß § 43 Abs. 4 Bundesdatenschutzgesetz (BDSG) darf die Meldung einer Datenpanne in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen bzw. Benachrichtigenden oder seine Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.[258] Diese Regelung im BDSG dient der Absicherung des Grundsatzes, dass niemand gezwungen werden darf, sich selbst

254 Siehe Art. 33, 34 DS-GVO

255 JB 2018, 1.3

256 Wobei zu beachten ist, dass die Zahlen erst Ende Mai mit Wirksamwerden der DS-GVO anstiegen.

257 874 Meldungen im nicht-öffentlichen Bereich, 143 Meldungen im öffentlichen Bereich (Stand: 31. Dezember 2019)

258 Nach der Gesetzesbegründung zu § 43 Abs. 4 BDSG (BT-Drs. 18/11325, S. 109) kann die Regelung auf die Öffnungsklausel des Art. 83 Abs. 8 DS-GVO gestützt werden, wonach angemessene Verfahrensgarantien geschaffen werden müssen.

in einem Straf- oder Ordnungswidrigkeitenverfahren zu belasten.[259] So soll das Spannungsverhältnis aufgelöst werden, in dem sich Verantwortliche befinden, weil sie sich entweder wegen eines sanktionsbewährten Datenschutzverstoßes selbst bezichtigen oder – um dies zu vermeiden – gegen die Melde- und Benachrichtigungspflichten verstoßen, was seinerseits sanktioniert werden kann.[260] Das bedeutet, dass allein aufgrund der Informationen in der Meldung kein Bußgeld verhängt werden darf.[261]

Fraglich ist allerdings, ob das auch dann gilt, wenn die Aufsichtsbehörde noch auf anderem Weg von der Datenpanne erfährt, z.B. durch die Beschwerde einer betroffenen Person. Hier ist maßgeblich, ob die Beschwerde als unmittelbare direkte Reaktion auf die Benachrichtigung der Betroffenen durch den Verantwortlichen erfolgte. Allerdings kann auch in diesen Fällen eine Verwarnung[262] wegen des materiell-rechtlichen Datenschutzverstoßes, der der Panne zugrunde liegt, ausgesprochen werden.

15.2 Einzelfälle

Mehrere **Kindertagesstätten** haben uns gemeldet, dass Digitalkameras mit Fotos von Ausflügen mit Kindern und Erziehern gestohlen wurden. Alle Verantwortlichen haben sowohl die betroffenen Beschäftigten (vorsorglich) als auch die betroffenen Eltern entweder mit einem Informationsschreiben oder per Aushang in der Kita über den Vorfall informiert – zu Recht, denn das Risiko, dass die Kinder-

259 „Nemo tenetur se ipsum accusare."; Dieser Grundsatz gehört zu den anerkannten Prinzipien eines rechtsstaatlichen Verfahrens und ist durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) verfassungsrechtlich verbürgt („Freiheit von Selbstbelastungszwang", siehe BVerfG, Beschluss vom 27. April 2010 – 2 BvL 13/07). Der Grundsatz ist im Übrigen Ausdruck des Fair-Trial-Prinzips in Art. 6 der Europäischen Menschenrechtskonvention (Recht auf ein faires Verfahren).

260 Art. 83 Abs. 4 lit. a DS-GVO

261 Nach anderer Ansicht ist das Verwendungsverbot in § 43 Abs. 4 BDSG europarechtswidrig, weil es keine „angemessene" Verfahrensgarantie i. S. d. Öffnungsklausel des Art. 83 Abs. 8 DS-GVO darstellt, sondern über diejenigen Verfahrensgarantien hinausgeht, die europarechtlich geboten sind. So Kühling/Buchner/Bergt, 2. Aufl. 2018, § 43, Rn. 13; ähnlich Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, 33. Tätigkeitsbericht, S. 17.

262 Art. 58 Abs. 2 lit. b DS-GVO

fotos über zwielichtige Kanäle im Internet gestreut werden, ist heutzutage leider hoch.

Das **Landesamt für Gesundheit und Soziales (LaGeSo)** meldete uns, dass es versehentlich insgesamt 18 Diktiergeräte an drei Bezirksämter, ein Amtsgericht und ein Finanzamt abgegeben habe, die personenbezogene Diktate über amtsärztliche Untersuchungen enthielten. Nachdem das LaGeSo den Fehler festgestellt hatte, hat es die Verwaltungen umgehend gebeten, die Diktate ungelesen zu löschen. Wir haben gleichwohl vom LaGesSo gefordert, dass alle Diktiergeräte unverzüglich an das LaGeSo zurückgegeben und sie von einer Person mit IT-Sachverstand sowie der behördlichen Datenschutzbeauftragten darauf überprüft werden, ob alle Diktate vollständig und unwiederbringlich gelöscht sind. Das LaGeSo folgte unserer Forderung.

Uns erreichte eine Meldung des Unternehmens, das den jährlichen **Berlin Marathon** organisiert. Eine technische Fehleinstellung in der Datenbank habe in einem Zeitfenster von ca. 15 Stunden dazu geführt, dass Marathon-Teilnehmende Einblick in die Notfallkontaktdaten anderer Läuferinnen und Läufer nehmen konnten, wobei ihnen die Zuordnung der Notfallkontakte zu den jeweiligen Läuferinnen und Läufern nicht möglich war. Die Gesamtzahl der möglicherweise betroffenen Notfallkontakte (jeweils mit Namen, Geburtsdatum und Telefonnummer) belief sich auf 5.242 und betraf Menschen aus ganz Europa. Deshalb handelte es sich um eine „grenzüberschreitende Verarbeitung".[263] Wir haben als in Europa federführende Aufsichtsbehörde den Fall bearbeitet. Der Verantwortliche hat alle betroffenen Notfallkontakte mangels E-Mail- bzw. Postadressen nicht direkt informieren können, sondern hat den Läuferinnen und Läufern ein Benachrichtigungsschreiben geschickt mit der Bitte, ihre Notfallkontakte hierüber zu informieren.

Ein Rückgang der Meldungen von Datenpannen ist weiterhin nicht zu erwarten, derzeit steigen die Zahlen eher noch an und es ist von einem Einpendeln auf einem hohen Niveau auszugehen.

263 Siehe Art. 4 Ziff. 23 lit. b DS-GVO

16 Internationale Entwicklungen im Datenschutz

16.1 Brexit – Folgen eines (No-)Deals

Der Austritt des Vereinigten Königreichs Großbritannien und Nordirland (VK) aus der Europäischen Union, allgemein bekannt als Brexit, war ursprünglich zum 29. März 2019 vorgesehen. Auf ihrem Sondergipfel am 10. April 2019 haben die EU-Staaten einem Brexit-Aufschub bis spätestens zum 31. Oktober 2019 zugestimmt. Kurz vor Ablauf dieser Frist haben sie einem weiteren britischen Antrag auf Fristverlängerung bis spätestens zum 31. Januar 2020 stattgegeben.[264]

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat Unternehmen, Behörden und anderen Institutionen in Deutschland Informationen in Bezug auf die Rechtslage hinsichtlich des Datenschutzes nach dem Brexit gegeben.[265] Dabei wurde zwischen einem auf der Grundlage des Austrittsabkommens geregelten Austritt („Deal-Brexit") und einem ungeregelten Austritt („No-Deal-Brexit") unterschieden. Im ersten Fall gelte das EU-Recht, also auch die DS-GVO, für einen Übergangszeitraum, der einmalig um höchstens zwei Jahre verlängert werden kann, bis Ende 2020 weiter. Während dieser Zeit dürften personenbezogene Daten in das VK unter denselben Voraussetzungen wie bisher übermittelt werden. Im zweiten Fall werde das VK zu einem Drittland im Sinne der DS-GVO. Verantwortliche, die personenbezogene Daten an Stellen im VK übermitteln wollen, müssten dann die Datenübermittlungen mit den besonderen Maßnahmen nach Kapitel 5 der DS-GVO absichern.[266] Solange es keine Feststellung über die Angemessenheit des Datenschutzniveaus im VK gebe,

264 Beschluss des Europäischen Rates vom 28. Oktober 2019 – EUCO XT 20024/2/19, REV 2

265 Beschluss der DSK vom 8. März 2019, abrufbar unter www.datenschutzkonferenz-online.de/beschluesse-dsk.html

266 Siehe Information des EDSA vom 12. Februar 2019 über Datentransfers im Rahmen der DS-GVO im Falle eines No-Deal-Brexits (als deutsche Arbeitsübersetzung abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/SonstigePapiere/EDSA_Info_NoDealBrexit_Arbeits%C3%BCbersetzung.html?nn=5217120)

stünden Datentransferinstrumente wie die Standarddatenschutzklauseln oder verbindliche unternehmensinterne Datenschutzvorschriften zur Verfügung. Auch ein Verhaltenskodex[267] oder ein Zertifizierungsmechanismus[268] könnte angemessene Garantien für die Übermittlung personenbezogener Daten in das VK bieten. Welche Anforderungen an diese, nach der DS-GVO neuen, Instrumente zu stellen sind, wird sich aus den Leitlinien ergeben, die der Europäische Datenschutzausschuss (EDSA) im kommenden Jahr verabschieden will.

Alle Stellen, die personenbezogene Daten in das VK übermitteln wollen, sind gut beraten, alle notwendigen Vorkehrungen für rechtmäßige Datenflüsse zu treffen.

16.2 Bericht aus der Berlin-Group

Im Jahr 2019 traf sich die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (IWGDPT) wie seit vielen Jahren zwei Mal unter dem Vorsitz der Berliner Beauftragten für Datenschutz und Informationsfreiheit.

16.2.1 Frühjahrstagung

Auf der Frühjahrstagung am 9. und 10. April in Bled in Slowenien stand der Schutz von Kindern im Mittelpunkt der Beratungen. Zwei Arbeitspapiere konnten verabschiedet werden: Zum einen zum Datenschutz bei Online-Diensten, die sich (auch) an Kinder richten, und zum anderen zu smarten Geräten, mit denen sie spielen oder lernen.

Kinder sind bei der Nutzung von Online-Diensten besonders gefährdet. Sie verbringen eine beträchtliche Zeit mit Online-Diensten: Mit Webseiten und den dort zur Verfügung gestellten Inhalten, mit sozialen Netzwerken und ähnlichen Diensten, mit Apps auf ihren Smartphones, die viele schon von jungen Jahren an besitzen, mit Kommunikationsdiensten, die auf diesen Smartphones laufen, mit

267 Art. 46 Abs. 2 lit. e DS-GVO
268 Art. 46 Abs. 2 lit. f DS-GVO

Spielen auf Smartphones, PCs und Spielkonsolen und mit sprachgesteuerten Assistenzsystemen. Auch bildet sich ihre Fähigkeit erst heraus, informiert über die Preisgabe von Daten zu entscheiden, die sie selbst oder ihr Umfeld betreffen. Der Absichten der Unternehmen, welche die Dienste bereitstellen oder die an dieser Bereitstellung beteiligt sind, sowie vieler mit der Nutzung verbundener Gefahren sind sie sich noch nicht bewusst. Die Konsequenzen ungewollter Offenbarung und Verwendung von sie betreffenden Daten können von kleinen Ärgernissen zu weit gravierenderen Beeinträchtigungen reichen, bis hin zu sexueller Ausbeutung durch andere Nutzerinnen und Nutzer der von ihnen besuchten Dienste.

Das von der Arbeitsgruppe veröffentlichte Papier konzentriert sich auf die Risiken, die von der unsachgemäßen Verarbeitung von Daten über Kinder durch die Betreiber der Dienste und die von ihnen eingebundenen Dienstleister ausgehen. Es identifiziert die bestehenden Risiken und spricht Empfehlungen aus, einerseits für Behörden und für die Reglementierung der Dienste durch Gesetze und andererseits für die Unternehmen, welche die Dienste erbringen. Diese Empfehlungen betreffen die Einholung gültiger Einwilligungen durch die Sorgeberechtigten; ausreichende Transparenz über die vorgesehenen Datenverarbeitungen durch Informationen sowohl für die Eltern, als auch – in einer an das Zielpublikum angepassten Sprache und Form – für die Kinder selbst; Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, die in die Dienste integriert werden sollten; die Löschung von Daten, die für die Erbringung der Dienste nicht mehr von Belang sind sowie die Gewährung des Auskunftsrechts und des Rechts auf Übertragung der bei einem Dienst gespeicherten Daten auf einen anderen, möglicherweise datenschutzfreundlicheren.

Für Kinder gedachte smarte Geräte umfassen elektronisch gesteuerte und ggf. mit dem Internet verbundene Spielzeuge, „intelligente" elektronische Uhren sowie Babyphones und andere Geräte zur Überwachung von Kindern. Diese Geräte nutzen die Verbindung zum Internet, um in Echtzeit ihren Standort (und damit den Aufenthaltsort der Kinder) zu bestimmen, Daten zu übertragen, mit denen das Verhalten von Kindern durch die Eltern überwacht werden kann, und sprachliche Kommunikation zu ermöglichen. Sie erfassen die Namen der Kinder und der Personen in ihrer Umgebung, Bilddaten, Daten über Aufenthaltsorte und Verhalten und ggf. sogar Gesundheitsdaten der Kinder. Bedauerlicherweise haben internationale Erfahrungen gezeigt, dass einige Hersteller solcher Spielzeuge oder Ge-

räte den Rechten der Verbraucherinnen und Verbraucher sowie dem Schutz ihrer Daten viel zu wenig Aufmerksamkeit geschenkt haben. Einige Spielzeuge mussten auf Anweisung von Aufsichtsbehörden vom Markt genommen werden.

Auch hier analysierte die Arbeitsgruppe die mit der Nutzung solcher Geräte und Spielzeuge verbundenen Risiken und formulierte Empfehlungen. Die festgestellten Risiken erstrecken sich auf intransparente und exzessive Datenerfassungen und -verarbeitungen, eine überlange Speicherung der erfassten Daten und ihre unzulässige Zweitverwendung, eine unzureichende Sicherheit der Geräte und der Kommunikation mit den Dienstleistern, mit denen sie sich verbinden, sowie anderweitig unrechtmäßige Verarbeitungsvorgänge.

Vielfach verwenden Hersteller hochgradig unbestimmte allgemeine Geschäftsbedingungen und Datenschutzerklärungen. Aus derart defizitären Dokumenten wird regelmäßig nicht klar, an welche anderen Unternehmen und Institutionen die mit den Geräten aufgenommenen Daten für welche Zwecke weitergegeben werden. Auch Speicherfristen werden nicht angegeben. In der Regel behält sich der Hersteller zusätzlich vor, die Bestimmungen jederzeit zu ändern. Aufgrund derart mangelhafter Angaben sind informierte Einwilligungen nicht möglich und die vielfach vorgenommenen Datenverarbeitungen, die über die reine Erbringung der mit den Geräten verbundenen Dienstleistung hinausgehen, bleiben ohne Rechtsgrundlage. Geräte und Spielzeuge, die eine Möglichkeit zur Steuerung der Verarbeitung aufweisen, stellen diese in den Anleitungen irreführend dar und verleiten die Eltern und ihre Kinder dazu, datenschutz-unfreundliche Vorgehensweisen, die sie als Voreinstellung vorgeben, zu akzeptieren. Vielfach gewähren gravierende und leicht auszunutzende Sicherheitslücken unbefugten Dritten die Kontrolle über Daten und Aufnahmegeräte (oft Mikrofone, zuweilen auch Kameras). Wenn Update-Funktionen nicht vorgesehen sind oder Updates nicht bereitgestellt werden, lassen sich diese Lücken auch nicht schließen.

Das Papier schließt an diese Analyse eine Reihe von Empfehlungen an, die sich vornehmlich an die Hersteller, aber auch an die Eltern und andere Sorgeberechtigte, an Schulen und Lehrpersonal sowie an die Datenschutzaufsichtsbehörden selbst richten.

16.2.2 Herbsttagung

Die zweite Sitzung des Jahres fokussierte sich auf die Arbeit an einem Papier zur Verfolgung und zum Profiling von Personen bei der Nutzung von Webangeboten, das im kommenden Jahr fertiggestellt und beschlossen werden soll. Weitere Themen waren Sensornetzwerke und Assistenzsysteme, die durch Sprache oder Gesten gesteuert werden.

Die Arbeitsgruppe nutzte diese Sitzung auch zu einer Evaluierung ihrer Tätigkeit und der neuen Arbeitsregularien, die sie sich vor zwei Jahren gegeben hatte. Da sich die in der Arbeitsgruppe bearbeitete Themenpalette über die Jahre verbreitert hat, wurde auch ein Namenswechsel beschlossen. Der neue Name lautet "International Working Group on Data Protection in Technology".

Die Berlin Group erfreut sich international großer Anerkennung. Die durch sie beschlossenen Papiere haben den unschätzbaren Vorteil, dass sie international auf breiter Basis abgestimmt sind und deshalb sowie aufgrund der in ihnen meist enthaltenen konkreten Handlungsempfehlungen fachlich eine belastbare Orientierung in schwierigen datenschutztechnischen Fragestellungen bieten.

17 Informationsfreiheit

17.1 Internationale Entwicklungen

Vom 10. bis 13. März 2019 fand die Internationale Konferenz der Informationsbeauftragten (ICIC) in Johannesburg/Republik Südafrika statt. Dort wurde per Resolution beschlossen, künftig als permanentes Netzwerk aufzutreten, und die sog. ICIC Johannesburg Charter als ein erstes Regelwerk vereinbart.[269] Damit hat die Konferenz einen regulierenden Rahmen zugunsten einer konstanteren Organisation erhalten. Auch wurden Leitlinien und Regularien zur Aufnahme und Beteiligung von Mitgliedern formuliert.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) hat an der Konferenz teilgenommen und inzwischen das Akkreditierungsverfahren erfolgreich absolviert. Als Mitglied der ICIC[270] ist sie berechtigt, an den geschlossenen Sitzungen der jährlichen Treffen teilzunehmen.

Zu dieser Konferenz hat die BlnBDI gemeinsam mit dem Bundesbeauftragten für Datenschutz und Informationsfreiheit das von der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) im letzten Jahr verabschiedete Positionspapier zur Frage der Transparenz der Verwaltung beim Einsatz von Algorithmen[271] in einer leicht gekürzten Version eingebracht, um zu diesem wichtigen Thema auch eine internationale Positionierung zu erreichen. Das Papier befindet sich im Umlaufverfahren und soll auf diesem Weg überarbeitet und von der ICIC beschlossen werden.

269 www.informationcommissioners.org
270 www.informationcommissioners.org/berlin
271 Siehe hierzu JB 2018, 13.1

17.2 Entwicklungen in Deutschland

17.2.1 Zusammenarbeit der Informationsfreiheitsbeauftragten

In diesem Jahr fand die IFK unter dem Vorsitz des Unabhängigen Datenschutzzentrums Saarland statt. Mit dem dort verabschiedeten Positionspapier „Informationszugang in den Behörden erleichtern durch ‚Informationsfreiheit by Design'" rief die Konferenz den Gesetzgeber dazu auf, die gesetzlichen Grundlagen und Rahmenbedingungen zu schaffen, damit die öffentliche Verwaltung die Anforderungen an die Informationsfreiheit bereits von Anfang an in die Gestaltung ihrer IT-Systeme und organisatorischen Prozesse einfließen lässt.[272]

Außerdem haben sich die Informationsfreiheitsbeauftragten in einer Entschließung für mehr Transparenz bei politischen Entscheidungsprozessen ausgesprochen.[273] Der Gesetzgeber wurde aufgefordert, ein verpflichtendes Lobbyregister einzuführen, in das sich die Interessenvertretungen mindestens unter Angabe ihrer Tätigkeit und Aktivität im jeweiligen Entscheidungsprozess eintragen müssen. In anderen Ländern gibt es derartige Lobbyregister bereits.[274]

17.2.2 Neues Bundesgesetz

Im April ist das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) in Kraft getreten.[275] Damit wurde die europäische „Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsge-

272 Positionspapier der IFK vom 12. Juni 2019, abrufbar unter www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-informationsfreiheit/

273 Entschließung der IFK vom 12. Juni 2019: Transparenz im Rahmen politischer Entscheidungsprozesse – verpflichtendes Lobbyregister einführen, abrufbar unter www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-informationsfreiheit/

274 So z.B. in Dänemark, Frankreich, Irland, Litauen, Slowenien, Kanada und USA

275 Siehe BGBl. I 2019, S. 466 ff.

heimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung" umgesetzt.[276] In dem neuen Gesetz wird der Begriff Geschäftsgeheimnis anders definiert als bislang durch die Rechtsprechung des Bundesverfassungsgerichts konkretisiert. Nach dieser Rechtsprechung wurden als Betriebs- und Geschäftsgeheimnis alle auf ein Unternehmen bezogenen Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat.[277] Nach der Legaldefinition im neuen Gesetz kommt es nunmehr zusätzlich auf den wirtschaftlichen Wert der Information und auf angemessene Geheimhaltungsmaßnahmen an.[278]

Damit ist die Hürde für die Begründung eines Schutzbedarfs von Geschäftsgeheimnissen höher als vom Bundesverfassungsgericht per Definition seit Jahren vorgegeben. Denn der rechtmäßige Inhaber des Geheimnisses muss „den Umständen nach angemessene Geheimhaltungsmaßnahmen" hinsichtlich nicht bekannter Informationen ergriffen haben. Fehlen solche Maßnahmen, liegt kein Geschäftsgeheimnis vor und demzufolge auch kein besonderer Schutzbedarf gegenüber der unerwünschten Verwertung der Informationen.

Ob die Legaldefinition des neuen Gesetzes Auswirkungen auf die nach den Informationsfreiheitsgesetzen zu prüfenden Betriebs- und Geschäftsgeheimnisse hat, wird zwar diskutiert, ist aber vor dem Hintergrund des eindeutigen Wortlauts des Gesetzes nebst Begründung fraglich: Im GeschGehG ist ausdrücklich normiert, dass öffentlich-rechtliche Vorschriften zur Geheimhaltung, Erlangung, Nutzung oder Offenlegung von Geschäftsgeheimnissen vorgehen;[279] darüber hinaus ist nach der Gesetzesbegründung die Anwendung des Gesetzes u. a. für Informationsansprüche gegen staatliche Stellen ausgeschlossen.[280] Dementsprechend geht auch das Verwaltungsgericht Berlin (jedenfalls bislang) davon aus, dass die

276 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016, ABl. L 157 vom 15. Juni 2016, S. 1

277 BVerfG, Beschluss vom 14. März 2006 – 1 BvR 2087/03, 1 BvR 2111/03

278 § 2 Nr. 1 a), b) GeschGehG

279 § 1 Abs. 2 GeschGehG

280 BT-Drs. 19/4724, S. 23

Regelungen des GeschGehG im Bereich der Informationsfreiheit nicht anwendbar sind.[281]

17.2.3 Neue Landesgesetze

Nach den Ländern Bremen, Hamburg und Rheinland-Pfalz verfügt nun auch Thüringen über ein Transparenzgesetz und damit über ein moderneres Informationsfreiheitsrecht, das den Menschen den kostenlosen Zugang zu staatlichen Informationen über ein Transparenzportal im Internet ermöglichen soll. Noch immer gibt es aber drei Bundesländer, die weder über ein Informationsfreiheits- noch über ein Transparenzgesetz verfügen: Bayern, Niedersachsen und Sachsen.

17.3 Entwicklungen in Berlin

Auch in Berlin sind erfreulicherweise erste Schritte in Richtung Transparenzgesetz erkennbar. So hat die FDP-Fraktion den Entwurf eines Berliner Transparenzgesetzes in das Abgeordnetenhaus eingebracht.[282] Hierzu fand eine Anhörung von Experten im federführenden Ausschuss für Kommunikationstechnologie und Datenschutz statt.[283]

Daneben hat ein Bündnis von 40 zivilgesellschaftlichen Organisationen rund um den Open Knowledge Foundation Deutschland e. V. und den Mehr Demokratie e. V. einen „Volksentscheid Transparenz Berlin" auf den Weg gebracht.[284] Er beinhaltet einen eigenen Gesetzentwurf für ein Berliner Transparenzgesetz. Im Dezember wurden die mehr als 30.000 Unterschriften an den Senat übergeben. Herzstück beider Initiativen ist die Verpflichtung des Landes Berlin zur aktiven Veröffentlichung von Informationen im Internet.

281 VG Berlin, Urteil vom 26. Juni 2019 – VG 2 K 179.18
282 Abghs.-Drs.18/1595 vom 16. Januar 2019
283 KTDat, Sitzung vom 25. November 2019
284 https://volksentscheid-transparenz.de/

Gegen Ende des Berichtszeitraums hat die Senatsverwaltung für Inneres und Sport als federführende Verwaltung ein erstes Eckpunktepapier für ein Transparenzgesetz formuliert. Die Erfüllung der Koalitionsvereinbarung von 2016 rückt in diesem Punkt ein kleines Stück näher.[285]

285 Siehe bereits JB 2018, 13.2.1

18 Aus der Dienststelle

18.1 Entwicklungen

Im vergangenen Jahr haben wir ausführlich über unsere ersten Erfahrungen als Aufsichtsbehörde für den Datenschutz nach dem Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 berichtet.[286] Im Ergebnis mussten wir feststellen, dass der Arbeitsanfall in der gesamten Behörde durch die immens gestiegene Anzahl von Eingaben, Beschwerden und Beratungsersuchen kaum zu bewältigen war. Die damals zu beobachtende Entwicklung hat sich im Berichtszeitraum dynamisch fortgesetzt.

Bei den Meldungen von Datenpannen durch Unternehmen und andere Verantwortliche, die allesamt recherchiert und innerhalb von engen Fristen Lösungen zugeführt werden müssen, hat es eine Versiebzehnfachung der Vorgänge gegeben.

Die Anzahl der Beschwerden von Bürgerinnen und Bürgern, die sich auf ihre Rechte nach der DS-GVO berufen, ist gleichbleibend hoch. Im Schnitt gehen monatlich fast 400 Eingaben von betroffenen Bürgerinnen und Bürger bei uns ein. Damit haben sich die Bürgereingaben seit Mai 2018 dauerhaft verdreifacht.[287] Durch die Vielzahl der Vorgänge war die Servicestelle Bürgereingaben, in der die Erstbearbeitung der Beschwerden (z.B. Prüfung der sachlichen und örtlichen Zuständigkeit, Vollständigkeit der Unterlagen usw.) zentral erfolgt, derartig überlastet, dass eine zeitnahe Bearbeitung der Fälle nur noch eingeschränkt erfolgen konnte.

Alle eingehenden Beschwerden – aber auch alle Fälle, in denen die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) von Amts wegen tätig wird, sowie die von Verantwortlichen gemeldeten Datenpannen – müssen nach Wirksamwerden der DS-GVO nunmehr auch daraufhin geprüft werden, ob eine grenzüberschreitende Datenverarbeitung vorliegt. Um diese für uns als Auf-

286 JB 2018, 14.1
287 Siehe 18.2.1

sichtsbehörde neue Aufgabe bewältigen zu können, wurde bereits im Vorjahr die Servicestelle Europaangelegenheiten eingerichtet.[288] Die arbeitsintensive Bearbeitung der grenzüberschreitenden Fälle erfolgt dort durch spezialisierte Dienstkräfte unter höchsten juristischen und technischen Anforderungen, zudem unter großem Zeitdruck und weitgehend in englischer Sprache. Die erforderliche Abstimmung mit den anderen nationalen und europäischen Aufsichtsbehörden erfolgt über das elektronische Binnenmarkt-Informationssystem (IMI). Bisher wurden europaweit rund 760 Fälle zur Bestimmung der federführenden und der betroffenen Aufsichtsbehörden in das IMI-System gemeldet. In über 360 Fällen wurde eine Betroffenheit der BlnBDI festgestellt, sodass wir uns inhaltlich mit dem gemeldeten Sachverhalt befassen mussten. Insgesamt 35 Fälle wurden im IMI unter unserer Federführung bearbeitet.

Die Sanktionsverfahren zur Ahndung von festgestellten datenschutzrechtlichen Verstößen werden in unserer Behörde zentral in der Servicestelle Sanktionen bearbeitet.[289] Dabei wird die überwiegende Anzahl der Fälle jetzt nach den neuen Bußgeldvorschriften bearbeitet, die in mehreren Verfahren zu Bußgeldern in relevanter Höhe nach den neuen Zumessungskriterien führten. Um die mit dem Wirksamwerden der DS-GVO neuen Regelungen, insbesondere zur Verfolgung von Ordnungswidrigkeiten, wirksam und effizient anwenden zu können, wurde der Bereich Sanktionen im Berichtszeitraum organisatorisch und personell neu strukturiert.

Unsere Angebote zur Vermittlung von Datenschutz und Medienkompetenz insbesondere bei Kindern haben wir im Berichtszeitraum ausgebaut.[290] Die sehr hohe Nachfrage im Zusammenhang mit den Projekttagen, die wir zum Thema Datenschutz und Medienkompetenz in Schulen durchführten, zeigt den immensen Bedarf in diesem Bereich. Dieser kann mit den uns zur Verfügung stehenden Mitteln und Ressourcen nicht annähernd abgedeckt werden, weswegen wir auch verstärkt Kooperationspartnerschaften und Netzwerke suchen. Wir haben unsere Kinderwebseite www.data-kids.de grundlegend überarbeitet und neu gestaltet. Die Nominierung dieser Seite für den deutschen Kindersoftwarepreis TOMMI und

288 Siehe 1.5
289 Siehe 12.1 bis 12.4
290 Siehe 5.6

das Erreichen der Endrunde im diesjährigen Wettbewerb zeigt uns, dass wir damit auf dem richtigen Weg sind.

Durch die Umsetzung der Regelungen der DS-GVO ist die Dienststelle in allen Bereichen einer extrem hohen Belastung ausgesetzt. Dass die Aufgaben wenigstens ansatzweise erledigt werden konnten, ist nicht zuletzt auf den bemerkenswerten Einsatz der hoch motivierten Mitarbeiterinnen und Mitarbeiter zurückzuführen. Rückstände in der Bearbeitung konnten nur durch die Leistung einer großen Zahl an Überstunden und teilweise in Wochenendarbeit bewältigt werden. Diese ständige Überlastung der Dienstkräfte hat jedoch auch zu krankheitsbedingten Ausfällen geführt und ist als Dauerzustand nicht tragbar.

Erfreulicherweise hat der Haushaltsgesetzgeber auf diese Missstände reagiert und für die Jahre 2020/2021 eine spürbare Verbesserung der Personalausstattung der BlnBDI beschlossen. Dies wird zwar nicht zu einer sofortigen Änderung der geschilderten Lage führen, da die (auf zwei Jahre verteilten) Stellen zunächst ausgeschrieben und besetzt, die neuen Mitarbeiterinnen und Mitarbeiter dann auch erst eingearbeitet werden müssen. Mit der Bereitstellung der neuen Personalmittel besteht jetzt jedoch eine greifbare Perspektive, dass sich die angespannte Situation im Laufe der nächsten zwei Jahre spürbar verbessern wird.

Die neuen europäischen Regelungen der DS-GVO haben zu einer beständigen Vervielfachung der Aufgaben der BlnBDI geführt. Es ist sehr erfreulich, dass der Berliner Gesetzgeber darauf reagiert und durch die Verstärkung der Personalmittel für unsere Behörde im Haushalt 2020/2021 ein starkes Zeichen für die Bedeutung des Datenschutzes in Berlin gesetzt hat.

18.2 Aus der Servicestelle Bürgereingaben

18.2.1 Eingabenentwicklung, Statistik, inhaltliche Trends, konzeptionelle Ansätze

Aus der Praxis

Auch nachdem die DS-GVO wirksam geworden ist, bleibt die Bearbeitung von Eingaben eine unserer wichtigsten Aufgaben. Die Servicestelle Bürgereingaben ist die erste Anlaufstelle für eingehende Bürgereingaben wie z.B. Beschwerden,[291] allgemeine Hinweise oder Beratungsanfragen.

Alle Eingänge werden zunächst in der Servicestelle gesichtet, wobei eine erste Einschätzung erfolgt. Dabei wird sowohl die sachliche als auch die örtliche Zuständigkeit geprüft. Außerdem wird kontrolliert, ob die Eingaben vollständig und alle erforderlichen Unterlagen vorhanden sind.

Eine Beschwerde kann von uns erst dann bearbeitet werden, wenn ein Verstoß gegen Datenschutzgesetze bei der Verarbeitung personenbezogener Daten nicht ausgeschlossen ist. Ein Teil der allgemeinen Anfragen kann durch derartige Vorprüfungen bereits in der Servicestelle vollumfänglich beantwortet werden. Die verbleibenden Anfragen sowie die (vervollständigten) Beschwerden werden anschließend an die jeweils zuständigen Fachreferate zur Bearbeitung weitergegeben. Sollten sich Bürgerinnen und Bürger mit Anliegen an uns wenden, bei denen wir ihnen aufgrund mangelnder Zuständigkeit nicht weiterhelfen können, verweisen wir diese an die zuständigen Stellen wie z.B. die Aufsichtsbehörden anderer Bundesländer, die Bundesnetzagentur, an Verbraucherschutzorganisationen oder auch an die Strafverfolgungsbehörden.

Nachdem sich das Aufkommen von Beschwerden mit Inkrafttreten der DS-GVO zunächst vervierfacht hatte, ist die Anzahl der Eingaben seither auf hohem Niveau konstant geblieben. Im Schnitt gingen seitdem monatlich fast 400 Bürgereingaben ein, was eine Verdreifachung gegenüber den Eingabezahlen aus der Zeit vor Wirksamwerden der DS-GVO bedeutet.

291 Art. 77 DS-GVO

Bei einer Vielzahl der Beschwerden handelt es sich um Beschwerden bezüglich nicht oder nicht vollständig erteilter Datenauskünfte oder wegen nicht erfolgter Löschung personenbezogener Daten. Sehr häufig geht es auch um den Erhalt von unerwünschten E-Mails und Newslettern.

Ein Großteil der eingehenden Bürgereingaben betrifft Unternehmen aus dem Bereich Wirtschaft wie z.B. Onlineshops, Lieferdienste oder soziale Netzwerke. Daneben sind aber auch Themenbereiche wie Wohnungswirtschaft, Gesundheit, Finanzdienstleistungen und Beschäftigtendatenschutz stark vertreten.

Wir halten den Anstieg der Beschwerdezahlen zwar einerseits für ein erfreuliches Zeichen, weil daraus ersichtlich wird, dass die Bürgerinnen und Bürgern ihre Rechte kennen und diese auch in Anspruch nehmen. Jedoch zeigt die Anzahl der Beschwerden zugleich leider auch, dass die in den Datenschutzgesetzen garantierten Rechte der Bürgerinnen und Bürger zu oft von Unternehmen missachtet werden.

Das Beschwerdeaufkommen ist auch im zweiten Jahr der Wirksamkeit der DS-GVO konstant hoch geblieben. Das zeigt, dass die DS-GVO von Beginn an gewirkt und nachhaltig dazu geführt hat, dass die Betroffenen ihre Datenschutzrechte kennen und auch geltend machen.

18.2.2 Meine perfekte Beschwerde – Hinweise zum Beschwerdeverfahren

Beschwerden von Bürgerinnen und Bürgern über die Verletzung von Betroffenenrechten sind die Hauptquelle für bei uns geführte Verfahren. Um Betroffenen ihre Eingabe zu erleichtern, bieten wir auf unserer Internetseite ein elektronisches Beschwerdeformular an.

Um als Servicestelle Bürgereingaben der BlnBDI für die betroffene Person tätig werden zu können, benötigen wir insbesondere Angaben über die für die Datenverarbeitung verantwortliche Stelle. Aufgrund der Komplexität des Datenschutzrechts ist eine abstrakte Bewertung des Vorgangs ohne die Angabe der verantwortlichen Stelle meist nicht möglich. Weiterhin benötigt die Servicestelle

Bürgereingaben zur Bearbeitung der jeweiligen Beschwerde eine genaue Beschreibung des datenschutzrechtlich relevanten Sachverhalts und natürlich Angaben dazu, worin die Verletzung der Datenschutzrechte konkret besteht.

Hierbei kann die Vorlage geeigneter Nachweise (z.B. E-Mail- oder Schriftverkehr mit der verantwortlichen Stelle oder sonstige Unterlagen, die den Verstoß belegen können) hilfreich sein. Das erspart der betroffenen Person Nachfragen unsererseits und dient somit auch der zügigeren Bearbeitung der Beschwerde. Generell sollte die Aufsichtsbehörde über Maßnahmen in Kenntnis gesetzt werden, die Betroffene selbst ergriffen haben.

Ziel der meisten Beschwerdeverfahren ist die Durchsetzung eines bestehenden, aber nicht gewährten Anspruchs aus den sog. Betroffenenrechten[292]; diese gegenüber den für die Datenverarbeitung Verantwortlichen geltend zu machen, obliegt zunächst den Betroffenen selbst. Betroffene Personen können sich bspw. schriftlich an Behörden oder private Stellen wenden und um Auskunft über die über sie gespeicherten Daten bitten. Zudem besteht die Möglichkeit, der Verarbeitung ihrer Daten zu widersprechen oder die Berichtigung oder Löschung der Daten zu verlangen, wenn die entsprechenden Voraussetzungen vorliegen. Sofern einem solchen Anliegen der betroffenen Person vonseiten der angeschriebenen Stelle nicht bzw. nicht fristgemäß entsprochen wird, hat sie das Recht, sich bei einer Datenschutz-Aufsichtsbehörde zu beschweren.

Die Vorlage von Dokumenten, die den geschilderten Sachverhalt stützen, kann zu einer besseren Beurteilung des Vorgangs und zum schnelleren Abschluss des Verfahrens beitragen. Gerade wenn ein Verstoß gegen datenschutzrechtliche Vorschriften aufgrund widerstreitender Aussagen von betroffener Person und verantwortlicher Stelle nicht zweifelsfrei festzustellen ist, kann die Vorlage geeigneter Nachweise für die Prüfung des geltend gemachten Datenschutzverstoßes sehr hilfreich sein und dazu beitragen, den Sachverhalt zu klären und einen festgestellten Verstoß dann ggf. zu ahnden.

292 Im Einzelnen die Rechte auf Selbstauskunft (Art. 15 DS-GVO), Berichtigung (Art. 16 DS-GVO) oder Löschung der eigenen Daten (Art. 17 DS-GVO); außerdem die Rechte auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) oder Widerspruch dagegen (Art. 21 DS-GVO) sowie das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)

In unserem Beschwerdeformular[293] wird genau aufgeführt, welche Angaben die Servicestelle Bürgereingaben von der betroffenen Person und ggf. weiteren Beteiligten benötigt. Diese Angaben können entweder auf dem Postweg oder auch direkt digital an die Servicestelle Bürgereingaben übersandt werden. Eine Verschlüsselung sorgt auch im letzteren Fall für eine datenschutzgerechte Übermittlung.

Sobald der Servicestelle Bürgereingaben alle benötigten Angaben vorliegen und eine örtliche Zuständigkeit unsererseits gegeben ist, wird die Beschwerde dem zuständigen Referat zugeteilt. Die Fachreferate bearbeiten die Beschwerde anschließend in eigener Zuständigkeit, informieren regelmäßig über den Sachstand des Verfahrens und erteilen nach Beendigung oder Einstellung des Verfahrens eine Abschlussnachricht.

Dank der vielen Eingaben der Bürgerinnen und Bürger konnten bereits zahlreiche Datenschutzverstöße aufgedeckt und die Verantwortlichen zur Rechenschaft gezogen werden. Diese Eingaben sind ein wichtiges Instrument, um auch langfristig die Einhaltung der Datenschutzgesetze gewährleisten und Datenschutzverstößen vorbeugen zu können.

18.3 Zusammenarbeit mit dem Abgeordnetenhaus von Berlin

Der Ausschuss für Kommunikationstechnologie und Datenschutz (KTDat) tagte in 10 Sitzungen, in denen die BlnBDI zu verschiedenen Themen Stellung nehmen und Empfehlungen abgeben konnte. Gegenstand der Befassung im Ausschuss waren u. a. ein Berliner Transparenzgesetz,[294] Jelbi – die sog. Mobilitäts-App der BVG,[295] der Schadsoftware-Befall beim Berliner Kammergericht[296] sowie der sog. Digitalpakt Schulen[297].

293 https://kontakt.datenschutz-berlin.de/
294 Siehe 17.3
295 Siehe 4.1
296 Siehe 2.4
297 Siehe 5.4

Anlässlich des einjährigen Geburtstags der DS-GVO lud die BlnBDI Abgeordnete aller im Parlament vertretenen Parteien des Berliner Abgeordnetenhauses am 24. Mai zu einem parlamentarischen Frühstück in ihre Dienststelle ein. Ziel war es, den Parlamentariern die Arbeitsweise der Behörde vorzustellen und insbesondere die durch die neuen europäischen Regelungen geänderten Verfahrensweisen zu veranschaulichen. In einem Vortrag stellten Mitarbeiterinnen und Mitarbeiter die einzelnen Arbeitsschritte bei Datenschutzbeschwerden mit grenzüberschreitendem Bezug vor, die in enger Kooperation mit anderen europäischen Aufsichtsbehörden bearbeitet werden. In einem weiteren Impulsvortrag wurde das überarbeitete und ergänzte medienpädagogische Angebot unserer Behörde, www.data-kids.de, präsentiert. Anschließend blieb Zeit für die teilnehmenden Abgeordneten, mit der Datenschutzbeauftragten und ihren Mitarbeitenden ins Gespräch zu kommen und weitere Fragen zu stellen. Da sich das Format als erfolgreich erwies, sind weitere Veranstaltungen dieser Art geplant.

18.4 Zusammenarbeit mit anderen Stellen

Die 2019 von Rheinland-Pfalz geleitete **Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)** tagte am 3./4. April auf dem Hambacher Schloss und am 6./7. November in Trier und fasste zahlreiche Entschließungen und Beschlüsse zu aktuellen Fragen des Datenschutzes.[298] Drei Zwischenkonferenzen fanden am 22. März in Berlin sowie am 25. Juni und 25. Oktober in Mainz statt. Dabei bewährte sich die nach Wirksamwerden der DS-GVO neu gefasste Geschäftsordnung der DSK in mehreren Fällen und zeigte sich als konstruktiv und zielführend.

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)** tagte am 12. Juni in Saarbrücken. Sie fasste eine Entschließung zur Einführung eines verpflichtenden Lobbyregisters für mehr Transparenz im Rahmen politischer Ent-

298 Alle Entschließungen und Beschlüsse der DSK sind auf der Webseite der DSK abrufbar: https://www.datenschutzkonferenz-online.de/entschliessungen.html https://www.datenschutzkonferenz-online.de/beschluesse-dsk.html

scheidungsprozesse sowie ein Positionspapier zum erleichterten Informationszugang in den Behörden durch „Informationsfreiheit by Design“.[299]

Die **Berlin-Group (IWGDPT)** tagte unter unserem Vorsitz am 9./10. April in Bled (Slovenien) sowie am 10./11. Oktober in Brüssel (Belgien).[300]

18.5 Pressearbeit

Das mediale Interesse an der Arbeit unserer Behörde ist auch im Jahr 2019 im Vergleich zum Vorjahr erneut angestiegen. In diesem Jahr beantworteten wir insgesamt 245 Presseanfragen. Während im Jahr 2018 thematisch allgemein die DS-GVO und ihre Umsetzung in Wirtschaft und Verwaltung im Vordergrund standen, interessierte sich die Öffentlichkeit in diesem Jahr besonders für die konkreten Auswirkungen der DS-GVO. Dabei ging es auch immer wieder um die Frage, ob und inwieweit wir bereits von unseren Möglichkeiten Gebrauch gemacht haben, Sanktionen nach der DS-GVO zu verhängen. Drei bekannt gewordene Bußgeldentscheidungen[301] hatten besonders viele Anfragen zur Folge, auch aus dem europäischen Ausland.

Weitere Themen, die für die mediale Öffentlichkeit von großem Interesse waren, waren von uns durchgeführte Prüfverfahren gegen den Bike-Sharing Anbieter Mobike und die Video-App TikTok. Auch Sicherheitsmängel in Verbindung mit den Informationssystemen der Berliner Polizei und deren missbräuchliche Nutzung beschäftigten unsere Pressestelle in hohem Maße. Unser Presseteam stand Journalistinnen und Journalisten zu diesen und vielen anderen Themen zur Verfügung, damit die teils schwierigen datenschutzrechtlichen und datenschutztechnischen Fragen in der Medienberichterstattung verständlich und richtig dargestellt werden konnten.

299 Beide Dokumente sind auf unserer Webseite abrufbar:https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-informationsfreiheit/

300 Zu den Ergebnissen siehe 16.2

301 Siehe 12.1 bis 12.3

Anlässlich des einjährigen Geburtstags der DS-GVO lud die BlnBDI Journalistinnen und Journalisten am 23. Mai zu einem Pressefrühstück in ihre Dienststelle ein. In zwei Kurzpräsentationen stellten wir unsere Arbeit in den Bereichen europäische Zusammenarbeit und Medienpädagogik vor und boten den Teilnehmenden so Einblicke in die Aufgaben und Arbeitsweise unserer Behörde. Bei einer anschließenden Diskussionsrunde blieb Zeit, mit der Datenschutzbeauftragten und ihren Mitarbeiterinnen und Mitarbeitern ins Gespräch zu kommen und offene Fragen zu klären. Da sich das Format als erfolgreich erwies, sind weitere Veranstaltungen dieser Art geplant.

Mit insgesamt 16 Pressemitteilungen wandte sich die BlnBDI mit eigenen Themen an die Öffentlichkeit. So machten wir auf problematische Gesetzgebungsvorhaben, bspw. zur Einführung einheitlicher verwaltungsübergreifender Personenkennzeichen oder das Datenschutz-Anpassungsgesetz[302], aufmerksam und informierten die Öffentlichkeit über unser medienpädagogisches Angebot sowie Neuveröffentlichungen der Berlin-Group[303] zu Themen wie Smart Devices, Online Services für Kinder und Künstliche Intelligenz.

Folgende Pressemitteilungen haben wir in diesem Jahr veröffentlicht:

- Drohbriefe aus Polizeikreisen – lückenlose Aufklärung gefordert (6. Februar 2019)
- Einladung zum Pressegespräch – Jahresbericht 2018 (22. März 2019)
- Jahresbericht 2018 (28. März 2019)
- Berliner Datenschutzbeauftragte beim Netzfest der re:publica (2. Mai 2019)
- Berlin Group veröffentlicht Arbeitspapier zu Datenschutz und künstlicher Intelligenz (9. Mai 2019)
- Berlin Group veröffentlicht Arbeitspapier zur großräumigen Standortverfolgung (10. Mai 2019)
- Maja Smoltczyk: Europa ist der Weg – Gehen Sie wählen! (23. Mai 2019)
- Datenschutz-Anpassungsgesetz – vermeintlicher Bürokratieabbau ist eine Milchmädchenrechnung (27. Juni 2019)

302 Siehe 14.1

303 Zu den Ergebnissen siehe 16.2

- Datenschutz für Grundschulen – überarbeitetes und erweitertes Angebot (30. Juli 2019)
- EuGH-Urteil zu Social-Media-Plugins – Webseitenbetreiber in der Pflicht (31. Juli 2019)
- Bürgerfreundliche Verwaltungsdigitalisierung geht auch ohne Personenkennzeichen (13. September 2019)
- Medienpädagogisches Angebot der BlnBDI für den Softwarepreis TOMMI nominiert (16. September 2019)
- Lieferdienst und Online-Bank – Berliner Datenschutzbeauftragte verhängt empfindliche Bußgelder (19. September 2019)
- Berlin Group veröffentlicht Arbeitspapier zu smarten Geräten für Kinder und die Privatsphäre von Kindern bei Online-Diensten (8. Oktober 2019)
- Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft (5. November 2019)
- Datenschutzbeauftragte: Google Analytics und ähnliche Dienste nur mit Einwilligung nutzbar (14. November 2019)

Alle Pressemitteilungen sind auf unserer Webseite abrufbar.[304] Mit einer E-Mail an die Adresse presse@datenschutz-berlin.de ist eine Aufnahme in unseren Presseverteiler möglich.

18.6 Öffentlichkeitsarbeit

Am 28. Januar fand auf Einladung der DSK aus Anlass des **13. Europäischen Datenschutztags** eine zentrale Veranstaltung in der Vertretung des Landes Nordrhein-Westfalen beim Bund in Berlin statt. Das Thema lautete „Europäischer Datenschutz: Chance oder Risiko? Acht Monate DS-GVO – Bilanz und Blick nach vorn".

Zum zweiten Mal nahm unsere Behörde am 4. und 5. Mai am **Netzfest der Internetkonferenz re:publica** im Park am Gleisdreieck teil. Im Programmteil „Politics & Society" des digitalen Volksfestes stellten drei Mitarbeiter der Behörde ihre Ar-

304 https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen/

beit vor. Neben dem Dauerbrenner DS-GVO war in diesem Jahr dem Thema Medienpädagogik ein besonderer Schwerpunkt gewidmet, so z.B. im Rahmen eines Workshops mit dem Titel „Digital Natives – Digitale Profis? Datenschutz für Kinder und Jugendliche". Am Informationsstand beantworteten die Mitarbeiterinnen und Mitarbeiter unserer Behörde zahlreiche Fragen von Bürgerinnen und Bürgern, nahmen Anregungen entgegen und verteilten Informationsmaterial zu Datenschutz und Informationsfreiheit.

Am 7. September waren wir wieder mit einem Informationsstand beim **Tag der offenen Tür im Abgeordnetenhaus** vertreten. In diesem Jahr stand die Veranstaltung in Verbindung mit dem 30. Jahrestag des Mauerfalls im November 1989. Wie bereits in den vergangenen Jahren nutzten wir diese Gelegenheit, um mit Bürgerinnen und Bürgern ins Gespräch zu kommen, Fragen zu beantworten und Anregungen entgegenzunehmen. Neben dem aktuellen Jahresbericht sowie den wichtigsten Gesetzestexten konnten Besucherinnen und Besucher des Informationsstands Ratgeber zum Datenschutz in sozialen Netzwerken, bei Bild-, Ton- und Videoaufnahmen in der Kita oder zum Schutz der Privatsphäre als Mieterinnen und Mieter mitnehmen. Die großen und kleinen Besucherinnen und Besucher des Stands konnten zudem ihre Datenschutzkenntnisse beim Datenschutzquiz testen und Einblicke in unser neues medienpädagogisches Angebot www.data-kids.de nehmen.

Der Umstellungsprozess der im Frühjahr 2018 gestarteten, vollständig überarbeiteten **Kinderwebseite** der BlnBDI **www.data-kids.de** ist nun gestalterisch abgeschlossen. Allerdings sollen die Inhalte auch weiter kontinuierlich ergänzt werden. Die Kinderwebseite bietet ein umfassendes medienpädagogisches Informationsangebot, das in vielerlei Weise eingesetzt werden kann. Grundschulkinder, Lehrkräfte und Eltern finden hier neben einem kindgerechten Begriffslexikon auch Spiele, Erklärvideos, Arbeitshefte, Bastelvorlagen und andere Materialien, die dabei helfen, sich in der Welt des Datenschutzes besser zurechtzufinden. Als Ergänzung zur Kinderwebseite bieten wir zumindest in der Anfangszeit Projekttage für Schulen an, um die Materialien zu testen und Sensibilität für das Thema Datenschutz zu entwickeln.[305]

305 Siehe 5.6

Wir erhalten sehr viele **Beratungsanfragen** von öffentlichen und nicht öffentlichen Stellen. Auch zahlreiche allgemeine Anfragen von Bürgerinnen und Bürgern, Unternehmen, Behörden, freiberuflich tätigen Personen, Vereinen, Verbänden etc. zu verschiedenen Themen gehen bei uns ein. Die meisten davon stehen im Zusammenhang mit der Umsetzung der DS-GVO. Viele dieser individuellen Beratungsanfragen mussten wir auch in diesem Jahr aus Kapazitätsgründen leider ablehnen.

Gleichwohl hielten sowohl die BlnBDI als auch ihre Mitarbeiterinnen und Mitarbeiter auch in diesem Jahr über 40 **Vorträge** im Rahmen von Schulungen, Workshops, Fachtagen und Vorlesungen. Der Bedarf war und ist allerdings viel größer. So konnten z.B. trotz zahlreicher Nachfragen nur einige wenige Seminare und Fortbildungsveranstaltungen für Datenschutzbeauftragte bzw. Datenschutzjuristinnen und -juristen angeboten werden. Auch der Verwaltungsakademie Berlin, die dringend Dozentinnen und Dozenten zu verschiedenen Themen im Bereich der Aus- und Fortbildung sucht, mussten wir leider eine Absage erteilen.

Die DS-GVO stand in diesem Jahr auf der Themenliste der Vorträge an erster Stelle. Allein zum Thema „Ein Jahr Datenschutz-Grundverordnung – Erfahrungen aus der aufsichtsbehördlichen Praxis" wurden 10 Vorträge gehalten: bei Verbänden, Non-Profit-Organisationen, freien Trägern, auf Kongressen, in Fachausschüssen und im Rahmen einer Ringvorlesung an der TU Berlin. Es gab aber auch zahlreiche Fachvorträge zu konkreten Fragen der Anwendung der Regelungen der DS-GVO und zu den sich daraus ergebenden Konsequenzen bzw. Problemen:

- Grundzüge der DS-GVO
- Anforderungen an eine „perfekte Beschwerde" gemäß DS-GVO
- Verhaltensregeln gemäß Art. 40 DS-GVO
- Rolle des Betriebsrats im Rahmen der DS-GVO
- Die DS-GVO in der Praxis und aus Sicht der BlnBDI
- Probleme der Berliner Wirtschaft bei der Umsetzung und Anwendung der DS-GVO; Verbesserungsvorschläge und Handlungsanleitungen
- Europäische Datenschutz-Grundverordnung in der Kinder- und Jugendhilfe

Schon zum 16. Mal fand in der Hochschule für Technik und Wirtschaft Berlin (HTW) vom 2. bis 23. November die **Vorlesungsreihe der KinderUni Lichtenberg**

(KUL) statt – ein jährliches Angebot für alle wissbegierigen Mädchen und Jungen im Alter ab acht Jahren. An den Sonnabenden gibt es zur gleichen Zeit immer Veranstaltungen für Eltern rund um Fragen der Erziehung, zu Familienleben und Schule. Regelmäßig bieten wir auch dort Vorträge an. Am 23. November fand eine Info- und Gesprächsrunde zum Umgang mit sozialen Medien statt, die auf großes Interesse gestoßen ist. Vorträge zum Thema „Datenschutz in sozialen Netzwerken", „Tipps zum Datenschutz im Internet" sowie „Check: WhatsApp – Möglichkeiten, Gefahren, Alternativen" werden von uns auch über das Jahr verteilt im Rahmen der KUL *unterwegs*[306] für interessierte Schulen angeboten.

Auf regelmäßig großes Interesse stoßen auch Vorträge und Schulungen zu anderen datenschutzrechtlichen Themen und zur Arbeit unserer Behörde. Hier einige Beispiele:

- Datenschutz und Informationssicherheit in der Arbeit bei Gericht und Staatsanwaltschaft
- Einwilligungen im Beschäftigungskontext
- Fragen zum Beschäftigtendatenschutz
- Datenschutz im Verkehrsbereich
- Strukturen, Arbeitsweisen und datenschutzrechtliche Bestimmungen im Jugendamt und in der Polizei Berlin – Möglichkeiten und Grenzen von Kooperationen
- Aktuelle Themen der Datenschutzaufsicht
- Praxisbericht – Aktuelles von der Aufsichtsbehörde
- Grundzüge der Arbeit, Aufgaben und Organisation der BlnBDI
- Die Vollzugspraxis der Aufsichtsbehörde – Aktuelles und Ausblick

Wir werden unsere Aktivitäten im Bereich der Öffentlichkeitsarbeit und unser medienpädagogisches Angebot in den nächsten Jahren weiter ausbauen, um dem dringenden Bedarf an datenschutzrechtlicher Aufklärung, Schulung und Beratung nachkommen zu können.

306 KUL *unterwegs* ist die KinderUni, die an die Schule kommt – mit Vorlesungen, Workshops sowie Ideen für Exkursionen. Das kostenlose Angebot richtet sich an verschiedene Klassen- bzw. Altersstufen und alle Schulen in Lichtenberg und Treptow-Köpenick, in Wuhletal und Berlin-Buch.

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.
App	Anwendungsprogramm für Mobiltelefone
Artikel-29-Datenschutzgruppe	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.
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

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.
Dashcam	Als Dashcam wird eine Videokamera bezeichnet, die am Armaturenbrett (engl. dash board) oder an der Windschutzscheibe eines Fahrzeugs befestigt ist.
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 verein-

heitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewärleistet werden. Die Verordnung ersetzt die aus dem Jahr 1995 stammende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Sie ist bereits am 24. Mai 2016 in Kraft getreten, wurde aber aufgrund einer zweijährigen Übergangsfrist erst am 25. Mai 2018 wirksam. Seitdem ist sie in allen Mitgliedstaaten der Europäischen Union unmittelbar anwendbar.

DSK

Die Datenschutzkonferenz (DSK) besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.

EDSA

Der Europäische Datenschutzausschuss (EDSA) ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beiträgt und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördert. Der EDSA besteht aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten (EDSB).

EG / Erwägungsgrund

Erwägungsgründe sind Erklärungen des Gesetzgebers zum eigentlichen Gesetzestext, die diesem regelmäßig bei europäischen Rechtsvorschriften beigefügt werden.

eID

„Elektronische Identität" - Dabei handelt es sich um einen elektronischen Identitätsnachweis (mit Chip), mit dessen Hilfe elektronische Vorgänge ausgeführt werden können.

Ende-zu-Ende-Verschlüsselung	Der Inhalt einer Datenübertragung wird so verschlüsselt, dass nur 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.
Gemeinsamer Bundesausschuss	Der Gemeinsame Bundesausschuss (GBA) wird von den vier großen Selbstverwaltungsorganisationen, der Kassenärztlichen Bundesvereinigung, der Kassenzahnärztlichen Bundesvereinigung, der Deutschen Krankenhausgesellschaft und dem Spitzenverband Bund der Krankenkassen gebildet. Er ist das höchste Beschlussgremium der gemeinsamen Selbstverwaltung im deutschen Gesundheitssystem und bestimmt in Form von Richtlinien Maßnahmen der Qualitätssicherung für Praxen und Krankenhäuser.

Geodaten	Digitale geologische Daten, die z. B. in Navigationssystemen verarbeitet werden.
GovData	Datenportal 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 Ausgangsdaten wie beispielsweise einem Dokument oder auch nur einem Wort bzw. einer Telefonnummer einen eindeutigen Hashwert mit fester Länge berechnet.
Informierte Einwilligung	Als „Informierte Einwilligung“ bezeichnet man eine Einwilligungserklärung, bei welcher die Nutzer nach vorheriger, vollständiger Information über die geplante Verarbeitung ihrer Daten, deren Art, Umfang und Zweck der Verarbeitung dieser dann eindeutig zugestimmt haben.
Integrität	Unter der Wahrung der Integrität von Daten versteht man ihren Schutz vor 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.
LABO	Das Landesamt für Bürger- und Ordnungsangelegenheiten ist eine der Senatsverwaltung für Inneres und Sport nachgeordnete Behörde. Es ist für Bürgerinnen und Bürger, Unternehmen und Behörden auf den Gebieten der Wiedergutmachung, des Personenstands- und Einwohnerwesens und des Kraftfahrzeugwesens tätig.
LaGeSo	Das Landesamt für Gesundheit und Soziales ist eine der Senatsverwaltung für Integration, Arbeit und Soziales nachgeordnete Behörde. Es ist in den Aufgabenbereichen Gesundheit, Soziales und Versorgung tätig.
Link	Verweis oder Sprung zu einem elektronischen Dokument
Marktortprinzip	Die DS-GVO ist anwendbar, sobald ein Unternehmen Waren und Dienstleistungen für Personen in der Europäischen Union anbietet oder das Verhalten von Bürgerinnen und Bürgern beobachtet und in diesem Zusammenhang personenbezogene Daten verarbeitet. Der Anwendungsbereich der DS-GVO erfasst damit auch außereuropäische Unternehmen, die auf dem europäischen Markt aktiv sind, selbst wenn sie keine Niederlassung in der Europäischen Union haben. Durch das

Marktortprinzip sollen einheitliche Wettbewerbsbedingungen für alle Unternehmen geschaffen werden, die auf dem europäischen Markt Waren und Dienstleistungen anbieten.

Messenger-Dienst

Telekommunikationsdienst, bei dem zwei oder mehr Teilnehmer Textnachrichten (ggf. auch Audio- oder Video-Nachrichten sowie weitere Dateien) so austauschen, dass die Nachrichten möglichst unmittelbar bei den Empfängern ankommen.

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 Kurznachrichtendienst eingestellt werden. Es geht beim Mikroblogging nicht darum, thematisch in die Tiefe zu gehen, sondern innerhalb kurzer Zeit und ohne großen Aufwand Nachrichten aller Art zu produzieren.

Neuronale Netze

Künstliche Neuronale Netze sind in der Regel an den Organisationsprinzipien und den Lernprozessen des menschlichen Gehirns orientierte Computermodelle.

One-Stop-Shop

Das One-Stop-Shop-Prinzip 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
Opt-in / Opt-out	Opt-in meint, das eine Datenverarbeitung nur zulässig ist, wenn die betroffene Person sich ausdrücklich dafür entschieden hat, also in der Regel ihre Einwilligung gegeben hat. Bei einem Opt-out-Verfahren dagegen muss die betroffene Person ausdrücklich aktiv werden, um die Datenverarbeitung zu verhindern.
Opt-Out-Modell	„Opt-Out-Modell" bezeichnet ein Verfahren, das die Einwilligung annimmt, wenn dieser nicht innerhalb eines vorher festgelegten Zeitraums widersprochen wurde.
Pixel	Kleine Grafiken auf Webseiten, die meist nur 1×1 Pixel messen und beim Aufruf einer Webseite von einem Server geladen werden. Das Herunterladen wird registriert und kann für Auswertungen im Bereich des Online-Marketings genutzt werden.
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.
Public Consultation	dt. öffentliche Konsulation – Vor der Verabschiedung von Leitlinien führt der Europäische Datenschutzausschuss (EDSA) öffentliche Konsultationen durch, um die Ansichten und Anliegen aller Interessenträgerinnen, Interessenträger, Bürgerinnen und Bürger zu hören. In der Regel werden Leitlinien vor ihrer endgültigen Verabschiedung auf der Internetseite des EDSA veröffentlicht. Dann besteht in der Regel für sechs bis acht Wochen die Möglichkeit, die Leitlinie zu kommentieren.

Hauptsächlich machen Wirtschaftsverbände und Unternehmen von dieser Möglichkeit Gebrauch. Der ESDA erhält aber auch Feedback von zivilgesellschaftlichen Gruppen sowie Bürgerinnen und Bürgern. Nach Ablauf der Konsultationsphase entscheidet der EDSA, welche Änderungswünsche berücksichtigt werden.

Quellcode

Der Programmcode (technische Grundlage) einer Software

Ringspeicher

Ein Ringspeicher speichert Daten kontinuierlich in einem gewissen Zeitraum und überschreibt diese nach Ablauf einer vorgegebenen Zeit wieder, um den Speicherplatz für neue Daten freizugeben.

Score-Wert

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

Social Plugins oder auch Social Media Plugins verbinden Webseiten oder Apps mit sozialen Netzwerken. Betreiberinnen und Betreiber fügen einen Programmcode in den Quellcode ihrer Webseite oder App ein, der automatisch Daten zum Betreiber des sozialen Netzwerks sendet und von diesen Daten abruft. Der Betreiber des sozialen Netzwerks erfährt so, wofür sich die Besucherinnen und Besucher der Webseite interessieren, und kann mittels Profiling Persönlichkeitsprofile erstellen und Werbung personalisieren. Der Betreiber kann beispielsweise anzeigen, dass Bekannte der Webseiten-Besucherin bzw. des Webseiten-Besuchers die Webseite mit „Gefällt mir" markiert haben. Durch Social

	Plugins können insbesondere durch Netzwerkeffekte erhebliche Besuchszahlen für Webseiten und in der Folge regelmäßig erhebliche Umsätze generiert werden.
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.
Telematiktarif	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	Tracking ist im Verständnis der Datenschutz-Aufsichtsbehörden das Protokollieren und Auswerten des Verhaltens von Besucherinnen und Besuchern von Webseiten oder Apps zur in der Regel webseitenübergreifenden Nachverfolgung. Die Anwendungsgebiete reichen von einer reinen Reichweitenmessung über statistische Auswertung etwa nach Browser, Betriebssystem, Spracheinstellungen sowie Aufenthalts-Land und Tests zur Benutzerfreundlichkeit von Webseiten bis zur detaillierten Beobachtung und Aufzeichnung sämtlicher Mausbewegungen und Eingaben sowie zur webseiten- und geräteübergreifenden Erstellung von Nutzungs- und Persönlichkeitsprofilen zu Werbezwecken.
Tracking / Cookie Walls	Verhinderung der Nutzung einer Webseite bei Nichtakzeptieren von Cookies
Verhaltensregeln	engl. Code of conduct - Es handelt sich dabei um ein Instrument der Selbstregulierung. Gemäß Art. 41 DS-GVO können Verbände und andere Vereinigungen Verhaltensregeln ausarbeiten, mit denen die Anwendung der

DS-GVO präzisiert wird. Aufgabe der Aufsichtsbehörden ist es, die Ausarbeitung solcher Verhaltensregeln zu fördern und zu genehmigen.

Verkehrsdaten

Technische Informationen, die bei der Nutzung eines Telekommunikationsdienstes anfallen, etwa bei einem Telefonanruf anrufende und angerufene Telefonnummer, Beginn und Ende der Verbindung und bei Telefonaten im Mobilfunknetz auch der Standort. Auch als Verbindungsdaten bezeichnet.

Wearable

Wearable Computer oder kurz Wearables sind Computer, die so klein sind, dass sie weder einen Raum ausfüllen noch einen Schreibtisch benötigen, sondern z. B. als Armband und Brille getragen oder in Kleidung eingearbeitet werden können. Während der Anwendung sind sie am Körper der Benutzenden befestigt und oftmals direkt mit dem Internet verbunden. So kann z. B. ein Blutdruckmessgerät, welches dauerhaft oder über einen längeren Zeitraum am Arm getragen wird, durchaus als Gerät aus dem Bereich Wearable Computing bezeichnet werden.

WIFI-Basisstationen

Gerät zur drahtlosen Datenübertragung; wird meist bei drahtgebundenen Internetzugängen verwendet, um mobilen Geräten in der Nähe eine Nutzung des Internets zu ermöglichen, ohne Kabel anschließen zu müssen.

WiFi-Tracking

Eine Technik, mit der Bewegungsverläufe von Personen anhand von Standortdaten verfolgt werden können, die unter Rückgriff auf das Smartphone dieser Personen erfasst werden.

Stichwortverzeichnis

A

B

C

D

E

F

G

H / I

J

K

L

M

N

O

P

Q / R

S

T

U

V

W

Z

Infothek der Berliner Beauftragten für Datenschutz und Informationsfreiheit

Tätigkeitsberichte: Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat von Berlin jährlich einen Bericht über ihre Tätigkeit vorzulegen. Neben aktuellen technischen und rechtlichen Entwicklungen wird darin über Schwerpunktthemen und Einzelfälle aus den jeweiligen Geschäftsbereichen berichtet. Der Tätigkeitsbericht wird von uns auch als Broschüre für die Bürgerinnen und Bürger veröffentlicht.

Ratgeber, 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.

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**.

Ein umfassendes medienpädagogisches Informationsangebot stellen wir auf unserer Kinderwebseite **www.data-kids.de** zur Verfügung. Dort finden Kinder, Lehrkräfte und Eltern umfangreiche Materialien, die dabei helfen, sich in der Welt des Datenschutzes besser zurechtzufinden.

Der Jahresbericht 2019 umfasst folgende Schwerpunkte:

Status unentbehrlich – Messenger-Dienste in Unternehmen und öffentlichen Einrichtungen; Künstliche Intelligenz; Adressvermietung für Werbung; Bußgeldkonzept; Die Kooperation der Datenschutzaufsichtsbehörden der EU nimmt Fahrt auf! – Die Servicestelle Europaangelegenheiten

www.datenschutz-berlin.de

be Berlin