Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

# Datenschutz und Informationsfreiheit

Jahresbericht 2017

# Jahresbericht 2017

## der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2017

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis ihrer Tätigkeit vorzulegen (§§ 29 Berliner Datenschutzgesetz, 18 Abs. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den am 7. April 2017 vorgelegten Jahresbericht 2016 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2017 ab.

Der Jahresbericht ist auch 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) 215 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: https://www.datenschutz-berlin.de

Gestaltung: april agentur GbR

Satz: Layoutmanufaktur.Berlin

Druck: ARNOLD group

# Inhalt

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

# Abkürzungsverzeichnis

| | |
|---|---|
| AGGVG | Gesetz zur Ausführung des Gerichtsverfassungsgesetzes Berlin |
| ASOG | Allgemeines Sicherheits- und Ordnungsgesetz |
| AufenthG | Aufenthaltsgesetz |
| BDSG | Bundesdatenschutzgesetz |
| BEEG | Bundeselterngeld- und Elternzeitgesetz |
| BGB | Bürgerliches Gesetzbuch |
| BGBl. | Bundesgesetzblatt |
| BGH | Bundesgerichtshof |
| BIK | Berliner Institut für Kriminalprävention |
| BIM | Berliner Immobilien Management GmbH |
| BlnAGBMG | Berliner Ausführungsgesetz zum Bundesmeldegesetz |
| BlnDSG | Berliner Datenschutzgesetz |
| BlnMDÜV | Verordnung zur Übermittlung von Meldedaten in Berlin |
| BMG | Bundesmeldegesetz |
| BR-Drs. | Bundesratsdrucksache |
| BT-Drs. | Bundestagsdrucksache |
| BVerwG | Bundesverwaltungsgericht |
| BVG | Berliner Verkehrsbetriebe |
| DGB | Deutscher Gewerkschaftsbund |
| DS-GVO | Europäische Datenschutz-Grundverordnung |
| DSK | Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder |
| DSFA | Datenschutz-Folgenabschätzung |
| ErwG | Erwägungsgrund |
| EU | Europäische Union |
| EuGH | Europäischer Gerichtshof |
| FAQ | Frequently Asked Questions, engl. für häufig gestellte Fragen |
| FZV | Fahrzeug-Zulassungsverordnung |
| GDG | Gesundheitsdienst-Gesetz |
| GG | Grundgesetz |
| GVBl. | Gesetz- und Verordnungsblatt für Berlin |

| | |
|---|---|
| GVG | Gerichtsverfassungsgesetz |
| GwG a. F. | Geldwäschegesetz, alte Fassung |
| IFG | Berliner Informationsfreiheitsgesetz |
| IFK | Konferenz der Informationsbeauftragten in Deutschland |
| ISBJ | Integrierte Software Berliner Jugendhilfe |
| ICDPPC | Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre |
| ICIC | Internationale Konferenz der Informationsfreiheitsbeauftragten |
| IP | Internet Protokoll |
| IT | Informationstechnik |
| IWGDPT | Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation (sog. Berlin Group) |
| JB | Jahresbericht |
| JI-Richtlinie | Europäische Datenschutz-Richtlinie für die Bereiche Justiz und Inneres |
| JVollzDSG | Justizvollzugsdatenschutzgesetz |
| KJSG | Kinder- und Jugendstärkungsgesetz |
| KTDat | Ausschuss für Kommunikationstechnologie und Datenschutz |
| KunstUrhG | Kunsturhebergesetz |
| LABO | Landesamt für Gesundheit und Soziales |
| LHO | Landeshaushaltsordnung Berlin |
| LBG | Landesbeamtengesetz |
| ÖPNV | Öffentlicher Personennahverkehr |
| OWiG | Gesetz über Ordnungswidrigkeiten |
| PAuswG | Personalausweisgesetz |
| SchfHwG | Schornsteinfeger-Handwerksgesetz |
| SGV IX | Sozialgesetzbuch IX |
| StGB | Strafgesetzbuch |
| StPO | Strafprozessordnung |
| StVG | Straßenverkehrsgesetz |
| UIG | Umweltinformationsgesetz |
| UPD | Unabhängige Patientenberatung Deutschland |
| VG | Verwaltungsgericht |
| VwVfG | Verwaltungsverfahrensgesetz |
| WHJ | Wirtschaftliche Jugendhilfe |

# Einleitung

2018 wird es zu einer Neuausrichtung des Datenschutzrechtes in Europa kommen: Ab dem 25. Mai wird die Datenschutz-Grundverordnung in allen Mitgliedstaaten der Europäischen Union unmittelbar anwendbar sein. Mit ihr wird damit erstmals ein komplettes Rechtsgebiet für alle europäischen Mitgliedstaaten verbindlich und im Detail geregelt. Die Datenschutz-Grundverordnung will ein europaweit einheitliches hohes Datenschutzniveau schaffen und dieses auch durchsetzen. Dem bisherigen Datenschutzflickenteppich soll ein Ende bereitet werden. Wahrlich ein bahnbrechender Schritt, der uns da bevorsteht, und zugleich eine riesige Herausforderung. Denn mit der Datenschutz-Grundverordnung ändern sich die Stellung, Aufgaben und Befugnisse meiner Behörde grundlegend.[1] Das Jahr 2017 stand dementsprechend auch deutlich im Zeichen dieser bevorstehenden Änderungen.

Die Datenschutzaufsichtsbehörden befinden sich in intensiven Vorbereitungen auf das neue Rechtssystem.[2] Staatliche Stellen, Unternehmen und nicht zuletzt auch die Bürgerinnen und Bürger müssen mit den neuen Regelungen und allen sich daraus ergebenden Rechten und Pflichten vertraut gemacht werden. Darüber hinaus muss das geltende nationale Datenschutzrecht an die neue Rechtslage angepasst werden. So steht auch das Berliner Landesrecht derzeit auf dem Prüfstand. Davon betroffen sind nicht nur die allgemeinen Regelungen des Berliner Datenschutzgesetzes, sondern auch die datenschutzrechtlichen Vorschriften in den bereichsspezifischen Landesgesetzen. Die entsprechenden Gesetzesanpassungen begleiten wir intensiv. Wir stehen dem Senat beratend zur Seite, um die jeweiligen landesrechtlichen Regelungen mit dem neuen europäischen Datenschutzrechtsrahmen in Übereinstimmung zu bringen.[3]

1 Siehe 16.1
2 Siehe 16.3
3 Siehe 1.1.2

Auf unserer neu gestalteten Homepage informieren wir fortwährend über aktuelle Entwicklungen und Grundsatzfragen zur europäischen Datenschutzreform.[4]

Außer von den Vorarbeiten für das neue Rechtssystem war das Jahr 2017 aber auch wieder geprägt von Diskussionen über Fragen von innerer Sicherheit und Privatheit, die in einem naturgegebenen Spannungsverhältnis stehen. Das Verhältnis von Position und Gegenposition unterliegt dabei stetigen Schwankungen. Nach den von Edward Snowden ausgelösten Veröffentlichungen über exzessive Überwachungspraktiken ausländischer Geheimdienste war der Vertrauensverlust insbesondere gegenüber staatlichen Institutionen immens. Die politischen Debatten waren geprägt von dem Bestreben, Maßnahmen zur Verhinderung einer allumfassenden staatlichen Überwachung zu ergreifen. Die Bundesregierung gab das Ziel aus, Deutschland zum „Verschlüsselungsstandort Nummer eins auf der Welt" zu machen.[5] Infolge von Terroranschlägen und Amokläufen hat sich der Schwerpunkt der politischen Diskussion jedoch deutlich verschoben. Staatliche Sicherheitsmaßnahmen erleben einen regelrechten Boom. Bereitwillig wird ihnen Vorrang gegenüber der informationellen Selbstbestimmung des Einzelnen eingeräumt.[6] Der Schutz personenbezogener Daten sowie die Herstellung einer Balance zwischen kollektiven Freiheitsrechten auf der einen und Sicherheitsbedürfnissen auf der anderen Seite treten zunehmend in den Hintergrund. Hingegen wäre gerade in Zeiten zunehmender Verunsicherung eine sachliche Abwägung unbedingt erforderlich, um nicht leichtfertig die Errungenschaften unserer freiheitlichen Demokratie zur Disposition zu stellen. Für diese in der Vergangenheit mühsam errungenen Bürgerrechte, die sich über die Jahre weiterentwickelt und verfestigt haben, werden wir international sehr beneidet. Wir sollten sie schützen, denn sie sind das Fundament unserer Gesellschaft und können in ihrer Bedeutung für unser Zusammenleben gar nicht hoch genug eingeschätzt werden. Dass meine Behörde als unabhängige Kontrollinstanz für das Grundrecht auf informationelle Selbstbestimmung einsteht, ist somit entscheidender denn je.

Datenschutz darf nicht zu einem Lippenbekenntnis verkommen. Ziel- und altersgruppengerechte Öffentlichkeitsarbeit verstehe ich daher als wesentlichen Teil

4 https://www.datenschutz-berlin.de/datenschutzreform.html

5 Digitale Agenda 2014-2017, S. 31; JB 2014, Einleitung

6 Siehe 1.2

meines gesetzlichen Auftrags; nicht zuletzt auch, um Erscheinungen wie dem sog. Privacy-Paradox[7] entgegenzuwirken. Es gilt, die Bedeutung und die Inhalte des Datenschutzes wie auch der Informationsfreiheit verstärkt und unablässig zu vermitteln. Auf unserer Homepage[8] stellen wir vielfältige Informationen für Bürgerinnen und Bürger, Wirtschaftsunternehmen und öffentliche Stellen zur Verfügung. Auch den Selbstdatenschutz möchten wir stärken: beispielsweise mithilfe der von uns entwickelten und kürzlich online gestellten Kinderwebseite www.data-kids.de, die Kinder bereits im Grundschulalter befähigen soll, souverän und verantwortungsvoll mit den eigenen Daten umzugehen.[9]

Das Jahr 2018 steht für uns im Wesentlichen, aber nicht ausschließlich, unter dem Vorzeichen der Datenschutz-Grundverordnung. Angesichts der mitunter tagesaktuell geprägten Suche nach Sicherheit wird es auch für 2018 unser Ziel sein, uns in der politischen wie gesellschaftlichen Debatte darüber, welchen Wert Privatsphäre haben soll, durch standfestes Eintreten für den Datenschutz Gehör zu verschaffen.

Berlin, den 23. März 2018

Maja Smoltczyk
Berliner Beauftragte für Datenschutz und Informationsfreiheit

7 Das Privacy-Paradox beschreibt das Phänomen, dass viele Menschen in Umfragen und persönlichen Gesprächen den Schutz der Privatsphäre als sehr wichtig einstufen, aber nur zu selten dazu bereit sind, tatsächlich etwas dafür zu tun bzw. Kosten dafür in Kauf zu nehmen.

8 www.datenschutz-berlin.de

9 Siehe 6.6

# 1 Schwerpunkte

## 1.1 Datenschutz-Grundverordnung

Am 25. Mai 2018 ist es soweit: Die Datenschutz-Grundverordnung („DS-GVO") wird wirksam. Gesetzgeber, Behörden, Unternehmen und Verbände haben sich in den letzten zwei Jahren akribisch auf dieses Datum vorbereitet. Aber welche praktischen Vorteile und Veränderungen bringt die DS-GVO den Bürgerinnen und Bürgern? Beleuchtet wird dies im folgenden Beitrag 1.1.1. „Ihre Rechte nach der Datenschutz-Grundverordnung".

Auch uns als Behörde stehen weitreichende Veränderungen aufgrund der DS-GVO bevor, u. a. weil unsere Behörde in ein komplexes System europäischer Datenschutzaufsicht eingegliedert wird (dazu mehr unter 1.1.2. „Unsere Vorbereitungen auf die Datenschutz-Grundverordnung"). Exemplarisch für die vielen inhaltlichen Neuerungen werden zudem zwei von Veränderungen besonders betroffene Bereiche vorgestellt: Verhaltensregeln (1.1.3.) und Datenschutzfolgeabschätzungen (1.1.4).

### 1.1.1 Ihre Rechte nach der Datenschutz-Grundverordnung

Die DS-GVO widmet ein ganzes Kapitel den Rechten der sog. betroffenen Personen. Darunter versteht die DS-GVO Bürgerinnen und Bürger, deren Daten von einem Unternehmen oder einer Behörde verarbeitet werden. Diese Rechte sollen dazu verhelfen, Datenschutz selbst in die Hand zu nehmen. Die Betroffenen sollen in die Lage versetzt werden, sich direkt an Unternehmen, Behörden oder andere Stellen zu wenden und sich auf diese Rechte zu berufen. Sollten dabei Probleme auftreten, besteht die Möglichkeit, die Aufsichtsbehörde einzuschalten.

**Transparenz und Auskunftsrechte**

Datenschutzrechte können nur dann wahrgenommen werden, wenn die Bürgerinnen und Bürger überhaupt wissen, welche Daten von welchen Stellen über sie

gespeichert und verarbeitet werden. Darüber den Überblick zu behalten, ist aufgrund der Digitalisierung von Wirtschaft und Gesellschaft nicht leicht. Deshalb wurden in der DS-GVO die Transparenzpflichten für datenverarbeitende Stellen erhöht.[10] Die mitzuteilenden Informationen reichen vom Zweck und der Dauer der Datenverarbeitung über die Kontaktdaten der oder des betrieblichen Datenschutzbeauftragten bis hin zu den Rechtsgrundlagen und dem Bestehen von Auskunfts- und Beschwerderechten. All diese Informationen müssen in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die bereits erfolgte oder die beabsichtigte Datenverarbeitung vermitteln. Sie müssen grundsätzlich ohne Aufforderung zugänglich gemacht werden. Darüber hinaus erhalten Bürgerinnen und Bürger durch die DS-GVO ein Auskunftsrecht.[11] Danach ist jede Stelle u. a. verpflichtet, auf Anfrage Auskunft zu erteilen, welche konkreten Daten zu der anfragenden Person verarbeitet werden.

### Recht auf Berichtigung

Wenn unrichtige Daten zu einer Person verarbeitet werden, kann diese deren Berichtigung verlangen.[12] Unvollständige Daten müssen unter Berücksichtigung des Zwecks der Verarbeitung vervollständigt werden.

### Recht auf Löschung („Recht auf Vergessenwerden")

Bei Vorliegen bestimmter in der DS-GVO aufgezählter Gründe haben Bürgerinnen und Bürger das Recht, die Löschung personenbezogener Daten zu verlangen.[13] Dies ist insbesondere dann der Fall, wenn die Daten zu dem Zweck, zu dem sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind, oder wenn eine Einwilligung widerrufen wurde und keine andere Rechtsgrundlage für die Datenverarbeitung vorhanden ist. Sind zu löschende Daten öffentlich gemacht worden, z. B. im Internet, besteht ein „Recht auf Vergessenwerden". Dieses soll u. a. dazu beitragen, dass sämtliche Links zu den entsprechenden Daten ebenfalls gelöscht werden.

10 Art. 12, 13 und 14 DS-GVO
11 Art. 15 DS-GVO
12 Art. 16 DS-GVO
13 Art. 17 DS-GVO

### Recht auf Datenübertragbarkeit

Neu eingeführt wurde das Recht, eine Kopie der eigenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten.[14] Dadurch sollen Bürgerinnen und Bürger in die Lage versetzt werden, ihre Daten zum Beispiel problemlos von einem sozialen Netzwerk zu einem anderen zu übertragen.

### Widerspruchsrecht

Grundsätzlich haben Bürgerinnen und Bürger durch die DS-GVO ein Widerspruchsrecht gegen die Verarbeitung sie betreffender personenbezogener Daten.[15] Dies gilt insbesondere bei Datenverarbeitungen zum Zwecke der Direktwerbung und – soweit es damit in Verbindung steht – auch beim sog. Profiling.[16] Auf dieses Recht muss spätestens bei der ersten Kommunikation, also z. B. im ersten Anschreiben, hingewiesen werden.

### Automatisierte Entscheidung im Einzelfall einschließlich Profiling

Betroffene Personen haben das grundsätzliche Recht, keiner automatisierten Entscheidung – einschließlich dem sog. Profiling[17] – unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.[18] Es muss die Möglichkeit der Anfechtung der Entscheidung, der Darlegung des eigenen Standpunktes und des menschlichen Eingreifens bestehen. Außerdem muss auf diese Rechte hingewiesen werden.[19]

### Beschwerderecht

Die DS-GVO stärkt die Position der betroffenen Personen, indem sie Beschwerderechte ausbaut und ihre Ausübung gerade gegenüber ausländischen Stellen erleichtert. Bisher waren die Kontrollmöglichkeiten der Berliner Aufsichtsbehörde für Datenschutz auf öffentliche und nicht öffentliche Stellen in Berlin beschränkt.

14 Art. 20 DS-GVO

15 Art. 21 DS-GVO

16 Profiling wird in Art. 4 Nr. 4 DS-GVO definiert als jede Art der automatisierten Verarbeitung personenbezogener Daten, um bestimmte persönliche Aspekte zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel einer natürlichen Person zu analysieren oder vorherzusagen.

17 Siehe Fn. 7

18 Art. 22 DS-GVO

19 Erwägungsgrund 71 DS-GVO

Da viele große Unternehmen, insbesondere Internetdienstleister, außerhalb der EU sitzen, liefen datenschutzrechtliche Regelungen bisher oft ins Leere, weil ihnen gegenüber keine Kontrollmöglichkeiten bestanden. Zukünftig können sich betroffene Personen bei uns auch über Datenverarbeitungen ausländischer Unternehmen innerhalb und außerhalb der EU beschweren. Wir werden dann zumindest am aufsichtsbehördlichen Verfahren beteiligt und können gemeinsam mit anderen europäischen Aufsichtsbehörden darauf hinwirken, dass die Datenschutzrechte gewahrt werden.[20]

### Verbesserter Schutz von Minderjährigen

Kinder und Jugendliche stehen unter dem besonderen Schutz der DS-GVO. Sie sind sich der Risiken und Folgen bei der Verarbeitung ihrer personenbezogenen Daten möglicherweise weniger bewusst, auch kennen sie nicht unbedingt ihre Rechte. Gerade bei der Verwendung ihrer Daten für Werbezwecke oder der Erstellung von Persönlichkeits- und Nutzungsprofilen sollen Minderjährige besonders geschützt werden. Daher sind verschiedene Schutzmechanismen vorgesehen.

So gelten die oben beschriebenen Transparenzpflichten besonders für Minderjährige. Die Daten verarbeitenden Stellen müssen ihren Informationspflichten ihnen gegenüber in einer altersgerechten, d. h. in einer klaren und verständlichen Form nachkommen.

Nur Minderjährige, die das 16. Lebensjahr vollendet haben, können selbst in die Verarbeitung ihrer Daten einwilligen, wenn sie Dienste der Informationsgesellschaft, z. B. soziale Netzwerke, Streaming-Dienste, Online-Spiele etc., nutzen. Haben Minderjährige in die Verarbeitung ihrer Daten eingewilligt, soll ihnen im Erwachsenenalter die Möglichkeit zustehen, eine Löschung ihrer Daten zu verlangen, die sie seinerzeit freiwillig z. B. in sozialen Netzwerken eingestellt haben.

20 Art. 55 ff. DS-GVO

## 1.1.2 Unsere Vorbereitungen auf die Datenschutz-Grundverordnung

Die DS-GVO stärkt die Rechte der betroffenen Personen.[21] Für Unternehmen und öffentliche Stellen ergeben sich ebenfalls zahlreiche Änderungen.[22] Aber auch für uns als Aufsichtsbehörde bringt die DS-GVO viele Neuerungen. Wir nutzen den Übergangszeitraum bis zum 25. Mai 2018 intensiv, um uns darauf vorzubereiten.

Auch für die Aufsichtsbehörden sieht die DS-GVO neue Aufgaben und Pflichten vor. Vor diesem Hintergrund müssen interne Prozesse überprüft und angepasst werden. Spezielle Zuständigkeiten in unserer Geschäftsverteilung wurden geschaffen. Zugleich wurde in der gesamten Dienststelle eine Bestandsaufnahme durchgeführt, um festzustellen, an welchen konkreten Stellen Anpassungsbedarf in den Arbeitsprozessen besteht. So ist sichergestellt, dass über den gesamten Zuständigkeitsbereich unserer Dienststelle inklusive der übergeordneten organisatorischen Fragen der Änderungsbedarf erfasst wurde.

Der ermittelte Anpassungsbedarf wurde zu Arbeitspaketen geschnürt und Verantwortlichen zur Umsetzung übertragen. In monatlichen Projekttreffen werden Informationen zum aktuellen Sachstand der Arbeitspakete sowie weiterer Entwicklungen zur DS-GVO ausgetauscht. Dieser Austausch wird auch genutzt, um immer wieder die Vollständigkeit der Arbeitspakete zu überprüfen.

Die gesamte Dienststelle wird regelmäßig in kurzen Veranstaltungen über wichtige Neuerungen informiert. Diese betreffen u. a. etwa die zukünftigen Anforderungen an Einwilligungen und Sanktionen; im Rahmen dieser Veranstaltungen wird aber auch über neue Hilfsmittel und Positionen zu Auslegungsfragen informiert und diskutiert. Um sich für die zukünftige intensivere Zusammenarbeit mit Aufsichtsbehörden anderer Mitgliedstaaten der EU vorzubereiten, wird verstärkt Englischunterricht für die Beschäftigten gefördert.

21 Siehe 1.1.1

22 JB 2016, 1.2.2 bis 1.2.5

Besonders aufgrund des Marktortprinzips[23], des One-Stop-Shop-Verfahrens[24] und des Kohärenzverfahrens[25], das nach einem festgelegten Verfahren der Zusammenarbeit der europäischen Aufsichtsbehörden verbindliche Beschlüsse durch einen neuen Europäischen Datenschutzausschuss vorsieht, werden nachhaltige Veränderungen erforderlich. Wir müssen in Zukunft grenzüberschreitende Fälle identifizieren und dann in komplizierten Abstimmungsverfahren in einen Austausch mit anderen europäischen Aufsichtsbehörden treten.

Aber auch im Übrigen muss unser Verfahren zur Bearbeitung von Beschwerden angepasst werden. Zu nennen ist hier insbesondere unsere Pflicht, das Einreichen von Beschwerden zu erleichtern, z. B. durch das Bereitstellen eines elektronischen Beschwerdeformulars.[26] Zudem müssen auch wir sicherstellen, dass unsere Informationen für Beschwerdeführer den Anforderungen der DS-GVO genügen.[27]

### 1.1.3 Verhaltensregeln – Mehrwert für den Datenschutz

Die DS-GVO enthält zahlreiche unbestimmte Rechtsbegriffe wie „erforderlich", „berechtigte Interessen", „Interessen der betroffenen Person" oder „in einer für die betroffenen Person nachvollziehbaren Weise verarbeitet". Zudem sind Abwägungserfordernisse vorgesehen.[28] Bei der praktischen Anwendung der DS-GVO werden sich daher viele Fragen zur Auslegung dieser Begriffe stellen. Hilfreich können hierbei Verhaltensregeln[29] bestimmter Branchen sein. Darunter sind Regelungen zu verstehen, die sich etwa Berufsverbände selbst geben. Sie konkretisieren den von der DS-GVO vorgegebenen Rahmen in enger Abstimmung mit den Aufsichtsbehörden.

23 Art. 3 Abs. 2 DS-GVO
24 Siehe 1.1.1
25 Art. 63 ff. DS-GVO
26 Art. 57 Abs. 2 DS-GVO; das Formular finden Sie unter datenschutz-berlin.de/beschwerde.html
27 Art. 12 ff., Art. 77 f. DS-GVO
28 Siehe etwa Art. 6 Abs. 1 lit. f DS-GVO
29 Diese Verhaltensregeln werden auch als Code of Conduct bezeichnet.

Bereits die Datenschutz-Richtlinie 95/46/EG[30] und das Bundesdatenschutzgesetz[31] kannten Verhaltensregeln. Ziel der DS-GVO ist es, die Selbstregulierung durch Verhaltensregeln weiter zu stärken. Gefördert werden soll insbesondere die Ausarbeitung von Verhaltensregeln, die die Besonderheiten und Bedürfnisse von Kleinst-, kleinen und mittleren Unternehmen berücksichtigen.[32]

Die DS-GVO nennt beispielhaft Bereiche, für die Verhaltensregeln ausgearbeitet werden können.[33] So erscheint es sinnvoll, für eine bestimmte Branche zu konkretisieren, worin eine faire und transparente Verarbeitung besteht und in welchen Fällen eine Erhebung personenbezogener Daten überhaupt erforderlich ist. Aber z. B. auch die Vorgaben zum Datenschutz durch Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen können bereichsspezifisch genauer definiert werden.[34] Es gibt grundsätzlich keine Beschränkungen der Regelungsbereiche für Verhaltensregeln. Inhaltlich müssen sie jedoch eine konkretisierte Beschreibung des Umgangs mit personenbezogenen Daten beinhalten oder in einer anderen Form einen Mehrwert schaffen. Eine reine Wiederholung des Wortlauts der DS-GVO reicht hierfür nicht aus. Des Weiteren dürfen die vorgeschlagenen Regelungen nicht im Widerspruch zur DS-GVO stehen.

Verhaltensregeln setzen eine Genehmigung der zuständigen Aufsichtsbehörde voraus.[35] Sie können weder neue Rechtsgrundlagen für eine Datenverarbeitung schaffen noch die Aufgaben und Befugnisse der Aufsichtsbehörden beschränken. Genehmigte Verhaltensregeln bieten allerdings eine erhöhte Rechtssicherheit, wie in bestimmten Konstellationen mit personenbezogenen Daten in zulässiger Weise umgegangen werden darf. Sie können insbesondere die teilweise sehr abstrakten Regelungen der DS-GVO bezogen auf eine bestimmte Branche konkretisieren und so ihre Anwendbarkeit fördern.

30 Art. 27 Richtlinie 95/46/EG
31 § 38a BDSG
32 Art. 40 Abs. 1 DS-GVO
33 Art. 40 Abs. 2 lit. a bis k DS-GVO
34 Siehe hierzu Art. 25 DS-GVO
35 Art. 40 Abs. 5 Satz 2 DS-GVO

Antragsberechtigt sind Verbände oder andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten. [36] Infrage kommen insoweit insbesondere Branchen- und Berufsverbände, aber auch Kammern, die für ihre Mitglieder Regelungen festlegen wollen. Nicht antragsberechtigt sind Konzerne. Der Antrag auf Genehmigung der Verhaltensregeln ist bei der zuständigen Aufsichtsbehörde zu stellen.[37] Dies ist in der Regel die Aufsichtsbehörde am Sitz des Antragstellers. Da die meisten Verbände und Vereinigungen ihren Sitz in Berlin haben, wird die Mehrzahl der in Deutschland beantragten Verhaltensregeln durch die Berliner Aufsichtsbehörde geprüft und genehmigt werden. Für Verhaltensregeln, die die Verarbeitung personenbezogener Daten bei der Erbringung von Post- und Telekommunikationsdiensten betreffen, ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die zuständige Aufsichtsbehörde.

Beziehen sich die vorgelegten Verhaltensregeln nicht auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten der EU, kann die zuständige Aufsichtsbehörde diese unmittelbar genehmigen.[38] Sie muss allerdings zu der Auffassung gelangt sein, dass die Verhaltensregeln ausreichend geeignete Garantien bieten. Die Genehmigung erfolgt in der Form eines Verwaltungsaktes, der – bezogen auf Deutschland – auch die anderen Aufsichtsbehörden bindet. Die genehmigten Verhaltensregeln sind von der zuständigen Aufsichtsbehörde in ein Verzeichnis aufzunehmen und zu veröffentlichen.

Etwas anderes gilt, wenn sich Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten der EU beziehen. Denkbar ist etwa, dass ein europäischer Branchenverband Verhaltensregeln für alle Mitgliedsunternehmen in ganz Europa erarbeitet. In diesem Fall hat die für den Hauptsitz des europäischen Branchenverbandes zuständige Aufsichtsbehörde vor einer Entscheidung über deren Genehmigung ein besonderes Abstimmungsverfahren zu beachten. Nach den Regeln des Kohärenzverfahrens[39] ist eine Stellungnahme des Europäischen Datenschutzausschusses einzuholen.[40] Hält dieser die Verhaltensregeln für vereinbar mit der DS-GVO, übermittelt er seine Stellungnahme zusätzlich an die

36 Art. 40 Abs. 2 DS-GVO
37 Art. 40 Abs. 5 Satz 2, Art. 55 DS-GVO
38 Art. 40 Abs. 5 DS-GVO
39 Art. 63, 64 Abs. 1 Satz 2 lit. b DS-GVO
40 Art. 40 Abs. 7 DS-GVO

EU-Kommission. Diese kann dann die Verhaltensregeln für in der Europäischen Union allgemein gültig erklären.[41]

Für die Überwachung der Einhaltung der Verhaltensregeln kann eine Kontrollstelle akkreditiert werden.[42] Diese hat die Aufgabe und die Befugnis, die Einhaltung der Verhaltensregeln zu überwachen. Bei festgestellten Verstößen gegen die Verhaltensregeln kann sie gegenüber dem jeweiligen Unternehmen Maßnahmen ergreifen. Hierzu gehört auch ein vorläufiger oder endgültiger Ausschluss von den Verhaltensregeln. Die Zuständigkeit der Aufsichtsbehörde wird dadurch allerdings nicht beschränkt.

Die DS-GVO spricht Verhaltensregeln an unterschiedlichen Stellen an. Bei der Auftragsverarbeitung kann die Einhaltung genehmigter Verhaltensregeln als ein Faktor herangezogen werden, um hinreichende Garantien dafür nachzuweisen, dass die Datenverarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.[43] Gleiches gilt für die allgemeinen Nachweispflichten[44], dass eine Verarbeitung entsprechend der DS-GVO erfolgt, sowie für den Nachweis der Sicherheit der Verarbeitung[45]. Bei der Datenschutz-Folgenabschätzung[46] ist zudem die Einhaltung genehmigter Verhaltensregeln gebührend zu berücksichtigen.[47] Im Rahmen von Datenübermittlungen in ein Drittland kann die Einhaltung von genehmigten Verhaltensregeln eine Rolle spielen.[48] Nicht zuletzt sind bestehende Verhaltensregeln auch bei der Entscheidung über Geldbußen zu berücksichtigen.[49] Der konkrete gesetzliche Mehrwert für die Einhaltung genehmigter Verhaltensregeln ist somit nicht zu unterschätzen.

41 Art. 40 Abs. 9 DS-GVO
42 Art. 41 DS-GVO
43 Art. 28 Abs. 5 DS-GVO
44 Art. 24 Abs. 3 DS-GVO
45 Art. 32 Abs. 3 DS-GVO
46 Siehe 1.1.4
47 Art. 35 Abs. 8 DS-GVO
48 Art. 46 Abs. 2 lit. e DS-GVO
49 Working Paper 253 der Art. 29-Gruppe, S. 15

Durch Verhaltensregeln ist ein Gewinn an Rechtssicherheit für den Umgang mit personenbezogenen Daten in bestimmten Bereichen möglich. Dies hilft nicht nur den Verantwortlichen und Auftragsverarbeitern, sondern auch den Aufsichtsbehörden bei ihrer Arbeit.

### 1.1.4 Hohe Risiken richtig behandeln: Die Datenschutz-Folgenabschätzung

Die im Mai 2018 wirksam werdende DS-GVO sieht als ein neues Instrument für die Sicherstellung des Datenschutzes bei Verfahren mit hohen Risiken für die Rechte und Freiheiten der betroffenen Personen eine sog. Datenschutz-Folgenabschätzung vor.[50]

Eine Datenschutz-Folgenabschätzung (DSFA) soll den Unternehmen und Behörden helfen, Datenverarbeitungen, die mit hohen Risiken für die betroffenen Bürgerinnen und Bürger verbunden sind, angemessen auszugestalten. Sie tritt an die Stelle der bisherigen Vorabkontrolle, die nur im öffentlichen Bereich eine nennenswerte Anwendung gefunden hat. Die DSFA unterscheidet sich jedoch von der Vorabkontrolle in mehreren Aspekten: unter welchen Voraussetzungen sie verpflichtend durchzuführen ist, wer sie vornimmt und welche Ergebnisse zu erzielen sind.

**Verpflichtung zur Datenschutz-Folgenabschätzung**

Anknüpfungspunkt für die Verpflichtung für die Durchführung einer DSFA ist ein hohes Risiko für die betroffenen Personen durch eine Datenverarbeitung. Wenn Angaben über eine Person als Datum erfasst und verarbeitet werden, dann ist diese Person „betroffen". Im Zuge der Verarbeitung kann ihr ein Schaden entstehen. Je gravierender dieser mögliche Schaden und je höher die Wahrscheinlichkeit, dass er eintritt, desto höher ist das Risiko.

Das Gesetz erkennt materielle und immaterielle Schäden an. Ein materieller Schaden tritt z. B. ein, wenn einer betroffenen Person aufgrund der Verarbeitung unrechtmäßig eine Leistung verweigert oder sie im Geschäftsverkehr ungerecht-

50 Art. 35 DS-GVO

fertigt benachteiligt wird. Zu einer solchen Benachteiligung kann es kommen, wenn Krankheiten, an denen die Person leidet, oder gegen sie gerichtete strafrechtliche Maßnahmen bekannt werden.

Ein immaterieller Schaden kann in einer Rufschädigung bestehen, aber auch bereits in einer unrechtmäßigen Datenverarbeitung. Jede unrechtmäßige Verarbeitung von Daten über eine Person greift in das Recht dieser Person ein, im Rahmen des Gesetzes selbst darüber zu bestimmen, wer wie und für welche Zwecke mit Informationen über sie umgeht. Die unrechtmäßige Verarbeitung von Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen einer Person oder ihre Gewerkschaftszugehörigkeit hervorgehen, von biometrischen Daten, die sich zur eindeutigen Identifikation einer Person eignen, von Daten über strafrechtliche Verurteilungen und Straftaten, von Gesundheitsdaten oder von Daten zum Sexualleben oder zur sexuellen Orientierung ist als ein schwerer Schaden aufzufassen.

Eintrittswahrscheinlichkeiten für Schäden sind schwer einzuschätzen. Oft fehlen Erfahrungswerte. Es ist jedoch unumgänglich, wenigstens grob Schäden danach zu unterscheiden, ob sie mit hoher oder niedriger Wahrscheinlichkeit eintreten können. Anknüpfungspunkt ist eine Einschätzung der Risikoquellen. Eine Risikoquelle kann in der Konstruktion eines eingesetzten Geräts liegen, die zu Fehlfunktionen führen kann, aber auch in einem Angreifer, also einer Person oder Institution, die ein besonderes Interesse daran hat, den Schadensfall eintreten zu lassen. Fehlfunktionen in Bezug auf die Sicherheit eines Gerätes sind insbesondere dann gehäuft zu erwarten, wenn die mit ihm verbundene Software nicht mehr gewartet wird. Bei Angreifern sind ihre Zahl, Motivation und die ihnen zur Verfügung stehenden Mittel zu berücksichtigen.

Werden neue Technologien eingesetzt, so ist aufgrund der damit noch verbundenen Unsicherheiten in der Regel davon auszugehen, dass ihr Einsatz mit beträchtlicher Wahrscheinlichkeit zu Schäden führt. Sobald ausreichende Erfahrungswerte vorliegen, ersetzen sie diese summarische Einschätzung.

Generell kann man sagen, dass ein Risiko dann als hoch zu bewerten ist, wenn ein gravierender Schaden mit nicht zu vernachlässigender oder ein sonstiger Schaden mit beträchtlicher Wahrscheinlichkeit eintreten kann. Um den verant-

wortlichen Stellen die Einschätzung zu erleichtern, werden die Datenschutzaufsichtsbehörden eine Liste von Verarbeitungsvorgängen veröffentlichen, für die auf jeden Fall eine DSFA durchzuführen ist. Bereits in der DS-GVO selbst sind drei Typen von Verarbeitungen aufgeführt, die eine DSFA erfordern: Eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die zu Entscheidungen mit Rechtswirkung für die Betroffenen führt, umfangreiche Verarbeitungen von Daten der o. g. besonders sensiblen Art und die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche. Beispiele für diese drei Typen sind die Erstellung von Persönlichkeitsprofilen von Käuferinnen und Käufern auf Handelsplattformen im Internet, wenn diese zur Preisdifferenzierung genutzt werden, die Verwaltung von Patientenakten durch Krankenhäuser und die Verfolgung der individuellen Wege von Personen in Gebäudekomplexen durch Aufzeichnung der Signale, die konstant von den Mobilfunkgeräten dieser Personen versandt werden.

Bereits betriebene Verfahren müssen keiner DSFA unterzogen werden, sofern sie rechtskonform eingeführt und unter sonst gleichbleibenden Verhältnissen an die technische Entwicklung und an veränderte Risiken angepasst wurden. Wurde für ein Verfahren eine Vorabkontrolle nach alter Gesetzeslage durchgeführt, so hat diese weiter Bestand. Sollte jedoch die Vorabkontrolle selbst nicht den gesetzlichen Vorschriften genügt haben, z. B. weil sie im öffentlichen Bereich nicht auf eine Risikoanalyse und ein regelkonformes Sicherheitskonzept zurückgreifen konnte oder die Berliner Beauftragte für Datenschutz und Informationsfreiheit entgegen der gesetzlichen Regelung nicht beteiligt wurde, so tritt mit dem 25. Mai 2018 die Pflicht zur Erstellung einer DSFA und zur Umsetzung der durch sie bestimmten Maßnahmen ein.

### Handelnde Personen

Ein wesentlicher Unterschied zwischen neuer DSFA und bisheriger Vorabkontrolle besteht darin, dass die Durchführung nicht mehr der bzw. dem betrieblichen oder behördlichen Datenschutzbeauftragten zugewiesen ist. Sie wird nunmehr unmittelbar von der Leitung des Unternehmens bzw. der Behörde verantwortet. Diese wird in der Regel eine Projektgruppe mit der Durchführung beauftragen. Die Datenschutzbeauftragten haben dabei nur noch eine beratende Funktion. Es ist sinnvoll, fachlich Verantwortliche, IT-Personal und IT-Sicherheitsexperten sowie ggf. Vertreterinnen oder Vertreter von Dienstleistern oder Herstellern einzusetzender

Software an der Projektgruppe zu beteiligen. Für den Prozess der Erstellung einer DSFA stehen internationale Standards zur Verfügung, deren Anwendung grundsätzlich empfohlen wird. Es muss allerdings dabei darauf geachtet werden, dass die gesetzlichen Vorgaben stets Vorrang vor den Vorgaben der Standards haben.

Neu ist ebenfalls, dass die Verantwortlichen gehalten sind, die Standpunkte von betroffenen Personen oder sie vertretender Organisationen einzuholen und zu berücksichtigen, soweit dies möglich ist, ohne gewerbliche oder öffentliche Interessen zu beeinträchtigen. So muss ein Unternehmen zum Zweck dieser Konsultation neue Geschäftsideen nicht offenlegen. Stattdessen kann sie Personen, die zukünftig von der geplanten Verarbeitung betroffen wären, auch abstrakt befragen. Sollen beispielsweise Bewegungsprofile angelegt oder Kommunikationsvorgänge inhaltlich ausgewertet werden, so ist eine Befragung hierzu durchaus möglich, ohne den beabsichtigten Zweck dieser Verarbeitungen offenzulegen.

Die verantwortlichen Stellen können auch die Hilfe Dritter bei der Erstellung einer DSFA in Anspruch nehmen. Dies bietet sich an, da die Ausführung einer DSFA eine komplexe Aufgabe ist.

**Datenschutz-Folgenabschätzung für mehrere Verarbeitungsvorgänge**

Im Gegensatz zu einer Vorabkontrolle kann sich eine DSFA auf mehrere Verarbeitungsvorgänge erstrecken, wenn diese hinreichend ähnlich sind. Dies ist eine erhebliche Erleichterung gegenüber der bisherigen Vorabkontrolle, die jede verantwortliche Stelle für sich durchzuführen hatte. Auch bei gleichartigen Verarbeitungen musste z. B. jedes einzelne Bezirksamt eine Vorabkontrolle vornehmen, wenn eine neue Software berlinweit zum Einsatz kommen sollte. Zukünftig wird es möglich sein, eine DSFA für alle Bezirksämter oder Senatsverwaltungen des Landes Berlin zentral durchzuführen.

Die Durchführung einer DSFA für mehrere Verarbeitungen ist dann möglich, wenn diese inhaltlich ähnlich sind und im Wesentlichen zu den gleichen Risiken führen. Das Gesetz nennt als Beispiele gemeinsame Anwendungen oder Verarbeitungsplattformen mehrerer öffentlicher Stellen oder Verarbeitungsumgebungen für einen Wirtschaftssektor oder ein Marktsegment. Typische Verarbeitungsumgebungen sind cloudbasierte Dienste für spezifische Funktionen wie beispielsweise für die Vergabe von Terminen an Kunden. Unterscheiden sich allerdings die

Zwecke der Nutzer dieser Verarbeitungsumgebungen so stark, dass auch die Risiken stark variieren, kann eine gemeinsame DSFA nicht mehr gesetzeskonform durchgeführt werden. In diesem Fall empfiehlt es sich, die datenschutzrechtlich relevanten Eigenschaften der Plattform zu analysieren und die Ergebnisse der Analyse den Anwendenden für deren eigene DSFA zur Verfügung zu stellen.

Wann immer eine DSFA durch oder für mehrere Verantwortliche erstellt wird, muss jede dieser Stellen dafür Sorge tragen, dass die in der DSFA getroffenen Annahmen über den Kontext und die Einsatzumgebung der neuen Verfahren den tatsächlichen Verhältnissen in der eigenen Organisation entsprechen. Bei Abweichungen muss eine Anpassung der DSFA erfolgen.

### Inhalte der Datenschutz-Folgenabschätzung

Das Gesetz gibt explizite Vorgaben zum Inhalt einer DSFA. Die vorgesehenen Verarbeitungsvorgänge müssen beschrieben werden, ebenso die Zwecke, denen sie dienen sollen. Die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug auf den Zweck muss eingeschätzt werden. Diese Verhältnismäßigkeit ist jedenfalls dann nicht gegeben, wenn durch die Verarbeitung tief in die Privatsphäre der Betroffenen eingegriffen wird, um einen relativ banalen oder auch anderweitig einfach zu erreichenden Zweck zu verfolgen. Zusätzlich müssen die Risiken für die Rechte und Freiheiten der betroffen Personen bestimmt und bewertet werden. Und schließlich muss geklärt werden, wie diese Risiken bewältigt werden sollen. Zur Bewältigung werden je nach Situation vertragliche Regelungen abzuschließen, organisatorische Prozesse einzurichten und technische Vorkehrungen insbesondere in Bezug auf die Sicherheit der Verarbeitung zu treffen sein.

Die Maßnahmen müssen sich darauf richten, dass unbefugte, unrechtmäßige und über die festgelegten Zwecke hinausgehende Verarbeitungen ausgeschlossen werden, die Transparenz gegenüber den Betroffenen sowohl im Regelbetrieb als auch bei Verletzungen des Schutzes der personenbezogenen Daten gewahrt bleibt und dass nur die erforderlichen Daten verarbeitet und sie nur denjenigen und nur in dem Umfang zugänglich gemacht werden, wie dies für den Geschäftsprozess tatsächlich notwendig ist. Identifizierende Angaben müssen so früh wie möglich gelöscht, eine unbeabsichtigte Veränderung oder Vernichtung der Daten dagegen vermieden werden. Schließlich muss eine DSFA klären, wie die Einhaltung der datenschutzrechtlichen Vorschriften während des Betriebs nachgewiesen werden

soll. Hierzu gehört neben der im ersten Schritt der DSFA erfolgten Dokumentation der Verarbeitungsvorgänge auch die Sicherstellung, dass sie später im Einzelnen nachvollzogen werden können.

### Nach Abschluss der Datenschutz-Folgenabschätzung

Steht nach Abschluss der DSFA fest, dass auch bei Anwendung der vorgesehenen Maßnahmen noch hohe Risiken verbleiben, dann ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit zu konsultieren. Dazu muss die Stelle eine Reihe von Angaben und Unterlagen bereitstellen, darunter die DSFA selbst.[51] Weitere Unterlagen können angefordert werden. Eine zügige Beantwortung der Anfrage mit festen Fristen ist gesetzlich vorgegeben.

In der Regel werden im Rahmen dieser Konsultation von der Berliner Beauftragten Empfehlungen für die Umsetzung der Verarbeitung und möglicherweise zusätzlich zu ergreifende Maßnahmen gegeben. Die Antwort kann auch eine Warnung enthalten, dass die beabsichtigten Verarbeitungsvorgänge voraussichtlich gegen das Gesetz verstoßen werden. Schließlich ist es möglich, dass die beabsichtigte Verarbeitung beschränkt oder untersagt wird.

Liegen die Ergebnisse der DSFA – möglicherweise nach Ergänzung im Zuge der vorherigen Konsultation – vor, sind die Verantwortlichen verpflichtet, die darin festgehaltenen Maßnahmen umzusetzen, **bevor** die Verarbeitung aufgenommen wird. Auch im weiteren Verlauf ist regelmäßig zu bewerten, ob die Verarbeitung gemäß den Ergebnissen der DSFA erfolgt und ob die getroffenen Maßnahmen sich als ausreichend wirksam erwiesen haben.

Zu berücksichtigen ist, dass es sich hier um einen fortwährenden Prozess handelt. Die technische Entwicklung schreitet fort, neue Risiken entstehen und auch der Kontext und die Zwecke der Verarbeitungen können sich wandeln. Daher muss in regelmäßigen Abständen und aus Anlass wesentlicher neuer Risiken überprüft werden, ob Analyse und Schlussfolgerungen der DSFA noch tragfähig sind. Gegebenenfalls ist eine Überarbeitung vorzunehmen. Für Bestandsverfahren können wesentliche Änderungen dazu führen, dass erstmals die Verpflichtung zur Durchführung einer DSFA entsteht.

51 Art. 36 Abs. 3 DS-GVO

Mit der Verpflichtung, Datenschutz-Folgenabschätzungen vorzunehmen, kommt auf die privaten und öffentlichen Stellen im Land eine neue Verpflichtung zu. Sie kann nur erfüllt werden, wenn frühzeitig vor Aufnahme einer neuen Verarbeitung personenbezogener Daten ausreichende Ressourcen für den erforderlichen Erarbeitungsprozess bereitgestellt werden. Datenverarbeitungen, die potenziell hohe Risiken für die Rechte und Freiheiten von natürlichen Personen aufweisen, dürfen erst nach Vornahme der Datenschutz-Folgenabschätzung und Umsetzung ihrer Ergebnisse aufgenommen werden.

## 1.2 Volksbegehren Videoüberwachung

Seit September sammelt eine private Initiative[52] im Rahmen eines Volksbegehrens Unterschriften für mehr öffentliche Videoüberwachung in Berlin. Der von der Initiative hierzu vorgelegte Gesetzesentwurf[53] ist in seiner derzeitigen Form verfassungsrechtlich höchst bedenklich.

Dies beginnt bereits damit, dass der Gesetzesentwurf Regelungen enthält, für die das Land Berlin keine Gesetzgebungskompetenz hat, was jedoch Voraussetzung für ein zulässiges Volksbegehren ist.[54] So soll u. a. die Verlängerung der Frist zur Speicherung von Videoaufzeichnungen den Strafverfolgungsbehörden bei der Aufklärung von Straftaten helfen und es soll eine Anstalt des öffentlichen Rechts errichtet werden, die unter Beteiligung von Strafverfolgungsbehörden u. a. Videoüberwachungstechnik zu Strafverfolgungszwecken entwickeln soll.[55] Auch wirbt die Initiative in ihren Zielen und durch Einstellung von diversen Videos über erfolgreiche Öffentlichkeitsfahndungen auf ihrer Webseite mit einer verbesserten Aufklärung von Straftaten durch mehr Videoüberwachung. Mit diesen Inhalten und auch mit ihrem Namen macht die Initiative deutlich, worum es ihr geht: um Videoaufklärung, also Strafverfolgung, und nicht um Gefahrenabwehr mittels Videoüberwachung. Das Abgeordnetenhaus verfügt jedoch nicht über die Gesetz-

52 „Aktionsbündnis für mehr Videoaufklärung und Datenschutz"

53 „Artikel-Gesetz für mehr Sicherheit und Datenschutz in Berlin", abrufbar auf der Webseite der Initiative

54 Art. 62 Abs. 1 Satz 1 der Verfassung von Berlin

55 Siehe Fn. 1, 11, 20, 25 des Gesetzesentwurfs der Initiative

gebungskompetenz, in Berliner Gesetzen Strafermittlungsmaßnahmen wie z. B. Datenerhebungen zur Strafverfolgung oder hierbei speziell zur Öffentlichkeitsfahndung sowie andere Aufgaben und Befugnisse von Strafverfolgungsbehörden zu regeln. Hierzu ist allein der Bundesgesetzgeber berechtigt.[56]

Unabhängig von dieser Zuständigkeitsproblematik ist der vorgelegte Gesetzentwurf auch inhaltlich nicht mit höherrangigem Recht vereinbar, da er jegliche Verhältnismäßigkeit vermissen lässt. Eine konkrete Abwägung von geplanten Überwachungsmaßnahmen mit den Rechten und Interessen betroffener Personen ist nicht vorgesehen. Lediglich in einer rechtlich unverbindlichen Fußnote wird allgemein auf die Beachtung der Verhältnismäßigkeit verwiesen, was jedoch das Fehlen von Abwägungsregeln im Gesetzestext nicht ausgleichen kann.[57] Eine nicht anlassbezogene großflächige Videoüberwachung stellt jedoch u. a. aufgrund ihrer Streubreite einen tiefen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der davon Betroffenen dar. Möglichkeiten, einer solchen Überwachung insbesondere an großen Plätzen und Verkehrsknotenpunkten auszuweichen, bestünden kaum. Gleichzeitig würden unabhängig von deren praktischem Nutzen Bewegungsprofile von einer Vielzahl unbeteiligter Personen entstehen. Der Europäische Gerichtshof hat jüngst dargelegt, dass eine derartige anlass- und unterschiedslose Speicherung von Daten auf Vorrat mit der Europäischen Grundrechte-Charta unvereinbar ist.[58]

Zu bemängeln ist auch, dass Zweck und Anlass der Datenverarbeitung nicht hinreichend bestimmt werden. Zwecke der Gefahrenabwehr und der Strafverfolgung werden miteinander vermischt. Zudem stellt der Entwurf auf Anhaltspunkte für eine abstrakte Bedrohung durch Straftaten, nicht aber auf eine konkrete Gefährdung von Bürgerinnen und Bürgern durch Straftaten ab. Aufgrund der fehlenden Eingrenzung verstößt dies gegen den Bestimmtheitsgrundsatz, weil eine abstrakte Bedrohung faktisch an jedem Ort möglich ist. Darüber hinaus legt der Entwurf bestimmte Objekte als gefährdet fest, ohne eindeutige Kriterien dafür zu benennen. Damit wird die Eingriffsschwelle von pauschalen Wertungen und Mutmaßungen abhängig gemacht.

56 Art. 74 Abs. 1 Nr. 1, 72 Abs. 1 GG i. V. m. StPO

57 Fn. 3 des Gesetzesentwurfs

58 EuGH, Urteil vom 21. Dezember 2016 – C-203/15 u. C-698/15 – Tele2 Sverige

Bemerkenswert ist außerdem, dass die Initiative bereits in ihrem Namen und auch darüber hinaus fortlaufend betont, dass das von ihr vorgeschlagene Gesetz den Datenschutz verbessern würde, obwohl das Gesetz zu einem sehr starken Anstieg der Verarbeitung von Daten einer großen Zahl insbesondere unbeteiligter Personen durch Videoüberwachung führen würde. Dies hätte genau das Gegenteil von Datenschutz zur Folge.

Der von der Initiative vorgelegte Gesetzesentwurf lässt eine dauerhafte Videoüberwachung zum Schutz gefährdeter Objekte zu. Zu diesen Objekten sollen insbesondere Gebäude, Gelände oder Bauwerke von öffentlichem Interesse, Verkehrs- und Versorgungsanlagen oder Versorgungseinrichtungen, öffentliche Verkehrsmittel und Amtsgebäude sowie Religionsstätten, Denkmäler und Friedhöfe zählen.[59]

Eine dauerhafte Videoüberwachung soll auch an sog. gefährlichen Orten möglich sein.[60] Insbesondere soll sie daher an belebten Orten und großen Fahrradabstellplätzen eingerichtet werden.[61]

Daneben soll eine Videoüberwachung an Orten möglich sein, an denen sich gewöhnlich große Menschenansammlungen befinden.[62] Dies kann laut den im Gesetzesentwurf genannten Beispielen zum einen temporär bei musikalischen oder sportlichen Großveranstaltungen, Volksfesten, Straßenfesten und Weihnachtsmärkten erfolgen, jedoch auch dauerhaft bei Orten von herausgehobenem touristischen Interesse oder in deren Umfeld.

Im Einzelnen sind besonders folgende Regelungen im Gesetzesentwurf der Initiative zu kritisieren:

1. Der Entwurf soll eine dauerhafte Erhebung von Daten mittels Anfertigung von Bild- und Tonaufnahmen durch die Polizei an Gebäuden, Geländen oder Bauwerken von öffentlichem Interesse zu Präventionszwecken ermöglichen.[63] Es wird nicht näher definiert, wann das Vorliegen eines öffentlichen Interesses zu

59 § 24a Abs. 1 Satz 1 Nr. 1 ASOG-E
60 § 24a Abs. 1 Satz 1 Nr. 2 ASOG-E
61 § 24a As. 1 Satz 2 ASOG-E
62 § 24a Abs. 1 Satz 1 Nr. 3 ASOG-E
63 § 24a Abs. 1 Satz 1 Nr. 1 ASOG-E

bejahen ist. Neben allen öffentlich zugänglichen Räumen, wie Einkaufszentren, Kaufhäusern, Restaurants, Schwimmbädern und Museen, fallen auch Privatgebäude und -gelände unter diese Norm, sobald diese von Belang für das Gemeinwohl sind, ohne dass nach konkreten Zwecken differenziert wird.

Es ist zu befürchten, dass diese Regelung zu einer dauerhaften Überwachung großflächiger Bereiche insbesondere der Innenstadt Berlins führen würde ohne Vorliegen konkreter einzelfallbezogener Anlässe. Für diese Befürchtung spricht, dass der Wortlaut des Gesetzesentwurfs eine polizeiliche Videoüberwachung bei abstrakter Gefährdungslage in und an vorgenannten Objekten und somit weiträumig in der Stadt zulassen würde.

2. Die zusätzliche Erhebung von Tonaufnahmen stellt eine gänzlich neue Qualität der Überwachung dar. In weiten Bereichen der Berliner Innenstadt können sich Bürgerinnen und Bürger nicht mehr sicher sein, wer ihnen wann zuhört, selbst in Kirchen, auf Friedhöfen oder in Gerichtsgebäuden sind sie vor Überwachungsmaßnahmen nicht sicher.

3. Außerdem soll eine dauerhafte Videoüberwachung bei Verkehrs- und Versorgungsanlagen oder -einrichtungen, öffentlichen Verkehrsmitteln und Amtsgebäuden sowie auch Religionsstätten, Denkmälern und Friedhöfen ermöglicht werden.[64] Insbesondere sollen auch Gebäude der Strafgerichtsbarkeit, der Staatsanwaltschaft und Justizvollzugsanstalten sowohl von innen als auch in deren äußerem Umfeld mit permanenten Bildaufzeichnungen überwacht werden können.[65] Dies dürfte allein schon aufgrund der Regelungen zum Beschäftigtendatenschutz und des Grundsatzes der Öffentlichkeit von Gerichtsverfahren, der keine Beschränkung des Zugangs von Personen durch deren durchgehende Überwachung erlaubt, in diesem Ausmaß unzulässig sein. Sämtliche datenschutzfreundlichen und sehr differenzierten Regelungen des Justizvollzugsdatenschutzgesetzes, die u. a. auch den notwendigen Kernbereichsschutz[66] garantieren, wären dadurch obsolet.

64 § 24a Abs. 1 Satz 1 Nr. 1 ASOG-E

65 Fn. 4 des Gesetzesentwurfs

66 „Nach der Rechtsprechung des Bundesverfassungsgerichts besteht ein letzter unantastbarer Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen und daher vor staatlichen Eingriffen geschützt ist."

4. Weiterhin soll künftig eine dauerhafte Videoüberwachung an gefährlichen Orten möglich sein, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Straftaten verabredet, vorbereitet oder verübt werden.[67] Die Formulierung lässt eine Videoüberwachung faktisch an jedem Ort zu, soweit dort abstrakt Straftaten drohen. Insbesondere soll immer dann eine ständige Videoüberwachung in diesem Zusammenhang erfolgen, wenn es sich um belebte Orte oder um große Fahrradabstellplätze handelt.[68] Betroffen hiervon wären Straßen und Plätze mit besonders hohem Passantenaufkommen sowie Verkehrsknotenpunkte. Derartige Örtlichkeiten sind in einer Großstadt wie Berlin eher die Regel als die Ausnahme. Ein Ausweichen vor einer Videoüberwachung wäre besonders in der Innenstadt Berlins kaum noch möglich. Bürgerinnen und Bürger, die nicht videoüberwacht werden wollen, wären zudem mit einer solchen Vorschrift z. B. von der Nutzung von der Stadt bereitgestellter großer öffentlicher Fahrradstellplätze ausgeschlossen.

5. Auch sollen die vorgenannten Maßnahmen mittels „intelligenter Videoaufklärung“ durchgeführt werden.[69] Soweit solche Videoüberwachungssysteme auf der Verarbeitung biometrischer Daten basieren, ist ihr Einsatz nur zulässig, wenn dies unbedingt erforderlich ist und eine Rechtsnorm dies ausdrücklich erlaubt bzw. die Identifizierung zur Wahrung lebenswichtiger Interessen erforderlich ist.[70] Verfahren, die mit biometrischen Daten arbeiten, sind besonders riskant, da biometrische Daten nicht veränderbar sind und ihr Besitz in falschen Händen für die Betroffenen lebenslange Folgen haben kann (z. B. Identitätsdiebstahl).[71] Eine Nutzung derartiger Systeme zum Zweck der Verhinderung von Vandalismus oder Fahrraddiebstählen ist daher regelmäßig nicht zulässig.

67 § 24a Abs. 1 Satz 1 Nr. 2 ASOG-E

68 § 24a Satz 2 i. V. m. Abs. 1 Satz 1 Nr. 2 ASOG-E

69 § 24a Abs. 1 Satz 4 ASOG-E

70 Richtlinie (EU) 2016/680 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 (JI-Richtlinie)

71 Siehe 1.3

6. Der Polizei soll zudem ermöglicht werden, bei Personen- oder Fahrzeugkontrollen im öffentlichen Verkehrsraum Bildaufzeichnungen durch sog. „Body-Cams“ anzufertigen.[72] Diese vorgeschlagene Gesetzesänderung verstößt gegen den Bestimmtheitsgrundsatz. Denn die Erweiterung der Befugnisse zum Einsatz optisch-elektronischer Mittel ergibt sich erst aus dem Fußnotentext. Der Gesetzeswortlaut selbst lässt weder klar erkennen, dass solche Körperkameras eingesetzt werden können, noch werden die genauen Voraussetzungen für den Einsatz benannt.

7. Schließlich schlägt die Initiative die Gründung eines sog. „Berliner Instituts für Kriminalprävention“ (BIK) vor.[73] Dieses Institut soll z. B. Anfragen in Bezug auf den datenschutzgerechten Einsatz von Videoüberwachung beantworten.[74] Dies verstößt gegen verfassungs- und europarechtliche Vorgaben zur Datenschutzaufsicht, die die Beratung in Datenschutzfragen den unabhängigen Aufsichtsbehörden zuweisen. Diese Aufgabe kann nicht zusätzlich auf eine weitere staatliche Stelle übertragen werden, die zudem nicht unabhängig ist.[75] Für die Bürgerinnen und Bürger wäre es auch schwer nachvollziehbar, wenn etwa das BIK zur Nutzung einer Videoüberwachungsanlage riete, deren Betrieb von der Berliner Beauftragten für Datenschutz und Informationsfreiheit im Nachhinein für rechtswidrig erklärt würde.

Welche polizeilichen Videoüberwachungsmaßnahmen zur Gefahrenabwehr geeignet und erforderlich sind, muss unter sorgfältiger Abwägung mit den Freiheitsrechten davon betroffener Personen sachlich analysiert und diskutiert werden. Ein allein von vermeintlichen Sicherheitsgefühlen geleiteter Gesetzesentwurf konterkariert solche notwendigen Erörterungen. Bürgerinnen und Bürger sollten die Initiative daher nicht unterstützen.

72 Fn. 13 des Gesetzesentwurfs i. V. m. § 19a Abs. 1 Satz 1 ASOG-E

73 Gesetzesentwurf zum Berliner Institut für Kriminalprävention (BIKG-E)

74 § 2 Abs. 2 Nr. 1 BIKG-E

75 Gemäß § 5 Abs. 1 Satz 1 BIKG-E sollen u. a. im Aufsichtsrat des Instituts der Präsident des Bundeskriminalamtes, der Präsident der Bundespolizei und der Generalbundesanwalt sitzen.

## 1.3 Identitätsdiebstahl

Unsere Einkaufswelt verändert sich grundlegend. Waren und Dienstleistungen werden vermehrt – teilweise sogar ausschließlich – online angeboten. Die veränderten Konsumwege bergen neuartige Risiken. Ein besonderes Problem stellt dabei der grassierende Identitätsbetrug dar. Der Onlinehandel ermöglicht dabei das Bestellen mit den Daten einer anderen Person und somit auch auf deren Rechnung.

Allein mit Vorname, Name und Geburtsdatum einer anderen Person ist eine Lieferung an eine beliebige Anschrift in betrügerischer Absicht möglich. Pakete werden mitunter selbst dann durch die Unternehmen ohne sofortige Zahlung des Kaufpreises bei Bestellung nur auf Rechnung versandt, wenn offensichtliche Unklarheiten hinsichtlich der bestellenden Person bestehen. Für Betroffene bedeutet ein solcher Betrugsfall viel Ärger und Aufwand, da bei Nichtzahlung der Rechnung Mahnverfahren gegen die vermeintlichen Bestellerinnen oder Besteller eingeleitet werden und Einträge gegen sie bei den Auskunfteien erfolgen, obwohl sie die Bestellung nicht veranlasst haben. Um diese Folgen zu verhindern, müssen die Betroffenen mit zahlreichen Stellen Kontakt aufnehmen. Dies ist nicht nur mit großem Recherche- und Zeitaufwand, sondern regelmäßig auch mit erheblichen Kosten verbunden.

Der Presse konnte entnommen werden, dass u. a. zahlreiche Landtags- und Bundestagsabgeordnete Opfer von Identitätsdiebstahl im Onlinehandel geworden sind. Aber nicht nur Prominente sind betroffen, bei der Beauftragten für Datenschutz und Informationsfreiheit gehen auch stetig Beschwerden betroffener Bürgerinnen und Bürger zu dieser Problematik ein. Dies führte uns zu der Prüfung, ob die beteiligten Branchen (Onlinehändler, Inkassounternehmen sowie Auskunfteien) adäquate Mittel zur Verhinderung und Abwendung von Identitätsbetrug einsetzen.

Wir haben die uns bekannten Betrugsvorfälle zum Anlass genommen, mit dem Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh) unmittelbar in einen Austausch zu treten. Ziel war es, Möglichkeiten zur Verhinderung von Identitätsdiebstahl und zur Abhilfe für Betroffene zu diskutieren. Da sich das Problem jedoch als branchenübergreifend erwies, haben wir einen Runden Tisch organisiert, an dem neben Vertretern des Versandhandels sowohl Vertreterinnen

und Vertreter der Wirtschaftsauskunfteien und des Bundesverbandes Deutscher Inkasso-Unternehmen als auch des Verbraucherschutzes teilgenommen haben. Außerdem waren das Bundesministerium des Innern, das Bundesministerium der Justiz und für Verbraucherschutz sowie Vertreterinnen und Vertreter weiterer Datenschutzaufsichtsbehörden beteiligt.

Wichtig war uns im Rahmen des Runden Tisches, den Fokus auf die risikobewusste Gestaltung von Bestell- und Mahnverfahren durch den Onlinehandel zu richten. Bei Auffälligkeiten, die auf Betrug hinweisen können, etwa eine abweichende Lieferanschrift, müssen genauere Kontrollen erfolgen (z. B. durch persönliche Rückfragen). Jedenfalls sollte eine Erstbestellung mit einer von der Rechnungsadresse abweichenden Lieferadresse nicht auf Rechnung möglich sein.

Um die Gefahren des Identitätsbetruges einzudämmen, werden wir uns auch für eine stärkere Verbreitung des Einsatzes des elektronischen Identitätsnachweises (sog. eID-Funktion) des neuen Personalausweises einsetzen. Diese für das Internetzeitalter entwickelte Technologie könnte sichere Identifizierungen unterstützen und Identitätsdiebstahl damit erheblich erschweren.

Uns sind zudem Fälle aus der Praxis bekannt, in denen Mahnungen für nicht bezahlte Rechnungen ausschließlich per E-Mail versandt wurden. Eine Mahnung per E-Mail gewährleistet allerdings nicht, dass diese bei der tatsächlich betroffenen Person ankommt und diese eine Chance erhält, den Sachverhalt aufzuklären. Oft gehen diese Mahn-E-Mails wieder an die betrügerischen Bestellerinnen oder Besteller, während die vom Betrug Betroffenen, die für die Bestellung haftbar gemacht werden, häufig nicht oder erst sehr spät von diesen „offenen Rechnungen" Kenntnis erhalten. Der Bundesverband Deutscher Inkassounternehmen hat uns gegenüber zugesagt, seine Mitgliedsunternehmen nochmals auf die Anforderungen hinzuweisen.

Gibt ein Unternehmen einen Vorgang ins Mahnverfahren ab, handeln die beauftragten Inkassounternehmen regelmäßig ohne Informationen darüber, ob Anhaltspunkte für einen Identitätsdiebstahl bestehen. Wenn bei einer Bestellung Unstimmigkeiten hinsichtlich der Identität der bestellenden Person aufgekommen sind, muss dieser Umstand auch einem später eingeschalteten Inkassounternehmen als Anhaltspunkt für einen möglichen Identitätsbetrug mitgeteilt werden.

Hinzu kommt, dass die Mahnverfahren zum Teil zu Negativeinträgen bei Wirtschaftsauskunfteien geführt haben. Fehlerhafte Datenbestände bei Auskunfteien können für die Betroffenen jedoch massive wirtschaftliche Folgen haben. Verschlechtert sich die Bonitätsbewertung einer Person, können beispielsweise Probleme beim Abschluss von Kredit- und Mietverträgen auftreten. Ein Negativeintrag bei einer Auskunftei sowie ein gerichtliches Vorgehen wegen Nichtzahlung einer Rechnung dürfen daher nur erfolgen, wenn ein Identitätsbetrug ausgeschlossen werden kann. Wer dies nicht sicherstellt, muss mit aufsichtsrechtlichen Maßnahmen wie der Einleitung eines Bußgeldverfahrens wegen unbefugter Verarbeitung personenbezogener Daten[76] rechnen.

Zudem haben wir effektive und einfache Beschwerdemöglichkeiten und Transparenzmaßnahmen für betroffene Personen gefordert. Sie benötigen Unterstützung, etwa in Form von gezielten Beschwerdeformularen, um ihren Sachverhalt in geeigneter Form vortragen zu können und Gehör zu finden. In jedem Fall muss der Kundenservice von Onlinehändlern, Auskunfteien und Inkassounternehmen für diese Thematik sensibilisiert werden.

Im Anschluss an unseren Runden Tisch hat im Juni im Berliner Abgeordnetenhaus eine Anhörung zu „Auswirkungen des Forderungsmanagements im Internetzeitalter auf Verbraucher und gesetzgeberischer Handlungsbedarf unter besonderer Berücksichtigung datenschutzrechtlicher Aspekte“ stattgefunden.[77] Im Rahmen dieser Anhörung haben sich strukturelle Mängel bei den am Identitätsdiebstahl beteiligten Akteuren gezeigt. Es werden nicht genügend Maßnahmen ergriffen, um Identitätsdiebstähle zu verhindern. Wir werden daher alle beteiligen Akteure weiter in die Verantwortung nehmen.

Unternehmen dürfen den Schutz von Betroffenen nicht hintanstellen, um Lieferungen möglichst rasch versenden und Umsatz erzeugen zu können. Onlinehändler müssen vor Auslieferung auf Rechnung geeignete Maßnahmen treffen, um einen Identitätsbetrug auszuschließen. Bei betrugsrelevanten Auffälligkeiten sind angemessene Kontrollen durchzuführen.

76 Siehe § 43 Abs. 2 Nr. 1 BDSG

77 Siehe Ausschussprotokoll 18/10 des Hauptausschusses des Abgeordnetenhauses Berlin

## 1.4 Entwurf einer ePrivacy-Verordnung – Noch mehr Datenschutz made in Europe!

Der neue EU-Datenschutzrahmen wird weiter ergänzt: Als Teil der europäischen „Strategie für einen digitalen Binnenmarkt" veröffentlichte die EU-Kommission am 10. Januar 2017 den Entwurf einer Verordnung über Privatsphäre und elektronische Kommunikation[78] (kurz: ePrivacy-Verordnung). Die Verordnung soll Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher und juristischer Personen bei der Bereitstellung und Nutzung elektronischer Kommunikationsdienste festlegen und dabei insbesondere die Rechte auf Achtung des Privatlebens und der Kommunikation sowie den Datenschutz in Europa neu regeln und weiter harmonisieren. Wie bereits bei der Datenschutz-Grundverordnung (DS-GVO) greift die Kommission für ihren Entwurf zur Form der europäischen Verordnung, die – anders als eine europäische Richtlinie – keiner Umsetzung in nationales Recht bedarf, sondern nach Annahme durch den Rat direkt in sämtlichen Mitgliedstaaten gilt.

Die geplante ePrivacy-Verordnung soll die bisherige Datenschutzrichtlinie für elektronische Kommunikation[79] aufheben, mit der Folge, dass auch darauf basierende nationale Gesetze, wie etwa die Datenschutzvorschriften im deutschen Telekommunikationsgesetz, abgelöst werden. Zudem erweitert der Entwurf den Anwendungsbereich im Vergleich zur Vorgängerrichtlinie: Auch sog. „Over-the-Top"-Kommunikationsdienste, d. h. internetgestützte Telefonie, Sofortnachrichtenübermittlung („Instant-Messaging") sowie webgestützte E-Mail-Dienste, sind erfasst. Das erklärte Ziel ist es, dass ein gleicher Standard der Vertraulichkeit gelten soll, unabhängig davon, ob Personen via SMS oder durch andere internetgestützte Dienste kommunizieren. Damit sollen für alle Telekommunikationsanbieter die gleichen Regelungen gelten und gleiche Wettbewerbs-

78 Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, COM(2017) 10 final, 2017/0003 (COD)

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

voraussetzungen geschaffen werden. Hinzu kommt, dass der Entwurf ebenso wie bei der DS-GVO das sog. Marktortprinzip einführt und festlegt, dass sich auch außerhalb der Europäischen Union ansässige Unternehmen, die elektronische Kommunikationsdienste für Endnutzerinnen und -nutzer innerhalb der Europäischen Union anbieten, an die Verordnung halten müssen.

Der Kommissionsentwurf enthält Bestimmungen für die Verarbeitung von Kommunikationsdaten, d. h. Kommunikationsinhalten und sog. Metadaten, die die Umstände einer Kommunikation betreffen (Uhrzeit, beteiligte Kommunikationspartner etc.), und macht auch Vorgaben zur vorrangigen Verarbeitung anonymisierter Daten. Darüber hinaus wird die Endeinrichtung der Nutzerinnen und Nutzer unter Schutz gestellt: Sämtliche Informationen in Bezug auf diese Endeinrichtungen fallen in den Anwendungsbereich des Verordnungsentwurfs. Damit ist z. B. das Speichern von Cookies auf den Endeinrichtungen genauso erfasst wie die Erhebung von Informationen aus den Endeinrichtungen, z. B. in Form des sog. „device- oder browser-fingerprinting". Letzteres betrifft das Sammeln und Zusammenführen von Informationen über eine Vielzahl von Geräte- und Browsereigenschaften eines Endgeräts, sodass sich aus der Kombination der verschiedenen Einstellungen ein einzigartiges Bild, d. h. ein digitaler Fingerabdruck eines Endgeräts, ergibt. All diese Aktivitäten dienen dazu, Nutzerinnen und Nutzer identifizierbar zu machen, um durch eine Verfolgung ihrer Bewegungen im Internet möglichst viele Informationen zu sammeln, diese eindeutig zuzuordnen und dadurch z. B. Angebote individuell für konkrete Personen zusammenstellen zu können. Der Verordnungsentwurf stellt dies nun grundsätzlich unter den Vorbehalt der Zustimmung durch die Endnutzerinnen und -nutzer.

Darüber hinaus enthält der Verordnungsentwurf auch erstmalig konkrete Regelungen, die sich auf das sog. WiFi-Tracking beziehen, d. h. auf eine Technik, mit der Bewegungsverläufe von Personen anhand von Standortdaten verfolgt werden können, die unter Rückgriff auf das Smartphone der Personen erfasst werden. Als weitere Neuheit umfasst der Verordnungsentwurf Vorgaben für die Hersteller von Software, die eine elektronische Kommunikation erlauben, d. h. etwa für Hersteller von Betriebssystemen, Browsern, Apps etc. Derartige Software muss zukünftig nach dem Willen der Kommission Einstellungsmöglichkeiten zur Privatsphäre bieten, die verhindern können, dass z. B. Cookies gesetzt werden.

Im April hat die Art. 29-Gruppe[80] zu dem Entwurf der Kommission Stellung genommen. Darin kritisieren die europäischen Datenschützer vor allen Dingen die niedrigen Hürden für das WiFi-Tracking. Nach dem Entwurf der Kommission wird für derartige Datenverarbeitungen vorrangig Transparenz gefordert. Weitergehende Anforderungen, wie etwa die Zustimmung der betroffenen Personen zur Standorterfassung, sind hingegen nicht vorgesehen. Ebenfalls problematisch ist die Unterscheidung zwischen Kommunikationsinhalt und Metadaten, die im Kommissionsentwurf vorgesehen ist. Aus Sicht der Datenschützer sind Metadaten nicht weniger schützenswert, da auch die Umstände einer Kommunikation viel über die jeweils betroffenen Kommunikationspartner aussagen können und insbesondere Rückschlüsse zulassen, wer wen kennt bzw. wer mit wem zu tun hat. Begrüßenswert ist hingegen, dass der Kommissionsentwurf das Nutzertracking, also das Verfolgen der Aktivitäten von Nutzerinnen und Nutzern im Internet, grundsätzlich von der Einwilligung der betroffenen Personen abhängig macht. Die Datenschützer befürworten allerdings eine Klarstellung dahingehend, dass die betroffenen Personen nicht de facto gezwungen werden können, die Zustimmung zur Nutzerverfolgung zu erteilen, weil sie ansonsten eine Sperrung ihres Zugangs zu Webseiten befürchten müssten. Durch diese Klarstellung soll sichergestellt werden, dass die Nutzerinnen und Nutzer von einem Webanbieter nicht deshalb ausgeschlossen werden können, weil sie ihr Internet-Nutzungsverhalten nicht über verschiedene Dienste hinweg verfolgen lassen wollen (Problem der sog. „Tracking / Cookie Walls“[81]).

Nicht zufriedenstellend ist zudem die Regelung für die Kommunikationssoftware. Ein verbesserter Schutz – gerade für weniger technikaffine Nutzerinnen und Nutzer – wäre zu erreichen, wenn nicht nur Möglichkeiten für Privatsphäre-Einstellungen vom Softwarehersteller angeboten, sondern zwingend die datenschutzfreundlichste Einstellung voreingestellt sein müsste (sog. „privacy-by-default“). Dann könnten die Nutzerinnen und Nutzer jederzeit selbst Änderungen vornehmen, wenn sie sich mit den Einstellungsmöglichkeiten vertraut gemacht haben. Sie wären aber beim ersten Einsatz erst einmal geschützt. Darüber hinaus sieht die Regelung lediglich vor, dass die Software verhindern soll, dass z. B. Cookies

80 Die Art. 29-Datenschutzgruppe ist benannt nach Art. 29 der Datenschutz-Richtlinie 95/46/EG und besteht aus Vertreterinnen und Vertretern sämtlicher europäischer Datenschutzbehörden. Sie hat beratende Funktion.

81 Verhinderung der Nutzung einer Webseite bei Nichtakzeptieren von Cookies

von „Dritten“ gesetzt werden. Übersehen wurde dabei, dass auch die Hersteller der Software daran gehindert sein müssen, die Aktivitäten der Nutzerinnen und Nutzer zu verfolgen.

Die Kommission hatte geplant, dass die ePrivacy-Verordnung gleichzeitig mit der DS-GVO im Mai 2018 Geltung erlangt, weil die DS-GVO und die ePrivacy-Verordnung nicht unabhängig voneinander existieren, sondern nach dem jetzigen Entwurf in einem lex specialis-Verhältnis zueinander stehen. Das bedeutet, dass die ePrivacy-Verordnung die DS-GVO ergänzen, präzisieren und überall dort vorrangig vor der DS-GVO gelten soll, wo sie eine Spezialregelung trifft. Gleichzeitig soll das Schutzniveau der DS-GVO bei den Spezialregelungen der ePrivacy-Verordnung nicht abgesenkt werden. Vor diesem Hintergrund könnten die Regelungen einer ePrivacy-Verordnung auch bei der Implementierung der DS-GVO für viele Unternehmen eine erhebliche Rolle spielen.

Angesichts des Verhandlungsstands im europäischen Gesetzgebungsprozess scheint die Zeitvorgabe der Kommission allerdings unerreichbar. Zwar hat das Europäische Parlament bereits Ende Oktober 2017 eine Verhandlungsposition festgelegt. Die darin vorgesehenen Änderungsanträge tragen dabei vielen Kritikpunkten der Art. 29-Gruppe Rechnung. Allerdings lässt der Europäische Rat auf sich warten. Ein Beschluss über die „allgemeine Ausrichtung“, d. h. die Verhandlungsposition des Rates, scheint noch in weiter Ferne. Dieser ist aber Voraussetzung, um in den sog. Trilog einzutreten, d. h. in das Vermittlungsverfahren zwischen Europäischer Kommission, Europäischem Parlament und Europäischem Rat, das das Gesetzgebungsverfahren der Verordnung zum Abschluss bringen kann. Darüber hinaus ist bereits absehbar, dass auch die ePrivacy-Verordnung einer Umsetzungsfrist bedarf.

Solange die ePrivacy-Verordnung die Datenschutzrichtlinie für elektronische Kommunikation nicht ersetzt, gilt diese auch nach dem Geltungsbeginn der DS-GVO im Mai 2018 fort.[82] Damit bleibt es zunächst auch bei den bestehenden Datenschutzregeln im Telekommunikationsgesetz, da diese die vorgenannte Richtlinie in Deutschland umsetzen. Etwas anderes gilt hingegen im Telemedienbereich. Wenn die ePrivacy-Verordnung nicht bis zum Geltungsbeginn der DS-GVO be-

82 Siehe Art. 95 der DS-GVO

schlossen ist, müssen sich die Telemedienanbieter bis auf Weiteres nach der DS-GVO richten, wohl wissend, dass sich mit einer zukünftigen ePrivacy-Verordnung für sie noch einiges ändern kann.

Darüber hinaus entsteht die Frage, wie die bisherige Regelung zu den Cookies in der Datenschutzrichtlinie für elektronische Kommunikation Eingang in das deutsche Recht finden wird. Nach europäischem Recht ist das Setzen von Cookies auch bisher schon grundsätzlich von der Einwilligung der Betroffenen abhängig.[83] Das Bundeswirtschaftsministerium hatte dazu immer die Auffassung vertreten, dass die Richtlinie im deutschen Recht bereits umgesetzt sei.[84] Eine konkrete Vorschrift ist dem deutschen Recht jedoch nicht zu entnehmen. Auch hier bleibt es abzuwarten, wie der deutsche Gesetzgeber sich positionieren wird.

Der Verordnungsentwurf der Kommission und die Verhandlungsposition des Europäischen Parlaments sind zum Teil massiver Kritik aus der Wirtschaft ausgesetzt, insbesondere der Verlags- und Werbewirtschaft. Es wird behauptet, dass bestehende Geschäftsmodelle verhindert würden. Dabei bleibt unberücksichtigt, dass die Rechtmäßigkeit vieler dieser zitierten Geschäftsmodelle bereits nach geltendem Recht in Frage steht. Rechtsunsicherheiten sind gerade in Deutschland insbesondere auch auf die unvollständige Umsetzung der europäischen Cookie-Regelungen zurückzuführen. Gleichwohl sind die Ideen für einen verbesserten Schutz der Nutzerinnen und Nutzer im Internet keinesfalls neu. Sie stellen vielmehr eine Fortführung dessen dar, was mit der Datenschutzrichtlinie für elektronische Kommunikation begonnen wurde und nun mit den rasanten Entwicklungen in diesem Bereich Schritt halten soll. Ob dies gelingt, wird sich in den nächsten zwei Jahren zeigen.

83 Art. 5 Abs. 3 der Richtlinie 2002/58/EG

84 Siehe ausführlich dazu: JB 2014, 13.2

# 2 Digitale Verwaltung

## 2.1 Service-Konto Berlin

Aus der Praxis

Bereits seit 2013 befasst sich die Senatsverwaltung für Inneres und Sport mit der Einführung des Service-Kontos Berlin. Als zentrale Identifizierungskomponente des Landes Berlin wird das Service-Konto künftig nicht nur Bürgerinnen und Bürgern, sondern auch Unternehmen die einmalige oder dauerhafte Identifizierung zur Inanspruchnahme von Verwaltungsleistungen ermöglichen.

Neben der Anmeldung mit Benutzungsname und Kennwort wird das Service-Konto auch die Nutzung des sicheren elektronischen Identitätsnachweises (eID) des neuen Personalausweises[85] sowie des elektronischen Aufenthaltstitels[86] ermöglichen. So werden in Zukunft selbst solche Verwaltungsleistungen vom heimischen Wohnzimmer aus erledigt werden können, bei denen bislang noch eine persönliche Vorsprache mit Identitätsprüfung erforderlich war.

Darüber hinaus ist vorgesehen, elektronische Verwaltungsakte zum Abruf über das Service-Konto bereitzustellen,[87] soweit die jeweilige Bürgerin bzw. der jeweilige Bürger diesem zugestimmt hat. In einer Vielzahl von Fällen wird daher eine komplett medienbruchfreie[88] elektronische Kommunikation mit der Verwaltung ermöglicht, ohne dass auf den Postweg zurückgegriffen werden muss.

Die Vorteile liegen auf der Hand: Bürgerinnen und Bürger sowie Unternehmen müssen in vielen Fällen keine wertvolle Zeit mehr für Behördengänge aufwenden, profitieren von kürzeren Bearbeitungszeiten und sparen Portokosten. Spiegelbildlich profitiert aber auch die Verwaltung, da die Vorgangsbearbeitung in der Regel

85 § 18 PAuswG

86 § 78 Abs. 5 AufenthG

87 § 3a Abs. 2 VwVfG i. V. m. § 1 Abs. 1 VwVfGBln

88 Als Medienbruch wird ein Wechsel des Mediums innerhalb eines Verfahrens bezeichnet, also z. B. wenn ein Antrag per Service-Konto gestellt wird, der Bescheid aber auf dem Postweg versandt wird.

vollständig elektronisch abgebildet werden kann, weniger Zeitaufwand für Publikumsverkehr entsteht und zudem auch Portokosten eingespart werden können. Insgesamt wird das Service-Konto perspektivisch dazu beitragen können, insbesondere die äußerst angespannte Terminsituation in den Berliner Bürgerämtern zu entschärfen.

Damit das Service-Konto Berlin zum Erfolgsmodell werden kann, ist jedoch die Berücksichtigung einer Vielzahl datenschutzrechtlicher Aspekte bereits bei der Konzeptionierung zwingend erforderlich.

So muss sichergestellt sein, dass Verwaltungsleistungen auch künftig ohne die Nutzung des Service-Kontos Berlin in Anspruch genommen werden können und dass deren einmalige Inanspruchnahme auch ohne dauerhafte Speicherung personenbezogener Daten möglich ist.[89] Keinesfalls dürfen Bürgerinnen und Bürger dazu verpflichtet werden, das Service-Konto zu nutzen, oder gar ein solches permanentes Nutzungskonto einzurichten.

Auch darf der Staat personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben nur aufgrund einer klaren Rechtsgrundlage verarbeiten. Daher ist für den Betrieb des Service-Kontos Berlin eine eigene Rechtsgrundlage zur Datenverarbeitung erforderlich. In dieser Rechtsgrundlage müssen der für das Service-Konto Berlin zuständigen Senatsverwaltung für Inneres und Sport entsprechende Aufgaben zugewiesen werden. Den Betrieb des Service-Kontos allein auf die Einwilligung der jeweiligen Bürgerinnen und Bürger zu stützen, wäre datenschutzrechtlich äußerst problematisch, da Betroffene zum Zeitpunkt der Einrichtung des Kontos in eine nicht überschaubare Anzahl potenzieller Datenübermittlungen einwilligen müssten, was faktisch nicht möglich ist. Darauf haben wir die Senatsverwaltung bereits frühzeitig hingewiesen.

Auf Bundesebene ist im August das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz des Bundes) in Kraft getreten. Dieses Gesetz verpflichtet zwar Bund und Länder, ihre Verwaltungsleistungen künftig auch elektronisch über Verwaltungsportale anzubieten, trifft jedoch im Übrigen nur Regelungen für die Einrichtung und den Betrieb von Service-Konten

89 Sog. temporäres Nutzungskonto

auf Bundesebene sowie für den übergreifenden informationstechnischen Zugang zu den Verwaltungsleistungen von Bund und Ländern. Entsprechende Regelungen für die Landesebene könnte der Bundesgesetzgeber ohnehin nicht treffen, da er nicht über die Gesetzgebungskompetenz verfügt, die Datenverarbeitung in Service-Konten auf Länderebene zu regeln.[90]

Vor diesem Hintergrund hatten wir der Senatsverwaltung noch im August einen Vorschlag für ein Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen der Berliner Verwaltung (Onlinezugangsgesetz Berlin) unterbreitet, der an das Onlinezugangsgesetz des Bundes anknüpft und dieses um notwendige Regelungen für den Einsatz und Betrieb von Service-Konten auf Landesebene ergänzt. Der von der Senatsverwaltung auf Grundlage unseres Entwurfes weiterentwickelte Referentenentwurf soll nunmehr zeitnah endgültig mit uns abgestimmt und sodann auf den Weg ins Gesetzgebungsverfahren gebracht werden.

Weiterhin hatten wir die Senatsverwaltung darauf hingewiesen, dass bei der notwendigen Übermittlung personenbezogener Daten für Fachverfahren nur die für die Erbringung der Verwaltungsleistung unbedingt erforderlichen personenbezogenen Daten der Bürgerinnen und Bürger übermittelt werden dürfen.[91] Die Übermittlung aller im Service-Konto vorhandenen Stammdaten wäre unzulässig.

Darüber hinaus ist bei der Anbindung von Fachverfahren und der damit verbundenen Nutzung des Service-Kontos der jeweilige Schutzbedarf der personenbezogenen Daten im Fachverfahren zu beachten. Das derzeitige Sicherheitskonzept des Service-Kontos geht nur von einem normalen Schutzbedarf der Daten aus. Sollen Fachverfahren an das Service-Konto angebunden werden, die einen hohen Schutzbedarf erfordern,[92] wären entsprechende technisch-organisatorische Maßnahmen zu ergreifen und das Sicherheitskonzept entsprechend anzupassen.

90 Umkehrschluss aus Art. 91c Abs. 5 GG

91 Grundsatz der Erforderlichkeit nach § 9 Abs. 1 BlnDSG

92 Etwa bei der Verarbeitung von Sozialdaten, die dem Sozialgeheimnis nach § 35 Abs. 1 SGB I unterliegen.

Das Service-Konto Berlin ist ein zentraler Meilenstein auf dem Weg zu einer modernen, digitalen und bürgernahen Verwaltung. Das Land Berlin kann mit dem Onlinezugangsgesetz Berlin, dem ersten seiner Art auf Länderebene, eine Vorreiterrolle für den Datenschutz beim Einsatz und Betrieb von Service-Konten einnehmen.

## 2.2 Entwurf der Verordnung zur Übermittlung von Meldedaten in Berlin



Durch das am 1. November 2015 in Kraft getretene Bundesmeldegesetz (BMG) wurden die Meldegesetze der Bundesländer abgelöst.[93] Die Länder dürfen seitdem eigene melderechtliche Vorschriften nur in den Fällen erlassen, in denen das BMG sie hierzu ermächtigt. Infolgedessen musste auch das Berliner Melderecht neu gefasst werden.

Als ersten Schritt hat das Abgeordnetenhaus im vergangenen Jahr bereits das Berliner Ausführungsgesetz zum Bundesmeldegesetz (BlnAGBMG) beschlossen.[94] In diesem Jahr hat nun die Senatsverwaltung für Inneres und Sport die Verordnung zur Übermittlung von Meldedaten in Berlin (BlnMDÜV) erlassen.[95] Wir hatten vorab Gelegenheit, zu dem Entwurf dieser Verordnung (BlnMDÜV-E) Stellung zu nehmen.

Eine von uns kritisierte Regelung des Verordnungsentwurfs hat die regelmäßigen Datenübermittlungen zur Durchführung polizeilicher Aufgaben zum Gegenstand, da insoweit keine Ermächtigung durch das Bundesmeldegesetz gegeben ist. Nach dieser Vorschrift sollten bestimmte Datensätze zur Durchführung allgemeiner polizeilicher Aufgaben regelmäßig an den Polizeipräsidenten von Berlin übermittelt werden, wenn bei Einwohnerdaten eine bestimmte Änderung eingetreten ist und eine regelmäßige Übermittlung der Daten der betroffenen Einwohnerinnen und Einwohner beantragt wurde. Der Verordnungsgeber ist aber nach dem Bun-

93 JB 2016, 3.1
94 GVBl. 2016, S. 430
95 Verordnungs-Nr. 18/073

desmeldegesetz[96] nur dann zu einer Regelung befugt, wenn formal eine regelmäßige Datenübermittlung vorliegt.

Bereits nach dem Wortlaut der Regelung handelte es sich hier jedoch nicht um eine regelmäßige Datenübermittlung im Sinne des Bundesmeldegesetzes, sondern vielmehr um ein Ersuchen in Bezug auf die Daten der betroffenen Einwohnerinnen und Einwohner. Dies kam vor allem durch das zunächst formulierte Antragserfordernis zum Ausdruck. Regelmäßige Datenübermittlungen im Sinne des Bundesmeldegesetzes erfolgen aber gerade ohne Ersuchen des Datenempfängers.[97]

Darüber hinaus war die Regelung zu unbestimmt, da sie offen ließ, unter welchen Voraussetzungen die regelmäßige Datenübermittlung beantragt werden kann. Es wäre dem Datenempfänger überlassen geblieben, zu entscheiden, wann er eine regelmäßige Datenübermittlung für erforderlich hält. Dies ist mit den Regelungen des Bundesmeldegesetzes und des Berliner Ausführungsgesetzes zum Bundesmeldegesetz zu den regelmäßigen Datenübermittlungen nicht vereinbar. Danach sind u. a. der Anlass und Zweck der regelmäßigen Datenübermittlungen festzulegen.[98] Allein die Änderung der Daten kann nicht der Anlass einer regelmäßigen Datenübermittlung sein, denn die geänderten Daten bilden nach der Systematik der vorgenannten gesetzlichen Regelungen üblicherweise den Inhalt der Übermittlung. Zudem ist die Durchführung allgemeiner polizeilicher Aufgaben[99] als Zweck nicht bestimmt genug.

Die Senatsverwaltung für Inneres und Sport konkretisierte den Zweck der Datenübermittlung an die Polizei, indem in der Vorschrift nunmehr konkret benannt wird, in welchen Fällen bzw. in Bezug auf welche Personen die regelmäßige Datenübermittlung erfolgen soll.[100] Zudem wurde das zu unbestimmt formulierte Antragserfordernis gestrichen und stattdessen ein neuer Absatz eingefügt, der ein entsprechendes Ersuchen des Polizeipräsidenten gegenüber der Meldebehörde

96 § 36 BMG

97 § 36 Abs. 1 BMG

98 § 36 Abs. 1 BMG sowie § 6 Abs. 1 BlnAGBMG

99 „Zur Verfolgung von Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung […]"

100 Siehe § 13 Abs. 1 BlnMDÜV

regelt.[101] Der neue Absatz der Vorschrift verdeutlicht dabei, dass die Übermittlung weiterhin auf Ersuchen der Polizei erfolgt, da diese die betroffenen Einwohnerinnen und Einwohner auswählt und ihre Namen an die übermittelnde Stelle weitergibt. Damit liegt gerade keine regelmäßige Datenübermittlung vor.[102] Der Polizeipräsident müsste die Daten im Rahmen einer regulären Anfrage auf Grundlage einer spezifischen gesetzlichen Rechtsvorschrift abfragen.[103] Die Antragsbefugnis der Verordnung zur Übermittlung von Meldedaten in Berlin ersetzt selbstverständlich keine spezifische Rechtsgrundlage für die Übermittlung der Meldedaten an den Polizeipräsidenten.

Neben dem dargestellten Beispiel haben wir weitere Regelungen der Verordnung zur Übermittlung von Meldedaten in Berlin kritisiert, da durch diese die regelmäßigen Datenübermittlungen sowie automatisierten Datenabrufe in verschiedenen Bereichen stark ausgeweitet wurden. Unsere Empfehlungen hat die Senatsverwaltung jedoch nur zum Teil berücksichtigt und umgesetzt.

Regelungen zur Übermittlung von Meldedaten dürfen nur unter strenger Beachtung der vom Bundesverfassungsgericht für das Recht auf informationelle Selbstbestimmung aufgestellten Eingriffsvoraussetzungen erlassen werden. Eingriffe dürfen nur auf Grundlage einer hinreichend bestimmten gesetzlichen Norm, die den Zweck der Verwendung der Meldedaten konkret benennt, erfolgen.

101 § 13 Abs. 2 BlnMDÜV

102 Im Sinne von § 36 BMG

103 Diese wäre auch für eine Vielzahl von Personen möglich, siehe § 24 Abs. 4 BlnMDÜV.

## 2.3 Einheitliches Fachverfahren für die Berliner Jugendämter – Fortsetzung



Wie in den vergangenen Jahren[104] haben wir auch in diesem Jahr die Einführung weiterer Module des verwaltungsübergreifenden Fachverfahrens ISBJ-Jugendhilfe (SoPart)[105] durch die Senatsverwaltung für Bildung, Jugend und Familie eng begleitet.

Sämtliche IT-Fachverfahren für die Jugendverwaltung und zum Teil auch für die Schulverwaltung laufen unter dem Dach der Verfahrenslandschaft des ISBJ-Verfahrens. Mit dem neuen Fachverfahren ISBJ-Jugendhilfe (SoPart) wird für die 2.200 Mitarbeiterinnen und Mitarbeiter der Berliner Jugendämter eine zentrale IT-Lösung geschaffen. Die Verantwortung für das Verfahren liegt zentral bei der Senatsverwaltung für Jugend, die auch die Administration zentral und einheitlich ausübt. In sämtlichen Bezirken werden Geschäftsprozesse in der Jugendhilfe standardisiert und vereinheitlicht.

Bei der Umsetzung des verwaltungsübergreifenden Großprojektes in einem so sensiblen Bereich wie der Jugendhilfe ist eine intensive und damit auch zeitaufwendige datenschutzrechtliche Begleitung notwendig. Die langjährigen und sehr konstruktiven Abstimmungsprozesse mit der Senatsverwaltung haben dazu geführt, dass datenschutzrechtlich notwendige Anpassungen immer sehr zeitnah definiert und umgesetzt werden konnten.

Seit Anfang 2017 wird die Abrechnung sämtlicher Jugendhilfeleistungen mit dem Modul Wirtschaftliche Jugendhilfe (WJH) in allen zwölf bezirklichen Jugendämtern über das neue Fachverfahren ISBJ-Jugendhilfe realisiert. Derzeit befindet sich das Modul für den Regionalen Sozialen Dienst der Jugendämter in der Pilotierungsphase. Die Jugendämter können ihr Fallmanagement mit Hilfe der modernen Software standardisiert und IT-gestützt steuern und so ihre Effizienz steigern. Zudem können Kinderschutzmeldungen mithilfe der Software vereinheitlicht werden. Sukzessive werden weitere Module für z. B. die Amtsvormundschaft/Un-

104 JB 2016, 5.4
105 Integrierte Software Berliner Jugendhilfe

terhaltsbeistandschaft sowie die Jugendberufshilfe und Jugendgerichtshilfe hinzukommen. Wie bei den übrigen Modulen wird sich unser Augenmerk auch hier wieder darauf richten, dass von vornherein möglichst datenschutzfreundliche Einstellungen gewählt werden. Wir werden darauf achten, dass die Software z. B. nur diejenigen Datenfelder vorsieht, die für die Aufgabenerfüllung tatsächlich erforderlich sind, Zugriffsmöglichkeiten nur für diejenigen eingerichtet werden, die diese wirklich benötigen, und Daten so früh wie möglich pseudonymisiert bzw. anonymisiert werden.

ISBJ-Jugendhilfe (SoPart) ist ein positives Beispiel für ein Fachverfahren, mit dem die nach der Datenschutz-Grundverordnung ab Mai 2018 verpflichtend einzuhaltenden Vorgaben für Datenschutz durch Technikgestaltung („Data protection by design“) und durch datenschutzrechtliche Voreinstellungen („Data protection by default“) bereits seit Beginn der Implementierung berücksichtigt werden. Wir gehen davon aus, dass sich der konstruktive Abstimmungsprozess mit der Senatsverwaltung auch bei der Einführung der weiteren Module fortsetzen wird.

## 2.4 Aktueller Stand der behördlichen IT-Sicherheitskonzepte in den Bezirken

Bereits 2013 baten wir die Bezirksämter um die Zusendung der behördlichen IT-Sicherheitskonzepte. In den Jahresberichten für 2013 und 2014 berichteten wir über die Ergebnisse.



Aufgrund des steten Wandels der Informationstechnologie müssen IT-Sicherheitskonzepte permanent angepasst werden, wie dies von den einschlägigen Normen gefordert wird. Da die behördlichen IT-Sicherheitskonzepte die Grundlage für alle weiterführenden IT-Sicherheitskonzepte bilden, baten wir vier Jahre später, im August 2017, um die Zusendung der aktuellen Versionen.

Wie beim letzten Mal war der Zulauf sehr unterschiedlich, was sowohl die Reaktion auf die Anfrage als auch die Qualität der Dokumente betrifft. Drei von 12 Bezirksämtern haben behördliche IT-Sicherheitskonzepte mit aktuellem Stand von

2016 bzw. 2017 zugeschickt. Mehrere Bezirksämter verwiesen auf ihre vorherigen Zusendungen bzw. sandten diese ein zweites Mal zu. Zwei Bezirksämter gaben an, dass Ende 2017 ein neues IT-Sicherheitskonzept vorliegen werde. Zwei weitere gaben keinen Fertigstellungstermin an.

Besonders herauszustellen sind die Bezirksämter Tempelhof-Schöneberg und Steglitz-Zehlendorf, welche auf die vorherigen Abfragen hin keine IT-Sicherheitskonzepte übermittelten. Tempelhof-Schöneberg hatte zwar die Zusendung eines aktuellen IT-Sicherheitskonzepts für Ende 2017 zugesagt, was grundsätzlich positiv zu bewerten war, leider jedoch nicht zu einer fristgerechten Vorlage geführt hat. Das Bezirksamt Steglitz-Zehlendorf hat demgegenüber von vornherein keinen Fertigstellungstermin angegeben. Die IT-Sicherheit ist somit für diese beiden Bezirksämter sowohl auf infrastruktur- als auch auf verfahrensspezifischer Ebene nicht nachweisbar.

Ein behördliches IT-Sicherheitskonzept ist die Sicherheitsbasis sämtlicher Verfahrensanwendungen innerhalb einer Behörde. Die Erstellung eines IT-Sicherheitskonzepts ist verbindlich vorgeschrieben. Dennoch haben nach wie vor nicht alle Berliner Bezirke ein entsprechendes Konzept erstellt.

# 3 Inneres

## 3.1 Umsetzung der JI-Richtlinie in den Bereichen Polizei und Strafvollstreckung



Zeitgleich mit der Datenschutz-Grundverordnung haben das Europäische Parlament und der Rat der Europäischen Union im April 2016 eine Datenschutz-Richtlinie für die Bereiche Justiz und Inneres erlassen.[106] Die sog. JI-Richtlinie soll zu einer Vereinheitlichung der Vorgaben für die Verarbeitung personenbezogener Daten durch Polizei und Justiz innerhalb der Europäischen Union führen.

Im Gegensatz zur Datenschutz-Grundverordnung, die in den Mitgliedstaaten der Europäischen Union unmittelbar gilt, sind die Bestimmungen der JI-Richtlinie nicht direkt wirksam, sondern müssen in nationales Recht umgesetzt werden. Dies erfordert u. a. eine Überarbeitung der Datenschutzvorschriften für die Polizei und den Justizvollzug des Landes Berlin.

Entsprechende Gesetzesänderungen werden gerade durch die Senatsverwaltung für Inneres und Sport und die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung vorbereitet. Wir haben mit Vertreterinnen und Vertretern beider Häuser hierzu erste Beratungsgespräche geführt.

Hierbei haben wir insbesondere auf die Beachtung folgender Vorgaben der JI-Richtlinie bei ihrer Umsetzung in landesrechtliche Regelungen hingewiesen:

Gemäß der JI-Richtlinie müssen wir als Aufsichtsbehörde über wirksame Abhilfebefugnisse bei Verstößen gegen datenschutzrechtliche Bestimmungen durch

106 Richtlinie (EU) 2016/680 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 (JI-Richtlinie)

Polizei und Justiz verfügen.[107] Unsere bisherigen Möglichkeiten der Mangelfeststellung oder Beanstandung, die die betreffenden Behörden nicht verbindlich verpflichten, Datenschutzmängel abzustellen, genügen insoweit den Anforderungen der JI-Richtlinie nicht. Daher sollten konkrete Anordnungsbefugnisse in den neu zu schaffenden Regelungen vorgesehen werden.

Zudem müssen gesetzliche Bestimmungen geschaffen werden, die die datenverarbeitenden Stellen verpflichten, soweit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen[108] klar zu unterscheiden[109]. Zukünftig muss bei der Datenverarbeitung auch soweit wie möglich zwischen faktenbasierten Daten und solchen Daten unterschieden werden, die auf persönlichen Einschätzungen beruhen.[110]

Der Gesetzgeber muss darüber hinaus festlegen, welche Sanktionen bei einem Verstoß gegen die nach der JI-Richtlinie erlassenen Vorschriften zu verhängen sind, und muss die zu ihrer Anwendung erforderlichen Maßnahmen definieren.[111] Insoweit haben wir neben den bereits bestehenden Straftatbeständen die Schaffung von Bußgeldtatbeständen angeregt. Hierfür spricht, dass nicht jeder Datenschutzverstoß strafbewehrt sein muss; auch ein Bußgeld kann eine wirksame, verhältnismäßige und abschreckende Sanktion sein.

Wir haben auch empfohlen, Vorschriften, die für alle öffentlichen Stellen im Anwendungsbereich der JI-Richtlinie gelten sollen, vergleichbar dem neuen Bundesdatenschutzgesetz in einem eigenen Abschnitt im neuen Berliner Datenschutzgesetz zu regeln. Lediglich Normen, deren Adressaten nur ausgewählte öffentliche Stellen sind, sollten in den bereichsspezifischen Gesetzen[112] festgelegt werden. Diese Empfehlung wurde zwischenzeitlich aufgegriffen.

107 Art. 47 Abs. 2 JI-Richtlinie
108 Z. B. Straftäter, Opfer, Zeugen
109 Art. 6 JI-Richtlinie
110 Art. 7 Abs. 1 JI-Richtlinie
111 Art. 57 JI-Richtlinie i. V. m. ErwG 89
112 Z. B. im ASOG oder im JVollzDSG

Der Gesetzgeber muss bis zum 6. Mai 2018 seiner Pflicht zur Umsetzung der JI-Richtlinie nachkommen.[113] Ihm verbleibt also nur noch wenig Zeit. Wir werden den Prozess durch fachliche Beratung weiterhin unterstützen.

## 3.2 Sonderermittler im Fall Anis Amri – Akteneinsicht ohne ersichtliche Rechtsgrundlage



Der Senat von Berlin bestellte im März den früheren Bundesanwalt Bruno Jost als Sonderermittler, um mögliche Fehler und Versäumnisse von Mitarbeiterinnen und Mitarbeitern Berliner Behörden im Fall von Anis Amri, der am 19. Dezember 2016 in Berlin 12 Personen tötete und fast 100 Personen verletzte, aufzuklären. Aufgrund von Eingaben haben wir die Rechtmäßigkeit der Datenverarbeitung durch den Sonderermittler im Rahmen seiner Beauftragung überprüft.

Die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung berief sich uns gegenüber hinsichtlich der Beauftragung des Sonderermittlers auf ihre Dienst- und Fachaufsichtsrechte.[114]

Wir haben dies – unabhängig von der Erforderlichkeit und Wichtigkeit der Untersuchungen im Fall Amri – aus folgenden Gründen bemängelt:

Die von der Senatsverwaltung angeführte Rechtsgrundlage erlaubt weder eine Einsichtnahme in Akten, Unterlagen und Datensätze noch eine Befragung aller Dienstkräfte durch den Sonderermittler im vorgenommenen Umfang, so wie es mit ihm vertraglich vereinbart wurde. Andere Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch den Sonderermittler, wie etwa ein Beleihungsgesetz, sind ebenfalls nicht ersichtlich.

Das zweifellos bestehende Recht der Dienst- und Fachaufsicht der Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung umfasst aus verfassungs- und organisationsrechtlichen Gründen nicht das Recht, Aufgaben, die mit

113 Art. 63 Abs. 1 Satz 1 JI-Richtlinie

114 § 147 Nr. 2 GVG i. V .m. §§ 14 Abs. 1 Nr. 1, 22 Abs. 5 Nr. 3 AGGVG

Grundrechtseingriffen wie dem Eingriff in das Recht auf informationelle Selbstbestimmung verbunden sind, auf unabhängige externe Stellen außerhalb der staatlichen Verwaltung zu delegieren. Hierbei ist insbesondere zu berücksichtigen, dass solche externen Stellen selbst nicht der Dienst- und Fachaufsicht der Aufsichtsbehörde unterliegen und somit weder die Erteilung von Weisungen möglich noch eine entsprechende Kontrolle ihrer Tätigkeit gewährleistet ist.

Wir haben jedoch positiv zur Kenntnis genommen, dass sich die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung bemüht hat, eine missbräuchliche Verwendung der erhobenen Daten auszuschließen, indem sie vertragliche Regelungen zur Verschwiegenheit des Sonderermittlers und zu dessen Pflicht, nach Vertragserfüllung noch gespeicherte personenbezogene Daten zu löschen und entsprechende Unterlagen zu vernichten, vereinbart hat. Diese Vorgaben ersetzen zwar nicht die fehlende Rechtsgrundlage für die Datenverarbeitung, jedoch gewährleisten sie ein gewisses Maß an Schutz des informationellen Selbstbestimmungsrechts der von der Datenverarbeitung betroffenen Personen.

Wir haben die Verabschiedung eines entsprechenden Beleihungsgesetzes, das die Beachtung der Betroffenenrechte hinreichend garantiert, empfohlen, soweit erwogen wird, künftig in vergleichbaren Ausnahmesituationen wie dem Fall Amri externe Stellen mit der Untersuchung von Verwaltungsvorgängen zu beauftragen. Alternativ könnten verwaltungsinterne Juristinnen und Juristen mit entsprechenden Prüfungen beauftragt werden, die nicht in die zu untersuchenden Vorgänge eingebunden waren und im Rahmen der Dienst- und Fachaufsicht unabhängig agieren können.

Unabhängig hiervon besteht die Möglichkeit, dass ein vom Abgeordnetenhaus von Berlin eingesetzter Untersuchungsausschuss in Fällen wie dem vorliegenden gemäß § 29 Untersuchungsausschussgesetz (UntAG) einen externen Sachverständigen zur Begutachtung der Verwaltungsvorgänge hinzuzieht.

Es ist unabdingbar, das Handeln von Behörden mit umfassenden Ermittlungsmöglichkeiten prüfen und hinterfragen zu können. Hierbei sind jedoch die verfassungsrechtlichen Vorgaben zum Vorrang des Gesetzes und des informationellen Selbstbestimmungsrechts zu beachten.

## 3.3 Geldwäscheverdachtsmeldung ≠ Strafanzeige



Ein Petent beschwerte sich bei uns darüber, dass die Staatsanwaltschaft Informationen über die Einstellung eines Ermittlungsverfahrens gegen ihn wegen des Vorwurfs der Geldwäsche einer Bank mitgeteilt hat. Die Bank hatte zuvor eine Geldwäscheverdachtsmeldung gegenüber der Staatsanwaltschaft erstattet, aufgrund derer das Verfahren eingeleitet wurde.

Die Generalstaatsanwaltschaft erklärte gegenüber dem Petenten, dass Geldwäscheverdachtsmeldungen stets als Strafanzeigen anzusehen seien, weshalb die bei Strafanzeigen gesetzlich erforderliche Einstellungsmitteilung an die Bank in dem vorgenommenen Umfang zulässig gewesen sei.

Die fachaufsichtsführende Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung teilte diese Ansicht nicht. Sie erklärte uns gegenüber auf Anfrage, Geldwäscheverdachtsmeldungen und Strafanzeigen seien nicht gleichzustellen. Allerdings werde von den meldepflichtigen Personen bei Verwendung der gängigen Formulare oft ergänzend zu den Verdachtsmeldungen eine Strafanzeige gestellt.

Bezogen auf den vorliegenden Fall stützte sich die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung in ihrer rechtlichen Begründung zur Übermittlung von Informationen über die Einstellung des Strafverfahrens gegen den Petenten auf das Recht auf Auskunftserteilung, das Stellen, die Geldwäscheverdachtsmeldungen gegenüber der Staatsanwalt vornehmen, auf Antrag zusteht.[115] Ein entsprechender Antrag sei in der Bitte der Bank an die Staatsanwaltschaft im Zusammenhang mit der Geldwäscheverdachtsmeldung zu sehen, sie über den weiteren Verlauf des Verfahrens zu informieren.

Wir haben die Angelegenheit gegenüber der Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung rechtlich wie folgt bewertet:

115 § 11 Abs. 8 Satz 3 GwG a. F. i. V. m. § 475 Abs. 4, 1 StPO

Die Übermittlung der näheren Erläuterungen zur Einstellung des Ermittlungsverfahrens gegen den Petenten durch die Staatsanwaltschaft an die Bank war unzulässig, da hierfür keine Rechtsgrundlage vorlag. Sie ist daher zu bemängeln.

Es ist bereits zweifelhaft, ob die allgemeine Bitte der Bank, im Rahmen der von ihr vorgenommenen Verdachtsmeldungen an die Staatsanwaltschaft über den weiteren Verlauf des Verfahrens informiert zu werden, einen Antrag auf Aktenauskunft darstellte. Selbst wenn man dies bejahen würde, hätte man jedenfalls vor Auskunftserteilung um Mitteilung des berechtigten Interesses bitten müssen, da das Darlegen dieses Interesses Bedingung für die Auskunftserteilung ist.

Auf die Darlegung des berechtigten Interesses konnte auch nicht mit Verweis darauf verzichtet werden, dass eine solche Auskunft ohnehin nur zum Zwecke der Überprüfung des Meldeverhaltens erfolgen kann.[116] Zwar darf eine Auskunft nur zum vorgenannten Zweck erfolgen, jedoch muss der Antragsteller anhand des konkreten Einzelfalls begründen, warum und inwieweit eine Auskunft zur Überprüfung seines Meldeverhaltens erforderlich ist. Anderenfalls wären die gesetzlichen Voraussetzungen für eine Auskunftserteilung[117] nicht durch die Staatsanwaltschaft überprüfbar.

Aber auch wenn die Bank einen begründeten Auskunftsantrag gestellt hätte, hätte die Staatsanwaltschaft keine weiteren Informationen zum Verlauf und zum Ergebnis der Ermittlungen in der vorgenommenen Weise übermitteln dürfen, da diese Informationen zur Überprüfung des Meldeverhaltens der Bank nicht erforderlich waren. Insbesondere die allgemeinen Mutmaßungen zur Herkunft der Gelder im Einstellungsbescheid stellen keine substanziellen Aussagen dar, anhand derer die Bank ihr konkretes Meldeverhalten anpassen bzw. verbessern könnte.

Die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung teilte uns mit, sie werde den Fall zum Anlass nehmen, das Verfahren bei Geldwäscheverdachtsmeldungen zu überprüfen und entsprechende Änderungen an dem verwendeten Formular vorzunehmen.

116 Siehe § 11 Abs. 8 Satz 3 GwG a. F.

117 „soweit erforderlich" und „soweit dargelegt" in § 11 Abs. 8 Satz 3 GwG a. F. i. V. m. § 475 StPO

Die Nichtbeachtung der gesetzlichen Voraussetzungen für die Auskunftserteilung aus Strafverfahrensakten kann erhebliche nachteilige Auswirkungen auf die hiervon Betroffenen haben. Die Staatsanwaltschaft ist daher verpflichtet, in jedem Einzelfall genau zu prüfen, welche Informationen sie aus welchen Gründen an Dritte weitergeben darf.

## 3.4 Ausweitung der Videoüberwachung im ÖPNV



Seitdem die ersten Videokameras vor über 20 Jahren auf den Verkehrsflächen des Öffentlichen Personennahverkehrs (ÖPNV) im Land Berlin installiert wurden, hat sich viel verändert. Mittlerweile gibt es eine umfangreiche Videoüberwachung auf den U- und S-Bahnhöfen, aber auch innerhalb der Züge.

Die beiden größten Berliner Verkehrsunternehmen sind die Berliner Verkehrsbetriebe (BVG) als Betreiber der U-Bahn-, Straßenbahn- und Omnibusnetze und die S-Bahn Berlin GmbH. Da es sich bei der BVG um einen landeseigenen Betrieb handelt, die S-Bahn Berlin GmbH hingegen privatrechtlich organisiert ist, basiert die Videoüberwachung auf unterschiedlichen Rechtsgrundlagen. Die grundsätzlichen rechtlichen Rahmenbedingungen sind jedoch ähnlich. In jedem Fall ist eine pauschale Videoüberwachung ohne den Nachweis ihrer Erforderlichkeit unzulässig.

**Videoüberwachung bei der BVG**

Derzeit werden 54 der ca. 180 U-Bahnhöfe permanent vollüberwacht, was bedeutet, dass in der Regel alle 25 bis 30 Meter eine Videokamera installiert ist. Diese 54 Bahnhöfe wurden ausgewählt, da es sich hierbei um besondere Kriminalitätsschwerpunkte handelt, an welchen Übergriffe auf Kunden und Personal der BVG zu erwarten sind.

An den übrigen 128 U-Bahnhöfen kommt Videotechnik lediglich anlassbezogen, d. h. zur Zugabfertigung und beim Absetzen von Notrufen an Notrufsäulen, zum Einsatz. Die BVG hat uns darüber informiert, dass bis Ende 2018 auch diese Bahnhöfe vollüberwacht werden sollen. Die BVG begründet die Ausweitung der Überwachungsmaßnahmen mit der ansteigenden Kriminalität auf den U-Bahnhöfen und in den Zügen im Allgemeinen.

Wir haben die BVG darauf hingewiesen, dass eine pauschale flächendeckende Videoüberwachung unzulässig ist. Vielmehr muss bei jedem Bahnhof im Einzelfall geprüft werden, ob objektive Anhaltspunkte dafür bestehen, dass eine Videoüberwachung erforderlich ist. Anhand einer Risikoanalyse muss die BVG nachweisen, dass konkrete Anhaltspunkte für kriminelle Handlungen an einzelnen Bahnhöfen zu erwarten sind. Die BVG hat in einem zweiten Schritt zu prüfen, ob andere wirksame Maßnahmen (z. B. mehr Sicherheitspersonal auf den Bahnhöfen, verbesserte Beleuchtung) in Betracht kommen, die weniger in das Persönlichkeitsrecht der Betroffenen eingreifen. Drittens muss die BVG begründen, dass keine Anhaltspunkte für ein Überwiegen schutzwürdiger Interessen der Betroffenen vorliegen. Die BVG hat uns versichert, dass diese gesetzlich vorgesehene Vorgehensweise eingehalten wird.

Wir haben die BVG aufgefordert, uns in Stichproben die Ergebnisse ihrer Einzelfallprüfungen von ausgesuchten Bahnhöfen vorzulegen, die künftig mit Videoüberwachung ausgestattet werden sollen. Diese sollten Belege enthalten, dass auf diesen Bahnhöfen mit Übergriffen zu rechnen ist, z. B. eine Dokumentation krimineller Vorfälle des vergangenen Jahres. Zudem haben wir von der BVG ein Sicherheitskonzept angefordert, aus dem hervorgeht, wie die Videoüberwachung zukünftig solche Vorfälle verhindern soll. Zum Redaktionsschluss lagen uns diese Unterlagen noch nicht vor.

### Videoüberwachung bei der S-Bahn

Auch die S-Bahn Berlin GmbH plant einen Ausbau ihrer Videoüberwachungsanlagen. Diese bezieht sich insbesondere auf die Überwachung des Innenraums von S-Bahnzügen, der bislang noch nicht überwacht wird. Auch hier gelten dieselben Grundsätze. Videoüberwachung darf nur dort eingesetzt werden, wo sie objektiv zu mehr Sicherheit beitragen kann und wo es keine anderen Mittel gibt, die dazu besser geeignet sind und gleichzeitig weniger in das Persönlichkeitsrecht eingreifen.

Wir haben auch die S-Bahn darauf hingewiesen, dass eine pauschale flächendeckende Videoüberwachung auch in Bezug auf die Zuginnenräume nicht zulässig ist. Aufgrund ihres größeren Streckennetzes hat die S-Bahn insbesondere zu prüfen, ob auf bestimmten Streckenabschnitten und zu bestimmten Zeiten eine Videoüberwachung überhaupt erforderlich ist. Sollte die S-Bahn keine Erforderlichkeit für das gesamte Netz nachweisen können, muss eine Videotechnik zum

Einsatz kommen, die temporär abgeschaltet werden kann. Die S-Bahn hat uns zugesichert, dies zu berücksichtigen und uns in ihre künftigen Planungen einzubeziehen.

Verkehrsunternehmen, die auf ihren Bahnhöfen und in ihren Fahrzeugen eine Videoüberwachungsanlage betreiben, sind verpflichtet, zu überprüfen, ob die Videoüberwachung im Einzelfall erforderlich ist. Eine pauschale Ausweitung aufgrund öffentlichen oder politischen Drucks ohne einen tatsächlichen Mehrwert für die Sicherheit von Personal und Kunden ist nicht zulässig. Wir werden den Ausbau der Videoüberwachung durch die beiden Unternehmen weiter kritisch begleiten.

## 3.5 Hautnahe Beobachtung – Bodycams bei der Deutschen Bahn



Das seit Ende Juli 2016 von der Deutschen Bahn AG (DB) durchgeführte Pilotprojekt, bei dem Beschäftigte der DB Sicherheit mit Körperkameras, sog. Bodycams, ausgestattet wurden, ist im Frühjahr 2017 beendet worden. Über den Projektinhalt und -ablauf haben wir bereits ausführlich berichtet.[118] Im Sommer 2017 hat uns die DB ihren Abschlussbericht zu diesem Projekt vorgelegt und bereits Ende des Jahres 2017 an einigen Bahnhöfen mit dem Regelbetrieb begonnen.

Die Auswertung des Projekts hat ergeben, dass der Einsatz von Bodycams für viele Bereiche ungeeignet war. Es gibt aber auch sinnvolle Anwendungsbereiche. Ungeeignet ist die Bodycam insbesondere dazu, um die Sicherheit von Fahrgästen zu verbessern. Im gesamten Projektzeitraum wurde kein Fall festgestellt, in dem eine Bodycam zur Sicherheit der Fahrgäste beigetragen hat. Auch Verletzungen des Hausrechts und Sachbeschädigungen von Bahneigentum konnten damit weder verhindert werden noch haben die Aufnahmen dazu beigetragen, dass die Bahn Schadensersatzansprüche wegen Vandalismus gegen die Verursacher geltend machen konnte. Auch die mögliche Steigerung eines subjektiven Sicherheitsgefühls der Fahrgäste kann einen Eingriff in das Grundrecht auf informatio-

118 JB 2016, 3.8.2

nelle Selbstbestimmung nicht rechtfertigen. Bodycams dürfen Fahrgästen kein (trügerisches) Gefühl von Sicherheit vermitteln, wo objektiv die Sicherheit nicht erhöht wurde.

Das im Testzeitraum gesammelte Zahlenmaterial konnte aber belegen, dass Übergriffe auf Bahnpersonal, das mit einer Bodycam ausgestattet war, deutlich gegenüber konventionellen Streifen zurückgegangen sind. Daher kann der Einsatz der Bodycam beschränkt auf diesen Zweck unter bestimmten Voraussetzungen als zulässig erachtet werden:

Um den Persönlichkeitsrechten von Unbeteiligten Rechnung zu tragen, darf die Kamera insbesondere nur im konkreten Anwendungsfall und nur dann aktiviert werden, wenn ein Übergriff zu erwarten ist. Ein Dauerbetrieb, auch eine Pre-Recording-Funktion mit einem sich ständig überschreibenden Ringspeicherverfahren, ist unzulässig. Der Fokus der Kamera muss so eingestellt werden, dass nur ein begrenzter Bildausschnitt aufgenommen wird, damit möglichst keine im Hintergrund befindlichen Unbeteiligten erfasst werden.

Die Zielperson muss vor dem Einschalten der Bodycam auf diese hingewiesen werden. Sollte sich die Situation bereits durch diesen Hinweis entschärfen, darf die Bodycam nicht aktiviert werden. Der Testlauf hatte in diesem Zusammenhang ergeben, dass die Bodycam in der überwiegenden Anzahl der Konfliktsituationen nicht aktiviert werden musste, da zur Entschärfung der Situation ein bloßer Hinweis auf die Kamera ausreichte.

Des Weiteren muss die Maßnahme u. a. hinreichend transparent gemacht werden. Dazu gehört, dass die Bodycam sichtbar am Körper getragen wird und die entsprechenden Mitarbeiter eine Warnweste mit der Aufschrift „Videoüberwachung“ tragen. Bei Aktivierung der Bodycam muss ein optisches Signal erkennbar sein, z. B. ein rotes Licht, das die Aufnahme anzeigt. Sollte es zu einer Datenerhebung gekommen sein, ist der Betroffene unverzüglich in geeigneter Form, z. B. durch ein Merkblatt oder einen mündlichen Hinweis, über die Datenerhebung zu informieren.

Die gewonnenen Daten sind unmittelbar nach Beendigung der täglichen Arbeitszeit auszuwerten und ggf. der Bundespolizei zu übergeben. Nicht benötigte Daten

müssen unverzüglich – spätestens jedoch 24 Stunden nach Beendigung der Aufzeichnung – gelöscht werden. Der Einsatz der Bodycams muss regelmäßig evaluiert und von unabhängigen externen Gutachtern begleitet werden. Insbesondere ist festzustellen, ob und wie weit auch der Regeleinsatz dazu führt, dass Übergriffe auf das Sicherheitspersonal rückläufig sind.

Die DB hat uns zugesagt, dass die genannten Voraussetzungen eingehalten werden. Der Regelbetrieb beschränkte sich bei Redaktionsschluss auf Bahnhöfe in Berlin und Köln. Soweit weitere Bahnhöfe aufgenommen werden, muss die DB aber zunächst im Rahmen einer Vorabkontrolle prüfen, ob die Bodycam für das spezifische Einsatzgebiet geeignet und erforderlich ist. Gegebenenfalls kann der Schutz ihrer Beschäftigten vor Übergriffen an einigen Bahnhöfen statt durch den Einsatz von Bodycams auch durch datenschutzfreundlichere Maßnahmen erreicht werden. Dies könnten z. B. eine Veränderung der Beleuchtung oder bauliche Maßnahmen im Bahnhof sein. Ebenfalls könnten die Beschäftigten mit Funksprechgeräten ausgestattet werden, die es ermöglichen, im Konfliktfall unterstützendes Personal anzufordern. Erst wenn sämtliche alternativen Maßnahmen geprüft wurden und nicht wirkungsvoll zur Eigensicherung beitragen konnten, darf die Bodycam eingesetzt werden.

Die Bodycam kann unter bestimmten Bedingungen auch von privaten Unternehmen eingesetzt werden. Allerdings sind an den datenschutzgerechten Betrieb hohe Anforderungen zu stellen. Unternehmen, die ihr Sicherheitspersonal mit Bodycams ausstatten möchten, müssen zunächst prüfen, ob der Zweck der Überwachung nicht mit anderen Mitteln erreicht werden kann.

## 3.6 Biometrische Gesichtserkennung

Der Einsatz biometrischer Technik hat in den unterschiedlichsten Bereichen stark zugenommen. Die Technik wird nicht mehr ausschließlich im Sicherheitsbereich, sondern auch im Werbebereich oder zur Authentifizierung (z. B. Videoidentverfahren) eingesetzt. Dabei birgt die Verarbeitung der Gesichter von Personen erhebliche Sicherheitsrisiken, da sich ein solches biometrisches Charakteristikum meist über das ganze Leben nicht ändert. Die Erhebung biometrischer Merkmale

ist daher immer mit einem tiefen Eingriff in die Privatsphäre verbunden. Da man diese Merkmale bei einem Verlust nicht gleich einem Passwort ändern kann, können Betroffene unter Umständen ein Leben lang Opfer von Identitätsdiebstahl und Folgekriminalität werden.

Der wohl prominenteste Einsatz biometrischer Gesichtserkennung fand in Berlin am Bahnhof Südkreuz statt. Da es sich dabei zunächst um ein Projekt der Bundespolizei handelt, fiel die aufsichtsrechtliche Beurteilung in erster Linie in die Zuständigkeit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Als Berliner Aufsichtsbehörde für den Datenschutz werden wir dennoch regelmäßig zu dem Projekt befragt, zudem ist die Berliner Bevölkerung naturgemäß direkt von der Durchführung betroffen. Wir haben es uns daher angesichts der sich stellenden gravierenden datenschutzrechtlichen Fragen zur Aufgabe gemacht, die Berlinerinnen und Berliner über das Projekt aufzuklären und auf die o. g. Risiken dieser Technik hinzuweisen.[119] Aufgrund verschiedener Unregelmäßigkeiten hatte die Bundesbeauftragte zwischenzeitlich die Unterbrechung des umstrittenen Projektes gefordert.

Der Einsatz biometrischer Gesichtserkennung beschränkt sich jedoch nicht auf den Sicherheitsbereich. Wir sind auf ein Berliner Unternehmen aufmerksam geworden, welches ein System zur Außenwerbung betreibt. Dieses ermöglicht mithilfe von Sensoren an Informationsbildschirmen, biometrische Merkmale von Umstehenden zu erfassen und Alter und Geschlecht dieser Personen zu analysieren. Das Produkt soll nach Auskunft des Unternehmens der besseren Verwertung von Werbekontakten dienen und wird bundesweit bereits an mehr als 500 Standorten eingesetzt.[120]

Die an einem Bildschirm angebrachten (Kamera-)Sensoren erkennen und erfassen zunächst das Gesicht der Betrachtenden. Diese Bilder werden als Videostream für den Bruchteil einer Sekunde in einem Zwischenspeicher der Kamera abgelegt, bevor die darin verbaute Software sie in Histogramme umwandelt. Die Kamera verfügt zudem über einen sog. Kalibriermodus, der eine Visualisierung der auf-

119 Siehe Pressemitteilungen vom 23. Februar 2017 und 31. Juli 2017

120 Bisherige Einsätze in Filialen der Post, an Tankstellen, im Lebensmitteleinzelhandel und in Hotels

gezeichneten Bilder ermöglicht. Die visualisierten Bilddaten sind grundsätzlich personenbeziehbar, sodass das System wegen deren Erhebung und Verarbeitung grundsätzlich dem Regelungsbereich des Bundesdatenschutzgesetzes unterfällt.[121] Die von der Software analysierten Daten werden dazu verwendet, die auf dem Bildschirm ausgegebenen Werbebotschaften an Alter und Geschlecht der umstehenden Personen anzupassen.

Das Verfahren war zum Redaktionsschluss noch nicht abgeschlossen. Entscheidend für unsere Bewertung wird jedoch sein, ob die eingesetzte Software eine eindeutige Identifizierung der Betroffenen ermöglicht. Eine solche ist nämlich nach der im Mai 2018 wirksam werdenden DS-GVO Wirtschaftsunternehmen zu Werbezwecken ausdrücklich verboten.[122] Sofern eine eindeutige Identifizierung ausgeschlossen ist, kommt es maßgeblich darauf an, wie das Risiko eines Datenmissbrauchs[123] eingedämmt wird und wie die gesetzlichen Anforderungen an die Transparenz[124] erfüllt werden.

Der Einsatz von Videoüberwachung mit Gesichtserkennungsfunktionen ist mit erheblichen Risiken verbunden und nur in engen Ausnahmefällen zulässig. Die Datenschutz-Grundverordnung stellt klar, dass ohne Einwilligung des Betroffenen eine Verarbeitung biometrischer Daten zur Identifizierung nicht zu bloßen wirtschaftlichen Zwecken (z. B. Werbezwecken) erfolgen darf.

## 3.7 „Ich sehe dich nackt, was du nicht siehst!“ – Videoüberwachung in Umkleidebereichen

Durch mehrere Gäste einer Wellness-Einrichtung sind wir darauf aufmerksam gemacht worden, dass der Wellness-Betreiber die Umkleidebereiche seiner Anlage videoüberwacht. Über dieses Thema, die Videoüberwachung in sensitiven



121 § 3 Abs. 1 BDSG
122 Art. 9 Abs. 1 DS-GVO
123 Art. 25 DS-GVO
124 Art. 12 ff. DS-GVO

Bereichen, haben wir in der Vergangenheit bereits mehrfach berichtet und dabei ihre generelle Unzulässigkeit festgestellt.[125]

Als Grund für die Installation der Videokameras in den Umkleidebereichen nannte der Wellness-Betreiber den Schutz seiner Gäste vor Diebstählen durch Spindaufbrüche. Nach seiner Aussage gebe es keine wirkungsvollere Abschreckungsmaßnahme als die Videoüberwachung. Nach einer Vorortprüfung in der Wellness-Einrichtung haben wir dem Betreiber erläutert, dass die Videoüberwachung in den Umkleidebereichen in besonderem Maße in die Intimsphäre seiner Gäste eingreift; sie ist, solange diese keine echte Wahlmöglichkeit haben, generell unzulässig.[126] Da bei einer Videoüberwachung in Umkleidebereichen regelmäßig von einem überwiegend berechtigten Interesse der Gäste auszugehen ist, haben wir den Betreiber zunächst aufgefordert, die Kameras abzuschalten und alternative Sicherungsmaßnahmen zu prüfen.

Eine mögliche Alternative wäre die Installation von Wertschließfächern im Eingangs- und Empfangsbereich der Wellness-Einrichtung oder an Ausgabetresen für Handtücher und Bademäntel. Durch die Präsenz des dort tätigen Personals würden sich die Wertschließfächer im dauerhaften Sichtbereich befinden, wodurch ein Aufbrechen sofort bemerkt würde. Damit wäre der Anreiz, die Spinde in den Umkleidebereichen aufzubrechen, deutlich reduziert.

Der Wellness-Betreiber war allerdings der Auffassung, dass einzig eine Videoüberwachung einen angemessenen Schutz biete. Wir haben ihm daraufhin mitgeteilt, dass nur in Ausnahmefällen eine eingeschränkte Videoüberwachung durchgeführt werden könne, wenn zuvor sämtliche Alternativen ausgeschöpft sind und diese nachweislich nicht zur Verbesserung der Situation geführt haben. Diese eingeschränkte Videoüberwachung wäre nur zulässig, wenn die Gäste eine Wahlmöglichkeit zwischen überwachten und nicht überwachten Umkleidebereichen hätten, d. h., wenn zu gleichen Teilen sowohl überwachte als auch nicht überwachte Umkleideräume für Damen und Herren zur Verfügung gestellt würden. Am Eingang müssten die Gäste vom Personal informiert werden, dass es überwachte und nicht überwachte Umkleidebereiche gibt; zudem verlangt die Hinweispflicht,

125 Siehe JB 2011, 2.4

126 § 6b Abs. 1 Nr. 3 BDSG i. V. m. § 28 Abs. 6 bis 9 BDSG

die überwachten Umkleidebereiche zusätzlich mit Schildern kenntlich zu machen. Nur unter dieser Voraussetzung wäre eine freie Entscheidung über die Wahl des Umkleidebereichs möglich.

Schutzwürdige Interessen der Betroffenen überwiegen immer, wenn die Intimsphäre der betroffenen Personen berührt ist, weswegen eine Videoüberwachung von Personen in Umkleidebereichen grundsätzlich unzulässig ist. Ausnahmen können nur dann bestehen, wenn keine anderen Maßnahmen in Betracht kommen und die Betroffenen sich freiwillig der Videoüberwachung aussetzen.

# 4 Wohnen und Umwelt

## 4.1 Wohnberechtigungsschein – Nur mit Mutterpass?

Aus der Praxis

Um eine Wohnung zu beziehen, die mit öffentlichen Mitteln gefördert wird („Sozialwohnung"), wird ein Wohnberechtigungsschein (WBS) benötigt, der von den Bürgerämtern der Bezirke ausgestellt wird. Das zuständige Bezirksamt prüft, ob die Voraussetzungen des Wohnraumförderungsgesetzes gegeben sind. Dabei ist u. a. zu beachten, ob und wie viele Kinder einziehen sollen. In diesem Rahmen werden auch Schwangerschaften berücksichtigt, wenn der dritte Schwangerschaftsmonat überschritten wurde.

Um dies zu prüfen, wird von den zuständigen Behörden meist ein ärztliches Attest oder eine Kopie des Mutterpasses verlangt. Da ein solches Attest in vielen Fällen nur gegen eine Gebühr ausgestellt wird, entscheiden sich viele Frauen für den Nachweis durch den Mutterpass.

Datenschutzrechtlich problematisch ist dabei, dass im Mutterpass eine Vielzahl von Daten enthalten sind, die über den Schwangerschaftsmonat hinausgehen. So ist z. B. dort verzeichnet, ob die Betroffene an Geschlechtskrankheiten leidet. Die Erhebung solcher Gesundheitsdaten ist nicht nur für den Antrag auf einen Wohnberechtigungsschein irrelevant, sie greift auch tief in das Persönlichkeitsrecht ein. Die Erhebung ist daher in diesem Zusammenhang unzulässig. Alle Daten, die für die Feststellung der Schwangerschaftswoche irrelevant sind, sollten daher in der jeweiligen Kopie vor der Antragstellung von der Betroffenen geschwärzt werden.

Wir haben das betreffende Bezirksamt auf diese Rechtslage hingewiesen. Die Thematik wurde in der Zusammenkunft der Fachämter der Bezirke besprochen, sodass die Problematik mittlerweile in allen Bezirksämtern bekannt sein dürfte. Zusätzlich haben wir die Senatsverwaltung für Stadtentwicklung und Wohnen gebeten, in den entsprechenden Antragsformularen und Informationsmaterialien auf die Schwärzungsmöglichkeit hinzuweisen. Dies wurde uns von der Senats-

verwaltung bereits bestätigt. Zusätzlich wurden die Bezirke angehalten, mögliche selbstverfasste Informationen oder Online-Erläuterungen anzupassen.

Bei der Bearbeitung von Anträgen auf einen Wohnberechtigungsschein dürfen aus dem Mutterpass nur die Daten zur Bestimmung der Schwangerschaftswoche erhoben werden. Alle anderen Daten sollte die Antragstellerin in der Kopie des Mutterpasses schwärzen.

## 4.2 Wann, was, wer? – Exzessive Datenerhebung bei der Durchsetzung des Zweckentfremdungsverbots



Das Zweckentfremdungsverbot-Gesetz soll seit einigen Jahren verhindern, dass in den zentralen Bezirken Berlins Wohnraum leer steht bzw. als Ferienwohnung oder Geschäftsraum genutzt und so dem regulären Wohnungsmarkt entzogen wird. Um dieses wichtige Anliegen durchzusetzen und zu kontrollieren, ob Wohnungen zu Wohnzwecken genutzt werden, stehen den Bezirksämtern nach dem Zweckentfremdungsverbot-Gesetz weitreichende Befugnisse zu. Unter Umständen dürfen sie sogar Wohnungen betreten und Vor-Ort-Kontrollen durchführen.

Dennoch sind einige Behörden über das Ziel hinausgeschossen. So wurden zum Beispiel Wohnungsinhaberinnen und -inhaber aufgefordert, eine Aufstellung vorzulegen, zu welchen Zeiten sie in der Wohnung geschlafen, sich Mahlzeiten zubereitet, Familienangehörige getroffen haben und welchen gesellschaftlichen Aktivitäten sie dort nachgegangen sind. In anderen Fällen wurden die Betroffenen aufgefordert, Theater- und Opernkarten oder Tankrechnungen einzureichen, obwohl diese für die Art der Wohnungsnutzung kaum verlässliche Anhaltspunkte bieten.

Wir haben den betreffenden Bezirksämtern mitgeteilt, dass diese Art der Datenerhebung über das gesetzlich Zulässige weit hinausgeht. Erlaubt ist hingegen, die Wohnungsinhaber zu befragen, ob und in welchem zeitlichen Umfang sie die Wohnung zu Wohnzwecken nutzen, da dies für die Erfüllung der Aufgaben aus dem Zweckentfremdungsverbot-Gesetz erforderlich und vom Wortlaut des Gesetzes gedeckt ist.

Der Bezirk Tempelhof-Schöneberg hat unsere Empfehlung sogleich aufgegriffen und praktisch umgesetzt.

Wir hoffen, dass auch andere Bezirke diesem guten Beispiel zeitnah folgen werden, da es zeigt, dass die Verhinderung der zweckwidrigen Nutzung von Wohnraum auch im Einklang mit den Datenschutzgesetzen möglich ist.

## 4.3 „Kennste einen, kennste alle“ – Datenschutzverstöße von Vermietungsgesellschaften bei Mietbewerbungsverfahren



Bei der Überprüfung der von Vermietern verwendeten Formulare zur Selbstauskunft für Mietbewerbungen zeigte sich im Rahmen einer Branchenprüfung, dass in fast allen Fällen unrechtmäßige Datenabfragen erfolgten.

Aus der kaum zu überblickenden Masse der Vermieter am Berliner Wohnungsmarkt wurde eine Stichprobe von gut 30 Unternehmen und Einzelpersonen überprüft. Diese wurden darauf hingewiesen, dass in den von ihnen im Vorfeld einer Wohnungsvermietung verwendeten Formularen zur Selbstauskunft unzulässige Abfragen erfolgten. Unzulässig erhoben wurden u. a. Angaben zur Staatsangehörigkeit, zum Familienstand oder dem vorherigen Mietverhältnis; außerdem fanden häufig Bonitätsabfragen bereits zu einem Zeitpunkt statt, zu dem noch nicht einmal das Interesse über eine Anmietung des betreffenden Wohnraums erklärt worden war. Der häufige Hinweis darauf, dass die Angaben freiwillig gemacht würden, konnte aufgrund der zu befürchtenden Benachteiligungen für weniger auskunftsfreudige Personen nicht überzeugen. Die Marktdominanz auf Vermieterseite führt zwangsläufig dazu, dass bei Mietbewerbungen nicht von freiwilligen Angaben ausgegangen werden kann.

Der Großteil der angeschriebenen Stellen zeigte sich einsichtig und änderte die verwendeten Formulare bzw. den Zeitpunkt, zu dem beispielsweise Abfragen zur Bonität erfolgen. Denn derartige Abfragen sind erst dann zulässig, wenn der Vertragsschluss nur noch von einem positiven Ergebnis der Auskunft abhängt. Auch bezüglich anderer Abfragen, beispielsweise zu den Daten über mit einziehende

Personen, musste mehrfach auf den zulässigen Umfang und Zeitpunkt hingewiesen werden.

Auch im nächsten Jahr werden wir Datenschutzverstößen beim Mietbewerbungsverfahren konsequent nachgehen. Aufgrund der hohen Anzahl der Unternehmen und des stark vermieterdominierten Marktes in Berlin ist zu befürchten, dass die mittlerweile als Massenverfahren geführten Vorgänge zu Mieterselbstauskünften auch im kommenden Jahr fortgeführt werden. Perspektivisch ist indes erst dann eine Besserung in Sicht, wenn der Mietmarkt in Berlin eine deutliche Entzerrung erfährt. Ebenso ist zu hoffen, dass die ab Mai 2018 durch die Datenschutz-Grundverordnung stark ansteigende Bußgeldhöhe Vermieter veranlasst, ihre gegenwärtige Praxis zu ändern. Anderenfalls ist zu befürchten, dass sich weiterhin viele Mieterinnen und Mieter bei der Wahl zwischen dem Schutz ihrer persönlichen Daten und einem Dach über dem Kopf für letzteres entscheiden (müssen).

Selbstauskünfte für Mietbewerbungen dürfen erst dann eingeholt werden, wenn ein ernsthaftes Interesse an der Anmietung bekundet wurde. Inhaltlich dürfen sodann ausschließlich für den Vertragsschluss erforderliche Angaben gefordert werden. Nachweise über die Bonität sind erst unmittelbar vor Vertragsschluss zulässig.

## 4.4 Gelöscht, aber noch online – Wohnungsvermittler lässt Nutzungsdaten offen im Netz liegen

Ein Anbieter für Wohnungsanzeigen im Internet hat über mehrere Jahre auf seiner Plattform hochgeladene Unterlagen teilweise so im Netz abgelegt, dass sie mithilfe von anderen Internetdiensten durchsucht werden konnten. In den Unterlagen befanden sich auch Daten zu den finanziellen und persönlichen Umständen Betroffener.

Wir gingen einem Hinweis aus der IT-Szene nach, wonach personenbezogene Daten aus dem Verantwortungsbereich des Unternehmens im Internet frei verfüg-

bar vorgehalten würden. Die geschätzte Anzahl der Dokumente bewegte sich im sechsstelligen Bereich.

In dem Verkaufs- oder Vermietungsangebot des betreffenden Wohnungsvermittlers können bei Schaltung einer Anzeige auch Bilder und Dokumente veröffentlicht werden. In aller Regel betrifft dies datenschutzrechtlich unbedenkliche Unterlagen wie z. B. Grundrisse und unausgefüllte Selbstauskunftsformulare. Mehrfach wurde der von der Plattform zur Verfügung gestellte Speicherplatz jedoch auch zur Zwischenspeicherung von Dokumenten, wie z. B. ausgefüllten Selbstauskunftsformularen oder Wirtschaftsplänen inklusive personenbezogener Daten, verwendet.

Die genannten Dokumente waren bis zur endgültigen Löschung der zugehörigen Anzeige weltweit abrufbar, auch wenn die Anzeige noch nicht freigegeben oder wieder deaktiviert wurde. Zudem waren Internet-Adressen der Dokumente leicht zu erraten, da sich die einzelnen Adressen nur in den Werten einer neunstelligen Zahl unterschieden, die zudem – wenn auch mit Lücken – für neue Anzeigen in fortlaufender Weise vergeben wurden. Für einen Hacker wäre es daher in kurzer Zeit und automatisiert möglich gewesen, sehr viele dieser Dokumente zu finden. Ein Teil dieser Dokumente war zudem in Suchmaschinen gelistet und somit potenziell für jeden Internetnutzer auch unbeabsichtigt auffindbar.

Wir haben von dem Unternehmen die unverzügliche Löschung der Dokumente gefordert und zusätzlich das Ergreifen von Maßnahmen zur Löschung der entsprechenden Einträge in den wichtigsten Suchmaschinen angemahnt. Diesen Forderungen ist das Unternehmen zwischenzeitlich nachgekommen. Zudem werden Nutzerinnen und Nutzer der Plattform beim Hochladen von Dokumenten nun deutlicher darauf hingewiesen, dass die Veröffentlichung personenbezogener Daten nicht gestattet ist.

Auch wenn die unzulässige Veröffentlichung personenbezogener Daten primär im Verantwortungsbereich der Nutzerinnen und Nutzern erfolgt, trägt eine Internetplattform einen wesentlichen Teil der Verantwortung mit, da bei der Nutzung davon ausgegangen werden kann, dass nicht (mehr) veröffentlichte Anzeigen und deren Inhalte Dritten nicht zugänglich sind. Ein datenschutzrechtlich verantwor-

tungsvolles Unternehmen sollte entsprechende Sicherheitslücken von Anfang an erkennen und angemessene Maßnahmen ergreifen.

Internetplattformen, die die Möglichkeit zum Hochladen von Daten für z. B. Wohnungsanzeigen anbieten, können die Verantwortung für die Sicherung dieser Daten nicht auf die Nutzerinnen und Nutzer der Plattform übertragen, sondern müssen selbst hinreichende Maßnahmen zur Verhinderung des Zugriffs Dritter ergreifen.

## 4.5 Keine Nutzung ohne Prüfung – Energieversorger und Verbraucherdaten



Zwei Unternehmen im Bereich der Energieversorgung hatten über Drittfirmen die Daten potenzieller Kunden erhalten. In beiden Fällen gab das jeweilige Unternehmen an, die Daten seien freiwillig und über Gewinnspiele der Drittfirmen zur werblichen Verarbeitung an diese übermittelt worden. In beiden Fällen konnten die Gewinnspielanbieter nicht belegen, dass die Daten von den Betroffenen selbst übermittelt worden waren.

Die beiden Eingaben zu zwei unterschiedlichen Unternehmen gründeten jeweils in den für die Petenten überraschenden Mitteilungen, ihre Energieversorger gewechselt zu haben. Zwar konnte in beiden Fällen der Vertragsschluss rückgängig gemacht werden. Die Herkunft der für den Vertrag notwendigen Daten blieb jedoch zunächst unklar und wurde auch auf Nachfrage von den Unternehmen nur unzureichend aufgeklärt.

Bei der Prüfung der Fälle konnten jeweils ähnlich gelagerte Geschäftsmodelle aufgedeckt werden, bei denen personenbezogene Daten potenzieller Kundschaft über von Drittfirmen im Internet angebotene Gewinnspiele erfasst werden sollen. Im Rahmen dieser Gewinnspiele werden dann auch umfassende Einwilligungserklärungen abgefordert, auf deren Grundlage die Personen nachträglich kontaktiert und mit einem Angebot eines Energieversorgers konfrontiert werden. Bei der Überprüfung der Gewinnspiele fielen sodann mehrere Verstöße sowohl bei der Datenerhebung als auch bei der entsprechenden Dokumentation auf. Die nicht in

Berlin ansässigen Gewinnspielanbieter stellten auf Nachfrage Gewinnspieldokumentationen bereit, welche neben den Daten der Petenten auch Werte und Angaben zum angeblichen Zeitpunkt der Teilnahme und der verwendeten IP-Adresse enthielten. Diese Dokumentationen waren jedoch nicht zum Beweis darüber geeignet, ob diese Angaben von den Petenten gemacht wurden. Dazu wurden Einwilligungserklärungen übersandt, die nicht den datenschutzrechtlichen Vorgaben entsprachen und teilweise lediglich auf den (ihrerseits unrechtmäßig ausgestalteten) Teilnahmebedingungen beruhten.

Wir haben die verantwortlichen Stellen auf die massiven Defizite ihrer Vertragspartner aufmerksam gemacht, woraufhin beide die jeweilige Zusammenarbeit eingestellt haben. Es erging zudem der Hinweis, dass sich die Unternehmen selbst davon hätten überzeugen müssen, dass die übermittelten Daten rechtmäßig durch die Vertragspartner erhoben wurden.

Die Verarbeitung der Daten war unrechtmäßig, sodass wir prüfen, ob gegen die Berliner Unternehmen ein Bußgeldverfahren eingeleitet wird. Die beteiligten Drittfirmen wurden an die jeweils zuständige Aufsichtsbehörde gemeldet.

Soweit Unternehmen personenbezogene Daten zur eigenen Verarbeitung von anderen Unternehmen erheben lassen, sind sie verpflichtet, die rechtmäßige Erhebung der Daten durch das beteiligte Unternehmen zu überprüfen. Die Verarbeitung unrechtmäßig durch Dritte erlangter Daten kann zur Einleitung eines Bußgeldverfahrens führen.

## 4.6 Speicherung von Parkbesuchen durch die Grün Berlin GmbH

Aus der Praxis

Parkanlagen dienen der Erholung und der Freizeitgestaltung. Sie sollen den Menschen Rückzugsräume bieten, in welchen sie sich entspannen und erholen können. An solchen Orten sollte man überwachungsfreie Räume erwarten können. Umso mehr hat uns die Praxis der Grün Berlin GmbH verwundert, Parkbesuche von Inhaberinnen und Inhabern von Jahreskarten aufzuzeichnen und genau zu dokumentieren, wann diese den Britzer Garten und die Gärten der Welt betreten

haben. Die Daten wurden über die gesamte Vertragsdauer gespeichert, die unter Umständen mehrere Jahre betragen konnte.

Die Grün Berlin GmbH wurde vom Land Berlin mit der Bewirtschaftung dieser Parkanlagen betraut. Das Unternehmen hatte bereits im Jahr 2015 damit begonnen, ein elektronisches Kassen- und Zugangssystem einzuführen. In diesem Zusammenhang bekamen Erwerberinnen und Erwerber von Jahreskarten Chipkarten ausgehändigt, durch die sie Zugang zu dem jeweiligen Park erhielten.

Da die Grün Berlin GmbH uns keinen plausiblen Grund für die Speicherung der Zugangsprofile nennen konnte, teilten wir ihr im September 2016 mit, dass die Datenverarbeitung unzulässig ist. Dennoch war das Unternehmen zunächst nicht bereit, auf die Datenerhebung zu verzichten. Als Begründung wurde uns u. a. mitgeteilt, dass es sich dabei um eine standardisierte Verwaltungssoftware handele. Außerdem erhoffe man sich davon, unberechtigte Zutritte zu verhindern.

Diese Argumente konnten jedoch nicht überzeugen. Insbesondere kann auch mit der Speicherung der Nutzungsprofile nicht ausgeschlossen werden, dass die Chipkarte weitergegeben und durch Unberechtigte genutzt wird. Allenfalls kann dadurch verhindert werden, dass sich mehrere Personen gleichzeitig mit derselben Jahreskarte Zutritt zum Park verschaffen. Dafür ist jedoch eine Speicherdauer von einem Tag völlig ausreichend.

Da das Unternehmen nicht bereit war, sich an die gesetzlichen Vorgaben zu halten, haben wir den Vorgang förmlich gegenüber der Senatsverwaltung für Umwelt, Verkehr und Klimaschutz beanstandet. Erst dann wurde uns die Umsetzung der datenschutzrechtlichen Vorgaben zugesagt.

Ein ähnliches Problem bestand auch bei den Toren zu den angrenzenden Friedhöfen. Auch hier wurde ein elektronisches Schließsystem eingebaut, welches registriert, wann die Schlüsselinhaber den Friedhof betreten, um die Gräber ihrer Angehörigen zu besuchen. Auch hier konnte das Unternehmen trotz mehrfacher Nachfragen nicht darlegen, wie damit Fälle des Schlüsselmissbrauchs durch Friedhofsbesucher verhindert werden sollen, sodass diese Praxis schließlich eingestellt werden musste.

Der Vorgang zeigt, wie wichtig es ist, dass unsere Behörde die Befugnis erhält, auch gegen Unternehmen der öffentlichen Hand wirksame Maßnahmen zu ergreifen. Ansonsten müssen Bürgerinnen und Bürger, die sich über ein solches Unternehmen beschweren, wie in diesem Fall sehr lange auf die Beseitigung von Missständen warten. Erfreulicherweise ist in der Datenschutz-Grundverordnung, die im Mai 2018 wirksam wird, eine solche Verbesserung des Rechtschutzes angelegt.[127] Dies setzt allerdings voraus, dass der Berliner Gesetzgeber diese nicht untergräbt, indem er die Möglichkeiten der Verwaltungsvollstreckung und der Verhängung von Bußgeldern wieder einschränkt.

127 Siehe 1.1

# 5 Verkehr und Tourismus

## 5.1 Fotokopien amtlicher Ausweisdokumente für die Kraftfahrzeugzulassung?



Eine Petentin wandte sich an uns, da die Kraftfahrzeugzulassungsstelle beim Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) für die Zulassung von Kraftfahrzeugen durch Zulassungsdienste regelmäßig die Vorlage des Personalausweises bzw. des Reisepasses der künftigen Halterin oder des künftigen Halters im Original verlangt. Während der gesamten Bearbeitungsdauer, in der Regel etwa eine Woche, ist das Personaldokument dann beim LABO hinterlegt. Die Betroffenen können in diesem Zeitraum nicht über ihr Personaldokument verfügen. Die Petentin bat um Klärung, ob die Dauer der Hinterlegung mit den Regelungen im Personalausweisgesetz im Einklang steht bzw. ob statt der Hinterlegung des Ausweisdokuments nicht die Anfertigung einer Fotokopie in Betracht kommen könne.

Wir wiesen das LABO darauf hin, dass beispielsweise in Thüringen unter bestimmten Voraussetzungen Fotokopien anstelle der Originaldokumente akzeptiert werden, und baten vor diesem Hintergrund um Stellungnahme zur Erforderlichkeit der Hinterlegung der Original-Ausweisdokumente über einen Zeitraum von mehreren Tagen sowie um Prüfung, ob unter entsprechenden Voraussetzungen die Vorlage von Fotokopien anstelle der Hinterlegung der amtlichen Dokumente in Betracht kommen könne.

Das LABO teilte uns hierauf mit, dass bei der Zulassung von Kraftfahrzeugen die Vorlage eines Ausweisdokuments verlangt wird, da die Halterdaten anzugeben und auf Verlangen nachzuweisen seien.[128] Fotokopien von Ausweisdokumenten könnten vor diesem Hintergrund nicht akzeptiert werden, da ein öffentliches Interesse an einem ordnungsgemäßen Zulassungsverfahren und der Vermeidung von Missbrauch bestehe und die Akzeptanz von Fotokopien das Risiko von Scheinan-

128 § 6 Abs. 1 FZV i. V. m. § 33 Abs. 1 Satz 1 Nr. 2 StVG

meldungen deutlich erhöhe. Auch sei für die Zulassungsbehörde nicht überprüfbar, ob die Fotokopie des Personalausweises von der Ausweisinhaberin bzw. dem Ausweisinhaber mit deren Zustimmung[129] erfolgt sei. Im Übrigen bestehe keine zeitliche Beschränkung der Hinterlegung von Ausweisdokumenten zum Zwecke der Identitätsfeststellung, vielmehr sei diese zulässig, solange sie erforderlich sei. Schließlich könne im Einzelfall die Identitätsprüfung bereits bei der Einreichung des Zulassungsantrags erfolgen, sodass eine weitere Hinterlegung nicht erforderlich sei.

Die Entscheidung des LABO, im Kraftfahrzeugzulassungsverfahren keine Fotokopien von Ausweisdokumenten anzuerkennen, war vor dem Hintergrund der Vermeidung von Missbrauch sowie dem öffentlichen Interesse an einem ordnungsgemäßen Zulassungsverfahren nicht zu beanstanden. Einerseits ist die Hinterlegung von Ausweisdokumenten nicht zwingend, da die Nutzung von Zulassungsdiensten freiwillig ist. Andererseits besteht tatsächlich keine konkrete zeitliche Beschränkung für die Hinterlegung von Ausweisdokumenten zum Zwecke der Identitätsfeststellung. Eine dauerhafte Hinterlegung wäre zwar unzulässig, hingegen ist die Hinterlegung für eine kurze Zeitspanne von etwa einer Woche nicht zu beanstanden.

Der Fall zeigt, dass die erst im Juli 2017 ausdrücklich normierte Zulässigkeit der Anfertigung von Personalausweiskopien[130] erheblichen praktischen Bedenken begegnet, da vom Empfänger einer solchen Fotokopie nicht geprüft werden kann, ob diese von der Ausweisinhaberin bzw. dem Ausweisinhaber mit deren Zustimmung angefertigt wurde. Verfahren, in denen Antragstellerinnen und Antragsteller sich bislang ausweisen müssen bzw. ihr Ausweisdokument zur Identitätsfeststellung hinterlegen müssen, sind daher prädestiniert dafür, künftig über das Service-Konto Berlin[131] angeboten zu werden.

129 § 20 Abs. 2 PAuswG

130 § 20 Abs. 2 PAuswG, geändert durch Artikel 1 des Gesetzes zur Förderung des elektronischen Identitätsnachweises vom 7. Juli 2017, BGBl. I, S. 2310 mit Wirkung vom 15. Juli 2017

131 Siehe auch 2.1

## 5.2 Vorlage des Berlinpasses beim Kauf von Tickets für den ÖPNV



Mehrere Petenten beschwerten sich darüber, dass sie beim Kauf des vergünstigten Berlin-Tickets S in Verkaufsstellen der Berliner Verkehrsbetriebe (BVG) ihren Berlinpass[132] vorlegen mussten, aus dem sich der Name und der Beginn des Leistungsbezugs ergibt. Das Berlin-Ticket S sei auch an den Fahrscheinautomaten der BVG – und zwar ohne Kontrolle des Berlinpasses – erhältlich und ohnehin nur in Verbindung mit diesem gültig.

Die Kontrolle des Berlinpasses beim Kauf der Fahrkarte in Verkaufsstellen und die damit einhergehende Datenerhebung waren nicht erforderlich[133], da das Berlin-Ticket S ohnehin nur mit eingetragener Berlinpass-Nummer und in Verbindung mit diesem genutzt werden kann. Gegen die Erforderlichkeit sprach zudem, dass das Ticket ohne entsprechende Kontrolle an Fahrscheinautomaten erworben und die Berlinpass-Nummer sodann von den Kundinnen und Kunden selbst eingetragen werden kann.

Hierzu teilte uns die BVG mit, dass die Kundinnen und Kunden beim Erwerb des Tickets am Fahrscheinautomaten die besondere Verantwortung hätten, die Berlinpass-Nummer selbst zu übertragen. Um sicherzustellen, dass eine ordnungsgemäße Eintragung der Berlinpass-Nummer auf dem Ticket erfolge, ließen sich die Mitarbeiterinnen und Mitarbeiter in den Verkaufsstellen den Berlinpass vorzeigen. Dies erfolge als reine Serviceleistung, damit die Kundinnen und Kunden sich im Falle einer Kontrolle im Besitz eines gültigen Fahrausweises befänden.

Wir stellten gegenüber der BVG klar, dass es ausreicht, die Kundinnen und Kunden auf die Verpflichtung zum ordnungsgemäßen Eintragen der Berlinpass-Nummer beim Erwerb des Berlin-Tickets S hinzuweisen. Die Eintragung der Berlinpass-Nummer durch die Mitarbeiterinnen und Mitarbeiter in den Verkaufsstellen darf zwar als freiwillige Serviceleistung angeboten, nicht jedoch verpflichtend

132 Der Berlinpass ermöglicht Berlinerinnen und Berlinern, die Arbeitslosengeld II, Sozialhilfe, Grundsicherung oder Leistungen nach dem Asylbewerberleistungsgesetz erhalten, u. a. den Erwerb vergünstigter Tickets im öffentlichen Nahverkehr.

133 § 9 BlnDSG

verlangt werden. Wir forderten die BVG auf, die Praxis in den Verkaufsstellen entsprechend anzupassen.

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist nur dann zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der jeweiligen Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist.[134] Die BVG darf demzufolge nur solche Daten verarbeiten, die sie zur Erfüllung der konkreten Aufgabe tatsächlich benötigt.

## 5.3 Gläserne Gruppenreisende

Aus der Praxis

Ein Petent, der über einen Reiseanbieter eine Flugreise nach Sri Lanka gebucht hatte, machte uns darauf aufmerksam, dass er anhand der Angaben auf seinem Flugticket über die Buchungsseite der Fluggesellschaft auf personenbezogene Daten anderer Passagiere zugreifen konnte.

Die Fluggesellschaft teilte uns hierzu mit, dass unter bestimmten Bedingungen tatsächlich die Namen sowie Sitzplatznummern von anderen Mitreisenden eingesehen werden könnten. Dazu könne es immer dann kommen, wenn der Reiseanbieter die Betroffenen als Mitglieder einer Reisegruppe benannt und unter Verwendung einer einzigen Buchungsnummer gebucht habe.

Wir konnten dem Petenten die erfreuliche Mitteilung machen, dass die Fluggesellschaft die Buchungsplattform auf seine Eingabe hin dahingehend geändert hat, dass künftig keine Möglichkeit mehr zum Abruf von Fluggastdaten Mitreisender besteht. Von dieser Änderung können künftig weltweit alle Kundinnen und Kunden der Fluggesellschaft profitieren.

Buchungsplattformen dürfen nicht den Abruf von Fluggastdaten Mitreisender ermöglichen.

134 § 9 Abs. 1 BlnDSG

## 5.4 Kopien beim Check-in



Ein Petent beschwerte sich bei uns darüber, dass beim Check-in in einem Hotel von ihm und seinen Mitreisenden verlangt worden sei, die Reisepässe und Kreditkarten zur Anfertigung von Fotokopien herauszugeben. Trotz ausdrücklichen Widerspruchs habe der Mitarbeiter an der Rezeption darauf bestanden und erklärt, dies werde auch in allen anderen Hotels so gehandhabt.

Das Hotel teilte uns mit, dass tatsächlich in Einzelfällen Fotokopien von Ausweisdokumenten und Kreditkarten angefertigt worden seien, um die zum Teil nicht zu entziffernden Daten auf den Meldescheinen der Gäste korrekt in die Gästekarteien einzufügen. Zudem wies man uns auf die terroristischen Ereignisse in Europa und auch in Berlin hin. Eine Rechtsgrundlage für die Anfertigung der Fotokopien gab es jedoch vorliegend nicht, die Datenverarbeitung war deshalb rechtswidrig.[135] Das Hotel hat die Anfertigung derartiger Fotokopien daraufhin eingestellt.

Die Anfertigung von Fotokopien von Ausweisdokumenten und Kreditkarten ist zur Durchführung des Beherbergungsvertrags regelmäßig nicht erforderlich und damit unzulässig. Sollten Eintragungen eines Gastes im Meldeschein für die Mitarbeiterinnen und Mitarbeiter an der Rezeption nicht lesbar sein, muss ggf. beim Gast nachgefragt werden.

## 5.5 Neugieriger Meldeschein



Ein Petent wandte sich an uns, da beim Check-in in einem Hotel von ihm verlangt wurde, seine Personalausweisnummer in den Meldeschein einzutragen. Auf seinen Protest, dass er als deutscher Staatsangehöriger nicht zur Angabe seiner Personalausweisnummer verpflichtet sei, habe der Mitarbeiter an der Rezeption mit Unverständnis reagiert und ihm mitgeteilt, dass er nicht in diesem Hotel übernachten müsse. Da er bereits eine Anzahlung geleistet hatte, hat der Petent dann notgedrungen seine Personalausweisnummer preisgegeben.

135 § 28 Abs. 1 Satz 1 Nr.1 BDSG

Das Vorgehen des Hotels war rechtswidrig, da nur bei ausländischen Gästen die Seriennummer des Ausweispapiers erfasst werden darf.[136] Das Hotel teilte uns auf Nachfrage mit, dass die Personalausweisnummer aufgrund eines Versehens des Mitarbeiters an der Rezeption verlangt worden sei. Die Personalausweisnummer sei inzwischen vernichtet worden.

Als Muster eines Meldescheins übersandte man uns den Auszug aus einer Tabelle, in der neben einer fortlaufenden Nummer u. a. Spalten für Namen, Anschriften und Seriennummern von Reisepässen aufgeführt waren. Es kam nicht etwa ein Meldeschein pro Gast zum Einsatz, sondern ein Sammel-Formular mit insgesamt 17 Zeilen für 17 Gäste. Das Hotel erläuterte, dass angesichts der Vielzahl an Gästen einzelne Meldescheine keine praktikable Lösung seien. Auf unsere Bedenken, dass Gäste hierdurch die Daten anderer Gäste einsehen könnten, wurde uns mitgeteilt, dass dies schon wegen der Unleserlichkeit der Daten als wenig problematisch angesehen werde.

Wir forderten das Hotel auf, den Einsatz von Sammelmeldescheinen einzustellen und künftig nur noch gesonderte Meldescheine pro Gast einzusetzen.

Meldescheine dürfen ausschließlich das Datum der Ankunft und das der voraussichtlichen Abreise, den Familiennamen nebst Vornamen, das Geburtsdatum, die Staatsangehörigkeiten, die Anschrift, die Zahl der Mitreisenden und ihre Staatsangehörigkeit sowie bei ausländischen Personen die Seriennummer des anerkannten und gültigen Passes oder Passersatzpapiers enthalten.[137] Diese sind so aufzubewahren, dass keine unbefugte Person – also insbesondere auch kein anderer Gast – sie einsehen kann.[138]

136 § 30 Abs. 2 Satz 1 Nr. 8 BMG
137 § 30 Abs. 2 Satz 1 BMG
138 § 30 Abs. 4 Satz 3 BMG

# 6 Jugend und Bildung

## 6.1 Was lange währt, wird endlich gut? – Neues zu den Ausführungsvorschriften für Maßnahmen zum Kinderschutz



Seit 2015[139] berichten wir über das Verfahren zur Neufassung der Ausführungsvorschriften für die Durchführung von Maßnahmen zum Kinderschutz in den Berliner Jugend-, Gesundheits- und Sozialämtern. Erneut haben wir uns mit dem Entwurf der Ausführungsvorschriften befasst.

Zweck der Vorschriften ist die Konkretisierung der gesetzlichen Aufgabenzuweisungen sowohl für den Umgang mit Fällen von Kindeswohlgefährdung als auch für präventive Maßnahmen im Bereich des Kinderschutzes. Da bei den Fachkräften der einzelnen Institutionen im Hinblick auf die Zusammenarbeit vielfach Unsicherheit über die Möglichkeiten und Grenzen des Datenaustauschs festzustellen ist, dringen wir seit Jahren darauf, dass die Ausführungsvorschriften endlich in Kraft gesetzt werden, damit in diesem wichtigen Bereich Rechtssicherheit für die Fachkräfte in der Praxis geschaffen wird.

Ein bereits Ende 2015 zwischen uns und der Senatsverwaltung für Bildung, Jugend und Familie abgestimmter Entwurf wurde aufgrund wiederholter Interventionen der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung – insbesondere auch auf politischer Ebene – nicht umgesetzt. In der Folge musste die Praxis auch im Jahre 2017 weiterhin auf die dringend benötigten Ausführungsvorschriften warten.

Wir haben daher im Sommer dieses Jahres erneut auf die noch umzusetzenden Datenschutzanforderungen hingewiesen. Die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung hat daraufhin zugesagt, unsere Vorschläge nunmehr umzusetzen.

139 JB 2015, 6.2; JB 2016, 5.1

Im Juli 2017 hat der Bundestag in seiner letzten Sitzung der vergangenen Legislaturperiode den Entwurf eines Gesetzes zur Stärkung von Kindern und Jugendlichen (Kinder- und Jugendstärkungsgesetz – KJSG[140]) beschlossen. Mit dem Gesetz sollten u. a. Rückmeldepflichten für die Jugendhilfe in Kinderschutzfällen geregelt werden, die ihrerseits auch Auswirkungen auf die Regelungen in den o. g. Ausführungsvorschriften gehabt hätten. Zur Verabschiedung des Gesetzes wäre allerdings noch die Zustimmung des Bundesrates erforderlich gewesen. Da dieser das Gesetz jedoch – aus uns nicht bekannten Gründen – bereits zweimal von der Tagesordnung genommen hat, ist nicht mehr damit zu rechnen, dass es mehrere Monate nach der Bundestagswahl noch zu einer Verabschiedung des vom alten Bundestag beschlossenen Gesetzes kommen wird.

Mit Verabschiedung des Kinder- und Jugendstärkungsgesetzes wären einige Anpassungen bzw. Ergänzungen in den Ausführungsvorschriften vorzunehmen gewesen. Nachdem mit einer Verabschiedung dieses Gesetzes derzeit nicht mehr gerechnet werden kann, müssen die Ausführungsvorschriften unserer Einschätzung nach nun nicht mehr umfassend überarbeitet werden. Wir erwarten daher, dass die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung die angekündigten notwendigen Nachbesserungen vornimmt und die in der Praxis dringend erwarteten Vorschriften dann zügig in Kraft gesetzt werden.

## 6.2 Anforderungen an Online-Beratungsangebote



Kinder und Jugendliche wachsen heutzutage in einer vielfältigen Medienlandschaft auf. Die in der Kinder- und Jugendhilfe beratenden Institutionen und Träger stehen zunehmend vor der Herausforderung, die Kinder und Jugendlichen in ihrer digitalen Welt zu erreichen, in der die Kommunikation per E-Mail, über Apps und soziale Netzwerke erfolgt. Zunehmend spielen Online-Beratungsangebote in der Praxis eine Rolle. Die Entwicklung eines solchen Angebotes im Bereich des Kinderschutzes haben wir im Rahmen eines von der Senatsverwaltung für Bildung,

140 BR-Drs. 553/17, BT-Drs. 18/12330, 18/12730

Jugend und Familie geförderten Kooperationsprojekts mit zwei Jugendhilfeträgern intensiv datenschutzrechtlich begleitet.

Kinder und Jugendliche in Not- und Konfliktlagen haben häufig Probleme, sich in herkömmlicher Weise an Beratungsstellen zu wenden oder telefonische Beratung anzunehmen. Neben dem veränderten Kommunikationsverhalten besteht die Hemmschwelle bei der Inanspruchnahme von Hilfe auch darin, sich seinem Gegenüber mit seiner Identität zu offenbaren. Mit Online-Beratungsangeboten besteht die Chance, diese Zielgruppe niedrigschwellig zu erreichen und ihnen größtmögliche Anonymität und Vertraulichkeit zusichern zu können. Entsprechende Angebote datenschutzgerecht und vor allem technisch sicher auszugestalten, erfordert allerdings einen gewissen Aufwand bei der Entwicklung.

Bei Online-Beratungsangeboten ist zu beachten, dass bei allen Bemühungen der Betreiber, ein anonymes Angebot anzubieten, was wir in jeder Hinsicht begrüßen, echte Anonymität nur in Ausnahmefällen tatsächlich erreicht werden kann. Da bei einem Online-Angebot aus technischen Gründen zumindest temporär personenbezogene Nutzungsdaten anfallen, führt dies bereits dazu, dass das Angebot nicht mehr anonym sein kann. Dies betrifft insbesondere die sog. IP-Adresse, die den Rechner, von dem aus zugegriffen wird, und damit auch die Nutzerin bzw. den Nutzer eindeutig identifiziert. Bei einigen asynchronen Angeboten, d. h. Beratungen, die nicht in Echtzeit, wie etwa in einem Chat, erfolgen, sondern zeitverzögert, indem Nachrichten zwischen den Beteiligten ausgetauscht werden, muss ein Nutzungskonto zumindest unter einem Pseudonym angelegt werden. Häufig räumen Anbieter auch die Möglichkeit ein, eine E-Mail-Adresse anzugeben, die die Nutzerinnen und Nutzer ebenfalls eindeutig zuordnet. Nicht zuletzt kann auch nie ausgeschlossen werden, dass Beratungssuchende identifizierende Angaben machen, die einen Personenbezug herstellen lassen.

Im Ergebnis kann die überwiegende Mehrzahl der Online-Beratungsangebote nicht als anonym bezeichnet werden. Wir haben bei dem uns zur Beratung vorgelegten Angebot darauf hingewirkt, dass die personenidentifizierenden Angaben auf ein Mindestmaß beschränkt wurden. Mit den Betreibern des Angebots haben wir uns im Sinne der Transparenz gegenüber den Kindern und Jugendlichen darauf verständigt, es als „vertrauliche Beratung“ zu bezeichnen.

Bei der Inanspruchnahme der Beratungsangebote fallen meistens sehr sensible Daten an. Häufig geht es um Probleme wie familiäre Gewalt, Sucht- oder Schuldenprobleme, psychische Erkrankungen, aber auch Kindeswohlgefährdungen oder Schulprobleme. Die Sensibilität der Beratung erfordert zwingend die Garantie eines besonders hohen Schutzes dieser Daten. Dies hat zur Folge, dass die Datensicherheit der Online-Beratungsangebote einem hohen Standard entsprechen muss. Ohne an dieser Stelle zu sehr ins Detail zu gehen, müssen hierfür mindestens bestimmte Grundanforderungen erfüllt werden, die vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) definiert werden. Für Webangebote unabdingbar sind u. a. eine sichere Verschlüsselung der Datenübertragung (HTTPS) sowie der Schutz des Datenspeichers durch mehrere vorgelagerte Schutzsysteme. Ein wichtiger Aspekt ist zudem, die Daten vor dem Zugriff unberechtigter Personen zu schützen. Sollen etwa Beraterinnen und Berater über das Internet auf die Nachrichten einer Vielzahl von Ratsuchenden zugreifen können, reicht es keinesfalls aus, dass sie sich nur durch Nutzungsname und Passwort legitimieren. Erforderlich für die Legitimation sind vielmehr zwei voneinander unabhängige Faktoren. So ist neben dem Faktor „Wissen", d. h. dem Passwort, noch ein weiterer Faktor „Besitz" (z. B. eine Chipkarte) notwendig, der nicht kopiert bzw. durch Wissen ersetzt werden kann.

Vertraulichkeit kann zudem nicht sichergestellt werden, wenn unsichere Kommunikationsmittel wie E-Mail eingesetzt werden, die keine durchgehend vertrauliche, d. h. sicher verschlüsselte Datenübertragung gewährleisten. Auch die Nutzung von Messenger-Diensten ist in diesem Zusammenhang in aller Regel ausgeschlossen, da deren Anbieter – wenn auch u. U. nicht die Inhalte der Nachrichten – dennoch die Tatsache in Erfahrung bringen können, dass ein Nachrichtenaustausch zwischen einer konkreten Nutzerin bzw. einem konkreten Nutzer und einem bestimmten Beratungsangebot stattgefunden hat. Dies könnte beispielsweise zur Profilerstellung verwendet werden, wie dies zu Werbezwecken bei vielen kostenlosen Diensten mittlerweile erfolgt.

Mit der Begleitung des Projektes konnte eine datenschutzkonforme Ausgestaltung des Online-Beratungsangebots erreicht werden. Zum einen können die Kinder und Jugendlichen mit dem Angebot niedrigschwellig in ihrer digitalen Welt erreicht werden. Zum anderen werden sie transparent über die erhobenen und gespeicherten Daten informiert. Wir gehen davon aus, dass die bei der

Beratung dringend erforderliche Vertraulichkeit auch unter veränderten Kommunikationsbedingungen gewährleistet werden kann. Wir haben die Angelegenheit zum Anlass genommen, die an entsprechende Beratungsangebote zu stellenden Anforderungen in einem Merkblatt zusammenzufassen, das auch anderen Beratungsdiensten helfen kann, ihre Angebote von vornherein datenschutzgerecht zu gestalten. Das Merkblatt kann bei uns angefordert werden.

## 6.3 Ein Online-Portal für die Kita-Eigenbetriebe



Wir haben den Kita-Eigenbetrieb NordOst weiterhin bei der Einführung des Fachverfahrens KitaPortal beraten.

Das Verfahren Kita-Portal ist eine Webanwendung zur Unterstützung der Verwaltungsarbeit in den Kindertagesstätten und der Verwaltung eines Kita-Eigenbetriebs. Es soll zuerst im Kita-Eigenbetrieb NordOst mit den dazugehörigen Kitas genutzt werden.

Bereits im Jahresbericht 2015[141] sind wir auf das geplante Fachverfahren eingegangen und haben dargestellt, dass die erörterten datenschutzrechtlichen Anforderungen nicht ausreichend umgesetzt wurden. Dieser Prozess zog sich leider trotz unserer intensiven Begleitung weiter fort. Erst zum Ende des Jahres 2017 konnte ein Stand erreicht werden, der eine ordnungsgemäße und datenschutzgerechte Einführung des Verfahrens möglich macht.

Problematisch war z. B. die Festlegung von Löschfristen im Löschkonzept. Hinsichtlich der Festlegung von Löschfristen gilt generell, dass sich diese an gesetzlichen Vorgaben und an der Erforderlichkeit zu orientieren haben. Konkrete Löschfristen sind zu benennen und zu begründen. Beim Grundsatz der Erforderlichkeit geht es nicht darum, ob die Daten in der Zukunft noch praktische Bedeutung haben und die Arbeit der zuständigen Stelle noch fördern könnten. Eine Datenverarbeitung ist nur dann erforderlich, wenn sie notwendig und nicht lediglich nützlich zur Erfüllung gesetzlicher Aufgaben der verantwortlichen Stelle ist. Auch

141 JB 2015, 6.5

ist die Speicherung der Daten so zu organisieren, dass – wenn notwendig – unterschiedliche Löschfristen für verschiedene Daten zu einer Person umgesetzt werden können. Dies wurde im vorliegenden Fall erreicht, indem die Gesundheitsdaten der Kinder in einer separaten Datenbanktabelle gespeichert werden, wodurch für diese Daten eine kürzere Löschfrist realisiert werden kann.

Unterschiedliche Auffassungen bestanden bei der Festlegung identischer Zugriffsrechte für die Mitarbeiterinnen und Mitarbeiter der Geschäfts- und Bereichsleitungen auf Kinderstammdaten aller zugehörigen Kitas. Auch für Zugriffsberechtigungen gilt, dass ein Zugriff auf personenbezogene Daten nur zulässig ist, wenn dieser für die Erbringung der Aufgabe erforderlich ist. Im Rahmen dieses Verfahrens wurde eine Evaluierung vereinbart, um nachvollziehbar prüfen und feststellen zu können, ob dies der Fall ist.

Der mit der Beratung des Eigenbetriebes verbundene Aufwand ging weit über das in vergleichbaren Vorgängen übliche und vertretbare Maß hinaus. Wir erwarten, dass die Festlegungen, die im Rahmen des Verfahrens im Kita-Eigenbetrieb NordOst getroffen wurden, auf die Fachverfahren in den anderen Kita-Eigenbetrieben übertragen werden.

## 6.4 Evaluierung des Elterngeldes Plus auf unzureichender Rechtsgrundlage

Aus der Praxis

Der Gesetzgeber hat das Bundesministerium für Familie, Senioren, Frauen und Jugend verpflichtet, dem Deutschen Bundestag bis zum 31. Dezember 2017 einen Bericht über die Auswirkungen der Vorschriften zum Elterngeld Plus, zum Partnerschaftsbonus und zur Elternzeit vorzulegen. Diese Regelungen sollen Teilzeitarbeit von Eltern und die partnerschaftliche Aufgabenverteilung fördern. Eltern sollen für den durch die Teilzeitbeschäftigung entfallenden Einkommensanteil Elterngeld in Anspruch nehmen können.[142] Dieses Verfahren soll nun evaluiert werden.

142 Siehe § 4 Abs. 4 Satz 3 und § 4 Abs. 6 Satz 2 BEEG

Das Bundesministerium hat das Institut für Demoskopie in Allensbach (IfD) beauftragt, den Bericht zu erstellen. Zu diesem Zweck sollte eine Befragung der Bezieherinnen und Bezieher des Elterngeldes Plus bzw. des Partnerschaftsbonus durchgeführt werden. Das Bundesministerium hat die Bundesländer aufgefordert, die Daten der die Leistung beziehenden Eltern an das IfD zu übermitteln, um diese kontaktieren zu können.

Hierbei hat sich das Bundesministerium auf Rechtsgrundlagen gestützt, mit denen eine Datenübermittlung nicht begründet werden konnte. Zum einen kamen die zu Grunde gelegten Vorschriften des Bundesdatenschutzgesetzes für die Übermittlung von Sozialdaten von vornherein nicht in Betracht, da für die Leistungen des Bundeselterngeldes die spezialgesetzlichen Regelungen des Sozialrechts gelten. Zum anderen erwies es sich als sehr zweifelhaft, ob sich die geplante Befragung überhaupt auf die Vorschriften des Bundeselterngeld- und Elternzeitgesetzes stützen ließ. Eine Befragung der Leistungsberechtigten für die Erstellung des Berichts ist im Gesetz nicht vorgesehen. Hinzu kam, dass das Gesetz die in den Bundesländern zuständigen Behörden ohnehin zu laufenden Erhebungen über das Elterngeld verpflichtet, die dann zur Erstellung einer Bundesstatistik an das Statistische Bundesamt weiterzuleiten sind.[143] Da von dieser Regelung sowohl das Elterngeld Plus als auch der Partnerschaftsbonus erfasst werden, erschienen uns die geltend gemachten Gründe für eine darüber hinausgehende Befragung der Leistungsberechtigten sowie für eine Übermittlung ihrer Daten ohne ihre zuvor eingeholte Einwilligung als nicht plausibel. Zudem sind wir der Meinung, dass hier auch andere Ausgestaltungen des Verfahrens, z. B. durch Nutzung eines sog. Adressmittlungsverfahrens[144], durchaus in Betracht gekommen wären. Die Elterngeldstellen hätten so den betroffenen Eltern die Unterlagen für eine schriftliche Befragung zuleiten können, ohne dass deren Sozialdaten an das Forschungsinstitut hätten weitergegeben werden müssen.

143 § 22 Abs. 2 BEEG

144 Bei einem Adressmittlungsverfahren übergeben die die Befragung durchführenden Stellen nicht adressierte Briefumschläge mit dem zu versendenden Material an diejenigen Stellen, die die Adressen der Befragungsempfänger kennen (hier wären dies die Elterngeldstellen) und die Briefe dann versenden. Die Betroffenen sind auf dieses Verfahren hinzuweisen.

Vor dem Hintergrund, dass die gleichartige Problematik bereits im Jahre 2008 aufgetreten und seinerzeit intensiv mit den Datenschutzbeauftragten des Bundes und der Länder erörtert worden ist, hätte das Bundesministerium ausreichend Zeit gehabt, ein datenschutzgerechtes Verfahren zu entwickeln und auf entsprechende Gesetzesänderungen hinzuwirken.

Die für das Bundesministerium für Familie, Senioren, Frauen und Jugend zuständige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat in Aussicht gestellt, an das Bundesministerium heranzutreten und für die Zukunft auf eine entsprechende Änderung des Bundeselterngeld- und Elternzeitgesetzes hinzuwirken.

Während die Landesbeauftragten für den Datenschutz in den übrigen Bundesländern entweder überhaupt nicht oder zu spät beteiligt wurden oder teilweise der Datenübermittlung auch zugestimmt haben, haben wir der Senatsverwaltung für Bildung, Jugend und Familie empfohlen, die Daten nicht zu übermitteln. Dieser Empfehlung ist die Senatsverwaltung gefolgt. Sozialdaten von Berliner Elterngeldbezieherinnen und -beziehern wurden insoweit nicht weitergegeben. Für die Zukunft erwarten wir, dass Verfahren etabliert werden, die eine Befragung datenschutzgerecht ausgestalten.

## 6.5 Handlungsleitfaden zu Videoaufnahmen in Berliner Kindertageseinrichtungen

Gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Familie haben wir einen Handlungsleitfaden zum Umgang mit Foto-, Video- und Tonaufnahmen in Kindertageseinrichtungen erarbeitet.

In den Jahren 2014[145] und 2015[146] haben wir über ein umfangreiches und mit Bundesmitteln gefördertes Forschungsprojekt zur Sprachförderung berichtet. Im Rahmen dieses Projekts wurden zahlreiche Videoaufnahmen von Kleinkindern

145 JB 2014, 4.1
146 JB 2015, 6.4

in ihrem Kitaalltag angefertigt und schließlich durch ein Forschungsinstitut ausgewertet. Dabei stellte sich heraus, dass die verwendeten Einverständniserklärungen nicht den datenschutzrechtlichen Anforderungen genügten. Zudem ergab sich das Problem, dass zwangsläufig Videoaufnahmen auch von den pädagogischen Fachkräften angefertigt wurden. Videoaufnahmen im Beschäftigtenverhältnis unterliegen jedoch strikten Restriktionen. So sind Einwilligungserklärungen wegen des Abhängigkeitsverhältnisses zwischen Arbeitnehmern und Arbeitgebern im Hinblick auf die Freiwilligkeit problematisch.

Für das Forschungsprojekt konnte mit allen Beteiligten eine datenschutzgerechte Lösung gefunden werden. Gesichter wurden zum Teil verpixelt und es wurde auf die Nennung von Namen der Kinder und der pädagogischen Fachkräfte verzichtet.[147] Die Problematik der Anfertigung von Fotos und Videoaufnahmen in Kindertageseinrichtungen stellt sich jedoch immer wieder in unterschiedlichen Zusammenhängen. In unserer Praxis zeigt sich dies durch eine zunehmende Zahl von Eingaben von Eltern, die uns zum Umgang mit Fotos ihrer Kinder in den Einrichtungen um datenschutzrechtliche Beratung und Prüfung bitten.

Mit dem nunmehr fertiggestellten Handlungsleitfaden soll den pädagogischen Fachkräften in kurzer und verständlicher Form ein Überblick über die datenschutzrechtlichen Regelungen gegeben werden, die im pädagogischen Alltag im Umgang mit den – mittlerweile nahezu ausschließlich in digitaler Form vorhandenen Aufnahmen – einzuhalten sind. Neben den Anforderungen, die an wirksame Einwilligungen zu stellen sind, wird u. a. über die Inhalte des Rechts am eigenen Bild informiert, auf die notwendigen technischen Schutzmaßnahmen eingegangen und aufgezeigt, welche Regeln im Umgang mit Aufnahmen von Beschäftigten einzuhalten sind. Um den Handlungsleitfaden möglichst praxisorientiert zu gestalten, wurde bei der Erstellung Wert auf eine Rückkoppelung mit der Praxis gelegt.

Wir gehen davon aus, dass der Handlungsleitfadenden Berliner Kindertageseinrichtungen den praktischen Umgang mit den teilweise durchaus schwierigen Datenschutzfragen erleichtert. Der Handlungsleifaden kann bei der Senatsverwaltung für Bildung, Jugend und Familie oder bei uns angefordert werden.

147 JB 2015, 6.4

## 6.6 Datenschutz als Bildungsauftrag – Stärkung von Datenschutz- und Medienkompetenz bei Grundschulkindern

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat es sich zum Ziel gesetzt, bereits Kinder im Grundschulalter über den Umgang mit ihren eigenen Daten aufzuklären und ihnen anhand von altersgerechten Materialien einen verständlichen Einblick in das Thema zu geben.

Je früher Kinder lernen, was personenbezogene Daten sind, was sich hinter dem Begriff „Datenschutz" verbirgt und wie sie selbst Einfluss darauf nehmen können, was mit ihren Daten geschieht, desto medienkompetenter und mündiger können sie später in unserer Gesellschaft von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen.

Um das Thema Datenschutz medienpädagogisch etablieren zu können, haben wir zunächst bereits vorhandene Materialien in Theorie und Praxis ausgewertet. Die Bestandsaufnahme zeigte uns, dass großer Bedarf bei der Aufbereitung des Themas für die jüngere Altersgruppe besteht. Hier fehlt es vor allem an grundlegenden Basismaterialien.

Um die Hauptzielgruppe und die dafür vorgesehene methodische Umsetzung eingrenzen zu können, haben wir neben den aktuellen politischen Maßnahmen und Vorhaben des Landes Berlin zur Medienbildung in der Schule die aktuellen Rahmenlehrpläne für die Grundschule und entsprechende Expertisen sowie Stellungnahmen zur Medienbildung herangezogen. Da Kinder aus entwicklungspsychologischer Sichtweise bereits mit Beginn des siebten bzw. achten Lebensjahres beginnen, Perspektiven einzunehmen, Nutzen und Vorteile abzuwägen und ein kritisches Bewusstsein zu entwickeln, bietet sich die Fokussierung auf diese Altersgruppe besonders an. Zudem enthält der Lehrplan der dritten und vierten Klassen gute Anknüpfungspunkte, das Thema „Datenschutz" in den Unterricht einzubinden.

Mit der Festlegung der Kernzielgruppe der Dritt- und Viertklässler haben wir in einem ersten Schritt Figuren (konkret: eine Roboterfamilie) entwickelt, die die

Kinder „an die Hand nehmen" und durch die komplexe Welt des Datenschutzes begleiten. Mit ihrer Unterstützung werden die Lerninhalte den Kindern vermittelt und veranschaulicht.

Ergänzend haben wir für Eltern, Lehrkräfte sowie Multiplikatorinnen und Multiplikatoren auf unserer Webseite Hinweise und Listen mit weiterführenden Links sowie ein Informationsblatt mit konkreten Tipps zum Umgang mit Datenspuren zusammengestellt. Mit unserem neuen Internetangebot für Kinder[148] sollen zunächst die Figuren, ihre Fähigkeiten und Eigenschaften definiert sowie erste Begrifflichkeiten eingeführt werden. Später möchten wir die Inhalte Schritt für Schritt weiterentwickeln und kindgerecht ausbauen.

Zudem sind wir im Austausch mit ausgewählten Berliner Grundschulen und erproben Workshops und Projekte zum Thema „Datenschutz", die sich an Kinder in dritten Grundschulklassen richten. Nach der Testphase und einer anschließenden Evaluation der Praxisphase wollen wir das Angebot nachhaltig etablieren und gezielt für Grundschulen oder Jugendeinrichtungen im Rahmen von zeitlich festgelegten Projektwochen anbieten.

Im Rahmen der Vorlesungsreihe der KinderUni Lichtenberg (KUL) und der mobilen KinderUni „KUL unterwegs" haben wir auch in diesem Jahr Vorträge zu Themen wie „WhatsApp" oder Risiken bei der Nutzung von sozialen Netzwerken angeboten. Die große Nachfrage und die durchweg positive Resonanz haben uns darin bestärkt, Angebote wie diese auch im nächsten Jahr aufrechtzuerhalten.

Die Vermittlung von Medienkompetenz an Kinder und Jugendliche ist untrennbar mit der Vermittlung von Datenschutzkompetenz verbunden. Angesichts der veränderten Bedingungen einer zunehmend digitalen Welt sehen wir es als unsere Aufgabe an, die Jüngsten der Gesellschaft so früh wie möglich für einen verantwortungsvollen Umgang mit ihren persönlichen Daten zu sensibilisieren. Die ab 25. Mai 2018 wirksam werdende Datenschutz-Grundverordnung weist uns diesen Auftrag auch gesetzlich zu.[149]

148 www.data-kids.de

149 Art. 57 Abs. 1 lit. b DS-GVO

# 7 Gesundheit und Soziales

## 7.1 Verordnung über den öffentlichen Gesundheitsdienst – Licht am Ende des Tunnels?



Bereits in unserem letzten Jahresbericht haben wir berichtet, dass starker Verbesserungsbedarf beim Gesundheitsdatenschutz in der öffentlichen Verwaltung besteht.[150] Hierzu gehört, dass die für die Tätigkeit des öffentlichen Gesundheitsdienstes zwingend erforderlichen Datenverarbeitungen auf eine ausreichende rechtliche Grundlage gestellt werden müssen.

Der öffentliche Gesundheitsschutz wird in Berlin durch eine Reihe verschiedener Institutionen gewährleistet (z. B. Landesamt für Gesundheit und Soziales, Gesundheitsämter der Bezirke). Aufgaben und Struktur des Gesundheitsdienstes regelt das Gesundheitsdienst-Gesetz (GDG). Die für Gesundheit zuständige Senatsverwaltung wird dadurch ermächtigt, das Nähere über die Verarbeitung personenbezogener Daten in einer Rechtsverordnung zu regeln. Gleiches gilt für die Regelungen zur Durchführung der integrierten Gesundheits- und Sozialberichterstattung.

Konnten wir im Jahr 2015 berichten,[151] dass die Senatsverwaltung nach knapp zweijährigem Stillstand die Arbeit an dem Entwurf der Verordnung zur Regelung der Datenverarbeitung in Einrichtungen des öffentlichen Gesundheitsdienstes (DatVO) wieder aufgenommen hat, ist die Bilanz am Ende des Jahres 2017 ernüchternd. Denn erlassen ist die Verordnung noch immer nicht.

Und mehr noch: Hatten wir es 2015 noch begrüßt, dass uns die für Gesundheit zuständige Senatsverwaltung bereits frühzeitig in den Erarbeitungsprozess eingebunden hat, hat sie uns im Verlaufe des Jahres 2017 signalisiert, uns nur noch

150 JB 2016, 1.3
151 JB 2015, 8.1

im Rahmen des verwaltungsinternen Mitzeichnungsverfahrens Gelegenheit zur Stellungnahme einzuräumen.

Ungeachtet der Frage, inwieweit diese Vorgehensweise mit der im Berliner Datenschutzgesetz vorgesehenen Anhörungspflicht der Berliner Beauftragten für Datenschutz und Informationsfreiheit zu vereinbaren ist,[152] ist diese Entscheidung sicher nicht im Interesse des öffentlichen Gesundheitsdienstes, der dringend Rechtssicherheit im Umgang mit Datenschutzfragen benötigt.

Die Verordnung soll den Umgang mit sensitiven Daten der Berliner Bevölkerung regeln. Gerade für solche Regelungen hat der Gesetzgeber im Berliner Datenschutzgesetz die Pflicht zur Einbindung unserer Behörde vorgesehen. Durch unsere frühzeitige und kontinuierliche Beratung kann verhindert werden, dass sich erst nach jahrelanger Arbeit herausstellt, dass eine Verordnung mit den Regelungen des Datenschutzrechts nicht zu vereinbaren ist. Denn damit wäre niemandem geholfen.

Ende des Jahres 2017 haben wir einen überarbeiteten Entwurf der Verordnung zur Stellungnahme erhalten. Erforderliche Anpassungen aufgrund der ab 25. Mai 2018 wirksam werdenden Datenschutz-Grundverordnung waren jedoch in dieser Entwurfsversion nicht berücksichtigt. In einem gemeinsamen Gespräch mit der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung haben wir darauf gedrängt, die Schaffung von europarechtskonformen Verarbeitungsbefugnissen von der geplanten Sozial- und Gesundheitsberichterstattung abzutrennen und diese zwar parallel, aber getrennt voneinander voranzutreiben.

So zeichnete sich im vergangenen Jahr ab, dass die Regelungen zur Gesundheits- und Sozialberichterstattung besondere Probleme bereiten. Hier ist neben der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung auch die Senatsverwaltung für Integration, Arbeit und Soziales am Zug, entsprechende Vorschläge für eine datenschutzgerechte Umsetzung zu liefern.

Wir erwarten nunmehr von der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung den zügigen Erlass entsprechender Vorschriften.

152 § 24 Abs. 1 Satz 3 BlnDSG

# 7.2 Evaluation der Unabhängigen Patientenberatung Deutschland



Nachdem wir im Jahr 2016 die Unabhängige Patientenberatung Deutschland (UPD) aufgrund einer Beschwerde geprüft hatten,[153] ist diese mit der Bitte an uns herangetreten, eine von ihr beabsichtigte Evaluation datenschutzrechtlich zu begleiten.

Die UPD soll Verbraucherinnen und Verbraucher sowie Patientinnen und Patienten in gesundheitlichen und gesundheitsrechtlichen Fragen qualitätsgesichert und kostenfrei informieren und beraten. Diese Aufgaben nimmt die UPD auf drei verschiedenen Wegen wahr: Online, per Telefon und in ihren Beratungsstellen vor Ort.

Die Evaluation soll nunmehr Aufschluss über die Struktur-, Prozess- und Ergebnisqualität der UPD geben. Hierzu soll u. a. eine Befragung der Ratsuchenden mittels Fragebogen erfolgen. Die Planung und Durchführung der Evaluation übernimmt nicht die UPD selbst, sondern ein darauf spezialisiertes Unternehmen.

Bei den Planungen stellte die Befragung der zahlenmäßig größten und damit interessantesten Nutzergruppe der telefonisch Ratsuchenden eine besondere Herausforderung dar. Denn einerseits sieht das Datenschutzkonzept der UPD vor, dass die Beratung grundsätzlich anonym erfolgt. Andererseits soll den Ratsuchenden im Anschluss an die Beratung postalisch ein Fragebogen übersendet werden, für dessen Zustellung die Kenntnis des jeweiligen Namens und der Anschrift nötig ist.

Zur Lösung dieses Problems haben wir vorgeschlagen, dass entgegen der ursprünglichen Planung nicht mehr die Mitarbeiterinnen und Mitarbeiter der UPD die benötigten Daten abfragen sollten. Stattdessen könnten die Anruferinnen und Anrufer nach Abschluss der Beratung an das mit der Evaluation beauftragte Unternehmen weitergeleitet werden. Dort könnte die Erhebung der Adressdaten z. B. durch einen speziell programmierten Anrufbeantworter erfolgen. Da dieses Unternehmen keine Kenntnis vom Inhalt des vorherigen Beratungsgesprächs ha-

153 JB 2016, 6.4

ben würde und die UPD wiederum nicht auf die Adressdaten zugreifen könnte, wäre auf diese Weise die Anonymität der Beratung weiterhin gewahrt.

Auch im Rahmen der Evaluation darf die vorgesehene Anonymität der Beratung nicht konterkariert werden. Wir begrüßen es daher, dass die UPD uns von sich aus in die Planung eingebunden hat. So konnten wir Hinweise geben, wie die Untersuchung sowohl für sie als auch für die Ratsuchenden datenschutzgerecht ausgestaltet werden kann.

## 7.3 Anforderungen an die Vernichtung von Patientenakten



Von einem Bürger erfuhren wir, dass sich in der von einer Arztpraxis gemeinsam mit weiteren Parteien des Hauses genutzten Papiertonne sehr grob geschredderte Patientenakten befänden, die sich problemlos wieder zusammensetzen ließen. Es bestand daher die Gefahr, dass sowohl die Namen als auch die Diagnosen einzelner Patientinnen und Patienten ohne großen Aufwand Dritten zur Kenntnis gelangen könnten. Nachdem wir uns zunächst vor Ort von den Angaben des Bürgers überzeugt hatten, nahmen wir diesen Fund zum Anlass, die Arztpraxis ebenfalls einer Prüfung zu unterziehen. Hierbei hat sich herausgestellt, dass der eingesetzte Aktenvernichter bei weitem nicht die Anforderungen erfüllte, die an eine sichere Vernichtung von Gesundheitsdaten zu stellen sind.

Liegt es auf der Hand, dass z. B. das bloße Zerreißen der Dokumente nicht ausreicht, um zu verhindern, dass Dritte Kenntnis von sensitiven Daten nehmen, wissen viele Verantwortliche hingegen nicht, welche Anforderungen bei der Vernichtung von Patientenunterlagen konkret zu beachten sind.

Heikel ist dieses Unwissen nicht nur für die betroffenen Patientinnen und Patienten. Auch für die Ärztinnen und Ärzte selbst kann der laxe Umgang mit Patientenakten unangenehme Folgen haben. So kann die unsachgemäße Vernichtung unter Umständen dazu führen, dass die Verantwortlichen die betroffenen Patientinnen

und Patienten benachrichtigen müssen.[154] Zudem kann hierin eine Verletzung der ärztlichen Schweigepflicht liegen, die sowohl straf- als auch berufsrechtliche Folgen für die Verantwortlichen nach sich ziehen kann.[155] All dies ließe sich von vornherein durch die Verwendung eines geeigneten Aktenvernichters verhindern.

Doch worauf sollte eine Arztpraxis bei der Anschaffung eines solchen Gerätes konkret achten? Geht es um Gesundheitsdaten, scheiden einfache Aktenvernichter, die das Papier lediglich in schmale Streifen schneiden, von vornherein aus. Hier sollte auf höherwertige Geräte zurückgegriffen werden, die zusätzlich horizontale Schnitte produzieren (sog. Partikelschnitt). Doch auch hier gibt es Unterschiede. Eine gute Hilfe bietet daher ein vom Deutschen Institut für Normung e. V. (DIN) erarbeiteter Standard für die Vernichtung von Datenträgern, an der sich die Gerätehersteller regelmäßig orientieren.[156]

Diese DIN-Norm definiert insgesamt drei Schutzklassen und sieben verschiedene Sicherheitsstufen. Welcher Schutzklasse die Daten unterfallen und welche Sicherheitsstufe bei deren Vernichtung einzuhalten ist, richtet sich wiederum nach der Schutzbedürftigkeit der in Rede stehenden Daten. Geht es – wie hier – um Gesundheitsdaten, so gehen wir grundsätzlich von einem sehr hohen Schutzbedarf aus und ordnen diese Datenträger daher der Schutzklasse 3 zu. Bei deren Vernichtung halten wir es regelmäßig für notwendig, aber auch für ausreichend, wenn der Aktenvernichter die Anforderungen der Sicherheitsstufe P-5 erfüllt. Die von den Geräteherstellern in den Produktbeschreibungen regelmäßig enthaltenen Hinweise bieten hier eine einfache und handhabbare Orientierungsmöglichkeit – das weiß jetzt auch der von uns geprüfte Arzt.

Bei der Vernichtung von Patientenakten muss gewährleistet sein, dass die Daten nach dem Schreddern in ausreichender Weise unkenntlich gemacht sind. Dies ist bei Gesundheitsdaten regelmäßig dann der Fall, wenn der eingesetzte Aktenvernichter die Anforderungen der Sicherheitsstufe P-5 erfüllt.

154 § 42a BDSG

155 Die ärztliche Schweigepflicht ist in § 203 StGB und § 9 der Berufsordnung der Ärztekammer Berlin geregelt.

156 DIN 66399 „Büro- und Datentechnik – Vernichtung von Datenträgern"

# 7.4 Aktuelle Fragen zu klinischen Studien



Wir haben uns gemeinsam mit weiteren Aufsichtsbehörden aktuellen Fragestellungen aus dem Bereich klinischer Studien gewidmet. Diese betreffen beispielsweise technische Geräte, die Prüfärztinnen und -ärzten zur Verfügung gestellt werden, und den Einsatz von Webportalen. Es fand hierzu ein Austausch mit dem Bundesverband der Pharmazeutischen Industrie e. V. statt.

Prüfärztinnen und -ärzte sind im Rahmen klinischer Studien tätig, um die teilnehmenden Personen zu untersuchen und im Sinne der klinischen Prüfung zu behandeln. Im Zuge dessen erheben sie von den teilnehmenden Personen die für die Dokumentation erforderlichen Daten. Hierfür werden sie durch die Sponsoren der Studien bzw. durch von diesen beauftragte sog. Clinical Research Organisations (CRO) ausgestattet. Papierbögen werden dabei zunehmend durch technische Geräte wie Tablets abgelöst.

Mit der Verwendung dieser Geräte verlieren die Prüfärztinnen und -ärzte einen beträchtlichen Teil der Kontrolle über ihre Datenverarbeitung. Vielfach haben sie keine Möglichkeit, die Voreinstellungen der Geräte einzusehen oder zu ändern. Dazu fehlen ihnen die Administratoren-Rechte, welche sich die Sponsoren oder CRO vorbehalten. So können eingebaute Kameras ohne ihr Wissen und Wollen aktiviert werden oder die Geräte anderweitig autonom Daten erheben oder senden. Beides läuft der Schweigepflicht der Prüfärztinnen und -ärzte zuwider und ist in jedem Fall zu vermeiden.

Neben der Schweigepflicht trifft auch die Aufklärungs- und die Dokumentationspflicht die Prüfärztinnen und -ärzte persönlich. Sie können diesen Pflichten nicht nachkommen, ohne über die Einstellungen und die Funktionsweise der zum Einsatz kommenden Geräte informiert zu sein. Nur wer selbst versteht, was vor sich geht, kann auch ein transparentes Verfahren gegenüber den teilnehmenden Personen gewährleisten und über die konkreten Umstände der Studie aufklären.

Die Aufklärung bildet die Grundlage für die Rechtmäßigkeit der Studien. Nur auf dieser Grundlage können die teilnehmenden Personen wirksam darüber entscheiden, ob sie an der Studie teilnehmen möchten. Neben den medizinischen

Aspekten muss die Aufklärung auch die Datenverarbeitung erfassen, die über das für die Behandlung Notwendige hinausgeht. Welche Informationen an die CRO und den Sponsor der Studien gehen, ist dabei eine entscheidende Information. Das betrifft auch die Daten, die nicht durch die Prüfärztinnen und -ärzte selbst eingegeben, sondern durch technische Komponenten unmerklich erfasst werden.

Prüfärztinnen und -ärzte sind verantwortliche Stellen. Sie setzen Geräte im Zweifel in eigener Verantwortlichkeit ein. Es ist in diesem Fall daher grundsätzlich notwendig, dass sie die Funktionsweise des Gerätes prüfen und bestimmen können. Dies kann und muss geschehen, ohne die Integrität der zu erhebenden Forschungsdaten zu gefährden. Denn ohne diese wäre der Erfolg der Studie in Frage gestellt.

CRO und Sponsor benötigen regelmäßig zunächst keine Angaben zur Identität der an einer Studie teilnehmenden Personen. Daher sind die Daten, die an sie gehen, zuvor zu pseudonymisieren. Das bedeutet, dass die identifizierenden Angaben wie Name und Wohnort entfernt und durch eine Nummer ersetzt werden. Was bei Textinformationen einfach umzusetzen ist, lässt sich bei Audioaufzeichnungen hingegen nur schwer realisieren. Die Rohdaten dieser Aufzeichnungen werden im Weiteren nur selten benötigt. Sie haben daher bei den Prüfärztinnen und -ärzten zu verbleiben. Nur das für die Forschung relevante Extrakt darf weitergegeben werden. Gegebenenfalls kann sich auch eine Verfremdung von Stimmen vor der Übermittlung als notwendig erweisen. Die Ausgestaltung muss bei jeder Studie, die derartige Aufzeichnungen erfordert, unter Einbeziehung der Prüfärztinnen und -ärzte sorgfältig abgewogen werden.

Vielfach werden Prüfärztinnen und -ärzte auch zur Nutzung von Webportalen zur Datenerfassung im Rahmen klinischer Studien aufgefordert. Diese Portale stellen Formulare bereit, die online ausgefüllt werden. Die Inhalte werden dem Sponsor bzw. der CRO zur Verfügung gestellt. Bei dieser Datenerhebung müssen regelmäßig die Anforderungen an die Datensicherheit nach dem aktuellen Stand der Technik für hoch schutzwürdige Daten erfüllt werden. Dies gilt auch, wenn über die Webportale nur mit einer Probandennummer versehene Daten eingegeben werden, solange nicht ausgeschlossen werden kann, dass die Daten eine Identifizierung der betroffenen Personen ermöglichen. Zu den Sicherheitsmaßnahmen gehören u. a. eine Mandantentrennung (Prüfärztinnen und -ärzte können nur auf ihre

eigenen Fälle zugreifen), eine 2-Faktor-Authentifizierung, eine ausreichende Verschlüsselung der Verbindung und die Einhaltung der OWASP 10-Kriterien durch das Webportal. Für die Gestaltung des Webportals verweisen wir zusätzlich auf die Standards des Bundesamtes für Sicherheit in der Informationstechnik zur Internet-Sicherheit und hierbei insbesondere auf die Reihe zur sicheren Bereitstellung von Web-Angeboten.[157]

Des Weiteren haben wir uns mit den besonderen Anforderungen an internationale Studien beschäftigt. Den CRO und den Sponsoren ist scheinbar oft nicht bewusst, dass für die Datenübermittlung in sog. Drittstaaten (außerhalb der Europäischen Union und des Europäischen Wirtschaftsraumes) eine weitere Rechtsgrundlage erforderlich ist. Es wird regelmäßig vor allem eine Einwilligung in Betracht kommen. Bei der Planung des Prüfverfahrens muss zunächst ermittelt werden, ob eine Datenübermittlung – ggf. durch Einschaltung weiterer Dienstleister – in Drittstaaten erfolgt. In diesem Fall muss eine datenschutzrechtliche Rechtsgrundlage für diese Übermittlung gefunden werden.

## 7.5 Noch nicht im Fahrwasser: Mangelhafter Datenschutz bei der Charité besteht fort

Im Jahr 2015 hatten wir die Charité Universitätsmedizin Berlin kontrolliert und gravierende Mängel bei der Führung des Verzeichnisses der Verarbeitungstätigkeiten und der Einführung neuer Verfahren beanstandet. Im folgenden Jahr zeigten sich großflächige Defizite bei der Gewährleistung der IT-Sicherheit. Die Bemühungen der Charité um Beseitigung der Mängel haben wir im Berichtsjahr einer weiteren Kontrolle unterzogen.



Das größte Universitätsklinikum Deutschlands bekommt seine vielfältigen Datenverarbeitungen für Zwecke der Krankenbehandlung, Ausbildung und Forschung nicht in den Griff.

157 Siehe https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Web-Server/web_server_node.html

Das Klinikum ist eine dynamische Institution, in der aktiv geforscht wird und Forschungsergebnisse in die Behandlung zurückfließen. Diagnostische Verfahren werden neu eingeführt und weiterentwickelt, Kooperationen eingegangen, Forschungsprojekte auf den Weg gebracht. Bei all dem kommt Informationstechnik zum Einsatz, die immer wieder ausgebaut und umgestellt wird. Die dabei entstehenden Risiken für Patientinnen und Patienten, Beschäftigte und im Rahmen ihrer Ausbildung tätige Personen müssen bewältigt werden. Dies geht nicht ohne klare Verantwortlichkeiten, geregelte Prozesse und Kontrolle. Wir haben geprüft, welche Fortschritte die Charité bei der Bewältigung jahrelanger Defizite gemacht hat.

Unser erster Blick galt dem Stand des Verzeichnisses der Datenverarbeitungen, dem Ausgangspunkt unserer Prüfung. Dabei mussten wir feststellen, dass nach wie vor nicht alle Datenverarbeitungen eingetragen sind und technische Angaben durchweg fehlen. Bei Verfahren, die wir stichprobenartig näher unter die Lupe genommen haben, haben wir selbst in Basisangaben Lücken entdeckt. So waren bei der Beschreibung der Patientenverwaltung Datenflüsse von und zu Einrichtungen wie dem Medizinischen Dienst der Krankenkassen und den Gesundheitsämtern nicht abgebildet. Zu einigen Verarbeitungen, auch besonders gefahrenträchtigen wie der Telemedizin, waren nur Überschriften zu finden. Welche einzelnen Vorgänge sich dahinter verbergen, war nicht zu erkennen. Eine zugesagte Übersicht über die Bestandteile weit gefasster Verfahrenskategorien erhielten wir nicht. Am Ende des Jahres wurde uns ein Arbeitsplan präsentiert, der eine Vervollständigung bis zum Mai 2018 vorsieht.

Als Zweites beurteilten wir die Vorgaben für allgemein gültige technische und organisatorische Maßnahmen für den Datenschutz. Wir mussten feststellen, dass Risiken zu eng gefasst wurden und die vorgegebenen Maßnahmen selbst diese Risiken nicht ausreichend mindern. Etablierte Vorgehensweisen wurden nicht einbezogen, eine Strukturierung entsprechend gängigen Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik nicht vorgenommen. Prozesse und Verantwortlichkeiten waren unzureichend definiert. Zentrale Bereiche wie Netzwerksicherheit, Vertrauensdienste und die Sicherheit des zentralen Systems zur Verarbeitung von Daten über Patientinnen und Patienten, Beschäftigte und Unternehmensressourcen wurden nicht ausreichend betrachtet. Anschließende Stichprobenprüfungen in der für das Informationssicherheitsmanagement angelegten

Datenbank der eingesetzten IT-Geräte und Komponenten förderten ähnliche Lücken zutage.

Im nächsten Schritt wandten wir uns den Medizingeräten zu, um dort die Zuständigkeiten und Vorgaben zum Schutz der Geräte insbesondere gegen unbefugten Zugang zu Wartungsschnittstellen zu prüfen. Wir erfuhren, dass der Betrieb der Medizingeräte an die Charité Facility Management GmbH (CFM) ausgelagert worden war. Doch war diese Auslagerung nie so, wie durch das Berliner Datenschutzgesetz gefordert, vertraglich geregelt worden. Ihrerseits hatte die CFM Wartungsaufträge an die Hersteller der Geräte vergeben. Auch hier lagen keine gesetzeskonformen Verträge vor. Für die Kontrolle der Zugriffe auf die Geräte fühlten sich letztlich weder die CFM noch die Charité selbst verantwortlich. Wie überall sonst fehlten auch hier im zweiten Jahr nach der Beanstandung jegliche Sicherheitskonzepte.

Für die Erarbeitung von Teilen der Sicherheitskonzeption für die IT-Infrastruktur hatten wir einen Arbeitsplan mit verschiedenen Arbeitspaketen von der Charité erhalten, dessen Einhaltung wir prüften. Mehr als zwei Monate nach der geplanten Fertigstellung der Arbeitspakete konnte die Charité jedoch noch keine Ergebnisse vorweisen. Auch für den wichtigen Arbeitsschritt der Risikoanalyse hatte die Charité zwei Monate nach Aufnahme der Arbeit noch keine Vorgaben für die Durchführung entwickelt.

Ein weiterer geprüfter Teilbereich betraf den Einsatz veralteter Betriebssystemversionen. Schwachstellen solch veralteter Software werden durch die Hersteller nicht mehr beseitigt und können daher durch Dritte ausgenutzt werden. Wir fanden derartige veraltete Software sowohl bei Servern als auch bei Arbeitsplatzrechnern und bei Medizingeräten vor. Im Laufe des Jahres wurde nach Mitteilung der Charité die veraltete Software bei den Servern ersetzt. Viele der anderen Geräte waren hingegen weiterhin im allgemeinen Netz der Charité frei zugänglich. Wir haben die Charité aufgefordert, Geräte mit veralteten Betriebssystemversionen unverzüglich außer Dienst zu nehmen bzw. vom Netz zu isolieren. Dafür liegt nunmehr endlich ein, wenn auch weit gefasster, Zeitplan vor.

Zum anderen haben wir darauf gedrängt, dass die Charité einen abgeschirmten Bereich für alle Geräte und Rechner einrichtet, mit denen die besonders schüt-

zenswerten medizinischen Daten verarbeitet werden. Zurzeit befindet sich diese sensible Technik zusammen mit verschiedensten Geräten unbestimmten Sicherheitszustands in einem einzigen Netz. Die Charité hat uns mittlerweile zugesagt, diesem Zustand abzuhelfen, und hat ein tragfähiges Vorgehensmodell vorgelegt. Allerdings ist noch unklar, wann der Schritt vollzogen sein wird.

Schließlich haben wir uns sowohl die Personalsituation der für Datenschutz und Informationssicherheit zuständigen Bereiche als auch einen Prozess zur Steuerung der Einführung neuer IT-Verfahren angesehen.

Das für den Datenschutz zuständige Team hat im Jahresverlauf zumindest zeitweilig eine Besetzung erfahren, wie sie für den laufenden Betrieb notwendig ist. Eine stellvertretende Datenschutzbeauftragte wurde bestellt. Es bleibt dennoch zweifelhaft, ob die Kapazitäten neben dem Tagespensum auch für die Aufarbeitung der Defizite ausreichen.

Die Rolle des internen Chief Information Security Officer (CISO) ist dagegen nach wie vor unbesetzt. Dies wird nur teilweise durch die Tätigkeit eines externen CISO aufgefangen. Die gleichfalls unbesetzte Rolle eines Informationssicherheitsmanagers wird kommissarisch durch einen Abteilungsleiter des Geschäftsbereichs Informationstechnik übernommen. Ohne personelle Verstärkung durch spezifisch im Bereich der IT-Sicherheit ausgebildete und erfahrene Fachkräfte werden die klaffenden Defizite im Bereich der Informationssicherheit nicht beseitigt werden können; zugleich ist die Entstehung neuer Defizite absehbar.

Der uns vorgestellte Prozess zur Steuerung der Einführung neuer IT-Verfahren, das sog. IT-Panel, offenbarte wesentliche Schwächen. Er ermöglicht zwar, dass die Zuständigen für Datenschutz und Informationsfreiheit gehört werden. Doch stellt er nicht sicher, dass Mittel erst freigegeben werden, wenn die Unbedenklichkeit der Datenverarbeitung feststeht, die vorgeschriebene Dokumentation vorgenommen und die notwendigen risikomindernden Maßnahmen geplant wurden. Darüber hinaus erstreckt er sich nur auf einen Teil der Vorhaben und deckt die eingangs beschriebene Dynamik keineswegs vollständig ab.

Aus dieser Gesamtsicht heraus haben wir in einem Gespräch zum Abschluss des Jahres die Lage mit dem Vorstandsvorsitzenden der Charité erörtert. Leider wurde auch in diesem Gespräch ein klarer Weg aus der Krise nicht deutlich.

Für die Behebung von weitreichenden Mängeln, die bei einer Datenschutzprüfung festgestellt werden, bedarf es einer effektiven Steuerung durch die Leitung der Institution, ausreichender Ressourcen und, wo nötig, der Bereitschaft, durchgreifende organisatorische Veränderungen herbeizuführen.

## 7.6 Die Novellierung des § 203 Strafgesetzbuch – „Freie Fahrt“ für die Einbindung externer Dienstleistungsunternehmen?



Im November 2017 ist das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen in Kraft getreten.[158] Damit hat der Bundesgesetzgeber insbesondere § 203 Strafgesetzbuch (StGB) novelliert. Die Vorschrift stellt die Verletzung von Privatgeheimnissen unter Strafe.

Bisher war es schweigepflichtigen Personen (z. B. Rechtsanwältinnen und Rechtsanwälten, Ärztinnen und Ärzten) nur schwer möglich, auf die Hilfe externer Dienstleistungsunternehmen z. B. für IT-Dienstleistungen zurückzugreifen. Dies galt jedenfalls dann, wenn die Ausübung der Dienstleistung es mit sich brachte, dass die externen Personen Kenntnis von den Berufsgeheimnissen erhalten konnten. In diesem Fall bestand für die Auftraggeberinnen und Auftraggeber nicht selten das Risiko, sich strafbar zu machen.

In der Praxis war und ist die Inanspruchnahme externer Dienstleistungsunternehmen für die Verantwortlichen jedoch oft alternativlos. Denn welche Ärztin oder welcher Arzt, welche Rechtsanwältin oder welcher Rechtsanwalt ist schon in der Lage, z. B. die eigene Informationstechnik einzurichten, zu betreiben oder zu warten?

158 BGBl. I, S. 3618

Dass die Rechtslage in dieser Hinsicht unbefriedigend war, hatte schon die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) angemerkt und den Bundesgesetzgeber u. a. dazu aufgefordert, Rechtssicherheit für die Berufsgeheimnisträgerinnen und -träger zu schaffen.[159]

Abhelfen soll nun die Neuregelung im Strafgesetzbuch. Fortan dürfen die im Gesetz genannten schweigepflichtigen Personen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, ohne sich strafbar zu machen.[160] Das gilt jedenfalls, soweit die Offenbarung für die Inanspruchnahme der Tätigkeit des Dritten auch erforderlich ist.[161] Spiegelbildlich hat der Gesetzgeber die Mitwirkenden ebenfalls einer strafbewehrten Schweigepflicht unterworfen[162] und die Regelungen in der Strafprozessordnung zum Zeugnisverweigerungsrecht[163] und Beschlagnahmeverbot[164] angepasst. Zudem müssen die Berufsgeheimnisträgerinnen und -träger die mitwirkenden Personen zur Geheimhaltung verpflichten.[165]

Also „freie Fahrt" für die Einbindung externer Dienstleistungsunternehmen? So einfach ist die Angelegenheit dann doch nicht. Machen sich Berliner Ärztinnen und Ärzte bei der Inanspruchnahme externer Dienstleistungen unter den genannten Voraussetzungen zwar nicht mehr strafbar, drohen ihnen gleichwohl berufsrechtliche Konsequenzen. Denn auch in der für sie geltenden Berufsordnung ist die ärztliche Schweigepflicht ausdrücklich normiert. Dieser Berufsordnung zufolge sind sie zur Offenbarung weiterhin nur dann befugt, wenn sie von der Schweigepflicht entbunden worden sind oder eine gesetzliche Regelung die Offenbarung erlaubt.[166] Damit auch niedergelassene Ärztinnen und Ärzten z. B. risikolos ihre

159 Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. und 19. März 2015 in Wiesbaden: „Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich"

160 § 203 Abs. 3 Satz 2 StGB

161 § 203 Abs. 3 Satz 2 StGB

162 § 203 Abs. 4 Satz 1 StGB

163 § 53a StPO

164 § 97 StPO

165 § 203 Abs. 4 Satz 2 StGB

166 § 9 Abs. 2 Berufsordnung der Ärztekammer Berlin

Geräte durch Dritte administrieren und warten lassen können, muss das Berufsrecht also „nachziehen".

Zudem darf die Formulierung im Strafgesetzbuch, nach der Berufsgeheimnisträgerinnen und -träger Geheimnisse an mitwirkende Dritte offenbaren dürfen, nicht darüber hinwegtäuschen, dass nach wie vor die Regelungen des Datenschutzrechts zu beachten sind. Für die Übermittlung von (Gesundheits-)Daten ist also weiterhin eine Befugnis erforderlich (eine gesetzliche Grundlage oder eine Einwilligung) und für die Weitergabe im Rahmen eines Auftragsdatenverarbeitungsverhältnisses der Abschluss eines entsprechenden Vertrages.

Die Novellierung des § 203 StGB ermöglicht es Berufsgeheimnisträgerinnen und -trägern jedenfalls aus strafrechtlicher Sicht, unter bestimmten Voraussetzungen externe Dienstleistungen in Anspruch zu nehmen. Um einen Gleichklang zwischen Berufs- und Strafrecht zu erreichen, bedarf es jedoch zunächst einer Anpassung der Berufsordnung.

## 7.7 Verfahren der Hilfe zur Pflege mit datenschutzrechtlicher Begleitung

Durch mehrere Eingaben erfuhren wir, dass Sozialleistungsträger im Verfahren der Hilfe zur Pflege Einsicht in medizinisch-pflegerische Unterlagen genommen haben. Die Betroffenen wurden vorab nicht aufgeklärt, Einwilligungs- und Schweigepflichtentbindungserklärungen wurden nicht eingeholt.



Hilfe zur Pflege wird Personen gewährt, die pflegebedürftig sind und nicht über ausreichende eigene finanzielle Mittel für Pflegeleistungen verfügen. Um zu entscheiden, ob und in welchem Umfang Hilfe zur Pflege zu gewähren ist, benötigt der Sozialhilfeträger medizinisch-pflegerische Unterlagen der Betroffenen. Oft benötigt er auch Auskünfte behandelnder Ärztinnen und Ärzte oder auch von Pflegediensten. Zwar erhebt der Sozialhilfeträger Sozialdaten möglichst direkt bei den Hilfeempfangenden, jedoch werden häufig Informationen auch von Dritten erforderlich. Bislang gab es hierfür keine schriftliche, transparente Unterrichtung der Betroffenen im Vorfeld der Datenabfrage, zudem wurde auch keine einheitliche

Einwilligungs- und Schweigepflichtentbindungserklärung von den Betroffenen eingeholt, wenn deren Sozialdaten bei Pflegediensten bzw. Ärztinnen und Ärzten abgefragt wurden. Pflegedienste waren unsicher, ob sie die begehrten Auskünfte erteilen dürften und haben uns um Prüfung gebeten. Wir haben daraufhin die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung bei der Erstellung datenschutzgerechter Formulare beraten.

Erhebt der Sozialhilfeträger Sozialdaten direkt bei den Betroffenen, so werden diese über die Datenerhebung vorab unterrichtet. Für sie ist nun klar erkennbar, wer welche Daten zu welchem Zweck erhebt. Auch auf die Folgen fehlender Mitwirkung, die sich aus den Vorschriften des Sozialgesetzbuches zur Sozialhilfe ergeben, wird hingewiesen.

Wenn der Sozialhilfeträger die Sozialdaten bei Dritten erhebt, bedarf es der vorherigen Einwilligung. Daneben müssen die Hilfeempfängerinnen und -empfänger ihre Pflegedienste, Ärztinnen und Ärzte ausdrücklich von deren Schweigepflicht entbinden. Nur wenn eine Schweigepflichtentbindungserklärung vorliegt, dürfen Daten an den Sozialhilfeträger weitergegeben werden.

Durch die gemeinsam mit der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung entwickelten Formulare wird für die Betroffenen ein berlinweit einheitliches Verfahren geschaffen, das für die Betroffenen, aber auch für die beteiligten Pflegedienste sowie für die Ärztinnen und Ärzte mehr Rechtssicherheit schafft.

## 7.8 Anforderung von Betreuungsgutachten für die Feststellung einer Behinderung

Aus der Praxis

Durch eine Eingabe erfuhren wir, dass das Landesamt für Gesundheit und Soziales, das eine Behinderung bzw. den Grad einer Behinderung feststellt, in diesem Zusammenhang vollständige Betreuungsgutachten von den Betroffenen bzw. deren Betreuern und auch von Betreuungsgerichten eingeholt hat.

Das Vorgehen des Landesamts für Gesundheit und Soziales war unzulässig. Das Landesamt benötigt nur diejenigen Informationen, die es ihm erlauben, das Vorliegen und den Grad einer Behinderung festzustellen. Die Betroffenen dürfen alle übrigen Angaben im Betreuungsgutachten schwärzen. Das Landesamt für Gesundheit und Soziales muss die Betroffenen darauf auch hinweisen.

Mit der Anforderung der Betreuungsgutachten direkt bei den Gerichten hat das Landesamt gegen datenschutzrechtliche Grundsätze verstoßen. Sozialdaten sind direkt bei den Betroffenen zu erheben. Nur in Ausnahmefällen können Daten bei Dritten erhoben werden. Hierfür bedarf es allerdings einer gesetzlichen Grundlage.

Auf unsere Intervention hin hat das Landesamt für Gesundheit und Soziales eingeräumt, dass die Anforderung vollständiger Betreuungsgutachten nicht erforderlich sei, und hat das Verfahren vorerst ausgesetzt. Wir haben Vorgaben gemacht, wie das Verfahren in Zukunft datenschutzgerecht auszugestalten ist, und werden die Umsetzung kontrollieren.

## 7.9 Weitergabe von personenbezogenen Daten eines politisch Verfolgten an die Botschaft seines Herkunftslandes

Im Zusammenhang mit einer ordnungsbehördlichen Bestattung wurden persönliche Daten (u. a. Anschrift und Mobilnummer) eines politisch Verfolgten mit Asylstatus in Deutschland, der für die Sterbeangelegenheit durch den Verstorbenen bevollmächtigt worden war, von dem vom Bezirksamt Charlottenburg-Wilmersdorf beauftragten Bestattungsunternehmen an die Botschaft seines Herkunftslandes weitergegeben. Der Betroffene hatte bei der Organisation der Bestattung die zuständigen Behörden mehrfach darauf hingewiesen, dass er ein durch das Regime politisch Verfolgter sei und seine Daten daher schutzbedürftig seien. Trotzdem wurde er von der Botschaft unter seiner privaten Handynummer kontaktiert.

Das Bestattungsunternehmen hatte dargelegt, dass es bei einer ordnungsbehördlichen Bestattung eine ordnungsgemäße Anmeldung durchführen und eine Sterbeurkunde sowie den Bestattungsschein beantragen müsse. Dazu würden die Personenstandsurkunden (wie die Geburtsurkunde) benötigt. Da der Verstorbene aufgrund der Flucht nach Deutschland über keine Geburtsurkunde verfügte, hatte das Bestattungsunternehmen die Botschaft seines Herkunftslandes kontaktiert, um die offiziellen Dokumente zu erhalten. In diesem Zusammenhang wurde der Auftrag des Ordnungsamtes zur ordnungsbehördlichen Bestattung mitgeschickt, in dem die Daten des Bevollmächtigten ungeschwärzt vermerkt waren.

Die Nennung des Bevollmächtigten zum Erhalt der Geburtsurkunde war jedoch nicht erforderlich. Das für die ordnungsbehördliche Bestattung zuständige Bezirksamt hatte die Daten des Bevollmächtigten dem Bestattungsunternehmen lediglich zum Zwecke der Organisation der Bestattung sowie der Trauerfeier mitgeteilt. Wir haben diesen Fall daher unserer Sanktionsstelle übergeben.

Dem zuständigen Bezirksamt haben wir aufgetragen, die eigenen Beschäftigten sowie die beauftragten Bestattungsunternehmen im Hinblick auf ähnlich gelagerte, sensible Fälle besser zu schulen bzw. zu unterweisen. Das Bezirksamt sagte zu, zukünftig auf die Angaben zu den Angehörigen bzw. Bevollmächtigten zu verzichten, sofern ein atypischer Fall (z. B. bei politisch Verfolgten) vorliege.

Zur Beantragung erforderlicher Urkunden bei der jeweiligen Botschaft hat das beauftragte Bestattungsunternehmen darauf zu achten, dass nicht erforderliche Daten geschwärzt werden. Dies gilt insbesondere bei Angaben zu Angehörigen sowie bevollmächtigten Personen, wenn diese z. B. politisch verfolgt sind und hierdurch in Gefahr geraten könnten.

# 7.10 Kontrolle einer sozialen Kriseneinrichtung für Wohnungslose



Durch eine Petition wurden wir auf ein Problem aufmerksam, das auch andere soziale Einrichtungen betreffen könnte. Oft berichten wir von Gefahren, die von der Digitalisierung des Alltags in Form von Smartphones und anderen elektronischen Geräten ausgehen. Aber auch bei herkömmlichen Papierakten können datenschutzrechtliche Probleme auftreten. Im konkreten Fall ging es um die Möglichkeit der Kenntnisnahme von Schriftstücken durch hierzu nicht berechtigte Personen und damit um den Verlust der Vertraulichkeit.

Soziale Einrichtungen verarbeiten naturgemäß soziale und ggf. medizinische Daten. Diese Daten sind besonders sensibel und unterliegen einem besonderen gesetzlichen Schutz. Bei der Kontrolle einer solchen Einrichtung fanden wir Akten mit vertraulichem Inhalt in frei zugänglichen Regalen, obwohl die Einrichtung über abschließbare Schränke verfügt.

Die Konzeption des Hauses stellt die freie Bewegung der Bewohnerinnen und Bewohner innerhalb der Einrichtung in den Vordergrund. Der Zutritt zum Haus soll leicht möglich sein. Auch wenn im Haus ständig Betreuungspersonal anwesend ist, ist nicht zu verhindern, dass hierzu nicht berechtigte Personen Einsicht in diese Akten nehmen könnten. Damit ist die Vertraulichkeit dieser Unterlagen gefährdet. Das Problem bestand nunmehr darin, die offene Konzeption des Hauses und die gesetzliche Vorgabe der Vertraulichkeit von Daten in Einklang zu bringen.

Eine Lösung wäre, nur die Akten mit Personenbezug in verschließbaren Schränken zu verwahren; dies würde jedoch hohe Sorgfalt bei der Ablage der Dokumente voraussetzen. Alternativ könnten sämtliche Akten verschlossen verwahrt werden, was zwar Fehler durch falsche Sortierung ausschließen, aber zu Investitionen in zusätzliche geeignete Schränke führen würde. Da die bei der ersten Variante erforderliche Sorgfalt in einer Kriseneinrichtung nicht immer gewährleistet werden kann, empfehlen wir die Unterbringung aller Akten in verschließbaren Schränken.

Während der Kontrolle stellte sich im Übrigen heraus, dass die betriebliche Datenschutzbeauftragte zugleich Mitglied des Vorstands war und damit in einer Lei-

tungsposition. Dadurch befand sie sich in einem Rollenkonflikt, weil sie sich letztlich selbst hätte kontrollieren müssen. Mittlerweile wurde eine andere Person für dieses Amt bestellt.

Während unserer Kontrolle war das Verständnis für unsere Anliegen zunächst gering, was die grundsätzliche Bedeutung von Schulungsmaßnahmen für das Personal solcher Einrichtungen unterstreicht. Erst durch Aufklärung kann eine nachhaltige Wahrung des Datenschutzes erreicht werden. Eine wiederholte datenschutzrechtliche Schulung der Beschäftigten sollte, insbesondere in sozialen Einrichtungen, verpflichtend werden.

Auch nicht automatisiert verarbeitete Daten wie Briefe, Akten und sonstige Schriftstücke unterliegen der Vertraulichkeit. Sie sind gegen unberechtigte Kenntnisnahme zu schützen. Das Amt der oder des Datenschutzbeauftragten darf nicht auf Leitungspersonen übertragen werden.

# 8 Beschäftigtendatenschutz

## 8.1 Änderungen durch den neuen Datenschutzrechtsrahmen



Die Datenschutz-Grundverordnung (DS-GVO) beeinflusst auch das Beschäftigtendatenschutzrecht. Die nationalen Gesetzgeber haben die Möglichkeit, Regelungsspielräume und Öffnungsklauseln auszufüllen. Für Datenverarbeitungen im Beschäftigungskontext findet sich in Art. 88 DS-GVO eine Öffnungsklausel, die von den nationalen Gesetzgebern mit spezifischen nationalen Regelungen ausgefüllt werden kann.

Damit ist es auf nationaler Ebene möglich, durch ausdifferenzierte gesetzliche Regelungen ein hohes Schutzniveau im Beschäftigtendatenschutz sicherzustellen, soweit dadurch kein Widerspruch zu allgemeinen Vorgaben der Datenschutz-Grundverordnung entsteht. Durch spezifischere Rechtsvorschriften oder Kollektivvereinbarungen kann der Schutz der Rechte und Freiheiten bei der Verarbeitung personenbezogener Beschäftigtendaten besser gewährleistet werden.

Am 27. April 2017 hat der deutsche Gesetzgeber ein neues Bundesdatenschutzgesetz (BDSG-neu) beschlossen. Es wird ebenso wie die Datenschutz-Grundverordnung am 25. Mai 2018 in Kraft treten. In § 26 BDSG-neu finden sich spezifische Vorgaben zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses.

So wird geregelt, dass personenbezogene Daten vor, im und nach dem Beschäftigungsverhältnis verarbeitet werden dürfen, soweit dies zum Zwecke des Beschäftigungsverhältnisses erforderlich ist. Im Rahmen der Erforderlichkeitsprüfung sind die widerstreitenden Grundrechtspositionen abzuwägen, d. h., die Interessen der Beschäftigungsstelle an der Datenverarbeitung und das Persönlichkeitsrecht der Beschäftigten sind zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.

Im Übrigen entspricht die Vorschrift im Wesentlichen dem bisherigen (alten) § 32 BDSG.

Die Einwilligung war als Erlaubnis zur Verarbeitung persönlicher Daten im Beschäftigungsverhältnis bisher sehr umstritten, da grundsätzlich Zweifel an der Freiwilligkeit einer von den Beschäftigten erteilten Einwilligung im Hinblick auf deren soziale Abhängigkeit von der Beschäftigungsstelle bestanden. Diese Problematik wurde vom Gesetzgeber nun aufgegriffen. Danach sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere dann vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder die Beschäftigungsstelle und die beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf dabei grundsätzlich der Schriftform.

Dies gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten (also sensitive Daten – z. B. Gesundheitsdaten). Die Einwilligung muss sich jedoch immer ausdrücklich auf diese Daten beziehen. Dabei sind die neuen gesetzlichen Regelungen und Vorgaben zur Verarbeitung besonderer Kategorien personenbezogener Daten von Beschäftigten (Beurteilung der Arbeitstätigkeit) zu beachten.[167] Danach hat der Arbeitgeber angemessene und spezifische Maßnahmen (z. B. technisch-organisatorische Maßnahmen) zur Wahrung der Interessen der betroffenen Person vorzusehen.[168]

Neben der Art des verarbeiteten Datums und der Eingriffstiefe kann z. B. auch der Zeitpunkt der Einwilligungserteilung maßgebend sein. Vor Abschluss eines Arbeitsvertrages werden Bewerberinnen und Bewerber regelmäßig einer größeren Drucksituation ausgesetzt sein und damit eine Einwilligung in eine Datenverarbeitung eher erteilen. Dies ist bei der Interessenabwägung zu beachten.

Im Gesetz wird nun auch klargestellt, dass personenbezogene Daten von Beschäftigten u. a. auch verarbeitet werden dürfen, wenn dies zur Ausübung oder

167 § 22 Abs. 1b i. V. m. Abs. 2 BDSG-neu
168 § 22 Abs. 2 Nrn. 1-10 BDSG-neu

Erfüllung der sich aus Kollektivvereinbarungen (z. B. Betriebsvereinbarungen) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.[169] Im Übrigen sind die Betroffenenrechte zu Auskunft, Widerspruch, Löschung und Berichtigung zu beachten.[170]

Es bedarf jedoch trotz dieser genannten Regelungen nach Auffassung der Aufsichtsbehörden für den Datenschutz einer detaillierten bereichsspezifischen Regelung auf Grundlage der Datenschutz-Grundverordnung im Bundesdatenschutzgesetz bzw. eines eigenständigen Beschäftigtendatenschutzgesetzes.

Da die Arbeitswelt 4.0 vielfältige, insbesondere offene und verdeckte technische Überwachung möglich macht, sind angesichts der mit Digitalisierung und Globalisierung verbundenen Herausforderungen und Risiken für Arbeitnehmerinnen und Arbeitnehmer klare und spezifische gesetzliche Regelungen erforderlich. Ein angemessener Ausgleich zwischen Informationsinteressen von Arbeitgeberinnen und Arbeitgebern und dem Recht auf informationelle Selbstbestimmung der Beschäftigten kann nur durch eine differenzierte, transparente gesetzliche Regelung erreicht werden.

Der Gesetzgeber hat dies erkannt und sich selbst verpflichtet, weitere Regelungen zum Beschäftigtendatenschutz zu erlassen.[171]

Der Bundestag sollte in dieser Legislaturperiode ein Beschäftigtendatenschutzgesetz verabschieden.

169 § 26 Abs. 1 und 4 BDSG-neu
170 §§ 32 – 37 BDSG-neu
171 BT-Drs. 18/11325, S. 97

## 8.2 Weitergabe von Personaldaten – Transparenzgesetz

Aus der Praxis

Von der Senatsverwaltung für Finanzen wurden wir um Stellungnahme zu der Frage gebeten, ob die Mitglieder der Gewährträgerversammlung[172] das Recht haben, von Vorständen der Berliner Stadtreinigungsbetriebe, Berliner Verkehrsbetriebe und Berliner Wasserbetriebe Auskunft über Daten von Beschäftigten der zweiten und dritten Führungsebene zu erhalten.

Nach der Landeshaushaltsordnung Berlin (LHO) sind diese Betriebe verpflichtet, für jedes namentlich benannte Mitglied ihrer Unternehmensorgane die für die Tätigkeit im Geschäftsjahr gewährten Gesamtbezüge im Anhang zum Jahresabschluss oder an anderer geeigneter Stelle zu veröffentlichen, jeweils einzeln aufgegliedert nach festen und variablen Bestandteilen und mit Auflistung der Einzelbestandteile.[173]

Diese Vorschrift gilt jedoch nur für Mitglieder der Organe, nicht dagegen für Personaldaten von Beschäftigten der zweiten und dritten Führungsebene. Die Landeshaushaltsordnung bietet daher keine Rechtsgrundlage für eine Weitergabe der Daten an die Gewährträgerversammlung, da ihre Vorschriften insoweit nicht einschlägig sind.[174]

Bei Daten zur Vergütung und zu sonstigen Vergütungsleistungen für Beschäftigte der zweiten und dritten Führungsebene der o. g. Landesunternehmen handelt es sich um Personalaktendaten. Diese unterliegen nach dem Landesbeamtengesetz (LBG), das über das in Berlin geltende Tarifrecht[175] auch für Angestellte im öffentlichen Dienst gilt, einer gesteigerten Geheimhaltungspflicht.[176] Sie sind vertraulich zu behandeln und nur einem eng begrenzten Kreis von Beschäftigten zugänglich zu machen.

172 Etwa: haftende Eigentümerversammlung
173 § 65 d i. V. m. § 65a LHO
174 § 65 d LHO i. V. m. § 65a LHO
175 § 3 des TV-L
176 § 84 ff. LBG

Zur Weitergabe von Personalaktendaten dieser Führungskräfte an die Gewährträgerversammlung ist daher eine Einwilligung der jeweils Betroffenen erforderlich.[177] Dabei sind die Vorgaben für eine Einwilligung[178] zu beachten, wonach die Einwilligung nur wirksam ist, wenn sie auf einer freien Entscheidung beruht und insbesondere dann unwirksam ist, wenn sie durch Androhung ungesetzlicher Nachteile oder durch fehlende Aufklärung bewirkt wurde.[179]

Ohne eine Rechtsvorschrift dürfen Personal-/Personalaktendaten nur mit Einwilligung der Betroffenen übermittelt und genutzt werden.

## 8.3 Weiterleitung vertraulicher E-Mails durch die Personalabteilung an den Vorgesetzten



Eine Richterin an einem Gericht beschwerte sich über ihre Personaldezernentin. Diese hatte eine mit ihr geführte E-Mail-Korrespondenz ohne ihr Einverständnis oder ihre Kenntnis u. a. an den Vorgesetzten der Richterin weitergeleitet. In dieser Korrespondenz bezog sich die Petentin auf ein mit ihrem Vorgesetzten geführtes „Interview" anlässlich ihrer Regelbeurteilung, wobei sie sich kritisch über ihn äußerte und ihrer Befürchtung Ausdruck verlieh, dass er ihr gegenüber voreingenommen sein könne. Auch erinnerte sie an ihre Erwägungen, den Senat wegen dieser Unstimmigkeiten zu wechseln. Die Personaldezernentin begründete die Weiterleitung der E-Mails mit dem Hinweis auf ihre Aufgabe, einen „tragfähigen" Interviewvermerk erstellen zu müssen. Dazu sei die umfängliche Information und Einbindung des betreffenden Vorgesetzten maßgeblich gewesen.

Die Weiterleitung der E-Mails durch die Personaldezernentin an den Vorgesetzen der Petentin bzw. Vorsitzenden Richter stellt eine Nutzung personenbezogener Daten dar. Diese ist nur dann erforderlich und zulässig, wenn die öffentliche Stelle im konkreten Einzelfall ihre Aufgabe ohne diese Datenweitergabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und außerdem die Daten

177 Nach § 88 Abs. 2 LBG
178 Nach § 6 Abs. 3 bis 6 BlnDSG
179 § 6 Abs. 5 BlnDSG

nur in dem Umfang, wie es die Aufgabenerfüllung gerade in Bezug auf die betroffene Person zum bestehenden Zeitpunkt erfordert, verwendet werden.

Darüber hinausgehende Informationen aus dem bilateralen E-Mail-Verkehr zwischen der Beschwerdeführerin und der Personaldezernentin waren vertraulich zu behandeln. Eines ausdrücklichen Hinweises auf die Vertraulichkeit bedarf es bei der Korrespondenz und bei Gesprächen zwischen Beschäftigten und Personalverantwortlichen nicht, denn dort anfallende Personaldaten sind grundsätzlich vertraulich zu behandeln, es sei denn, die Nutzung der Daten ist erforderlich (s. o.) oder wird von einem klaren Einverständnis[180] der Betroffenen gedeckt.[181]

Die Weiterleitung der gesamten E-Mail-Korrespondenz war als Nutzung der personenbezogenen Daten weder geeignet noch für die Erfüllung der Aufgaben im Beurteilungsverfahren erforderlich und damit unzulässig.

Vor der Weiterleitung der E-Mails von Beschäftigten ist die Frage der Vertraulichkeit ihres Inhalts sorgfältig zu prüfen.

## 8.4 Weiterleitung von Gesundheitsdaten durch den DGB an das Integrationsamt

Aus der Praxis

Eine schwerbehinderte Beschäftigte des DGB hat sich mit der Beschwerde an uns gewandt, dass ihr Arbeitgeber im Rahmen eines Präventionsverfahrens sensible Personaldaten (Gesundheitsdaten, Abmahnungen und ein inzwischen aufgehobenes Urteil) an den Betriebsrat, die Schwerbehindertenvertretung und das Integrationsamt weitergegeben habe. Die Weiterleitung sei ohne ihr Einverständnis erfolgt.

Bezüglich der Nutzung der Personal- bzw. Personalaktendaten durch den Betriebsrat sind die besonderen gesetzlichen Vorgaben zu Beschäftigten im Bundesdatenschutzgesetz zu beachten. Danach dürfen personenbezogene Daten (auch

180 § 6 Abs. 3 – 6 BlnDSG
181 § 32 BDSG

Personalaktendaten) für Zwecke des Beschäftigungsverhältnisses verarbeitet und genutzt werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist.[182]

Sowohl die (aufgehobene) Gerichtsentscheidung als auch die Abmahnungen enthielten Personalaktendaten der Petentin. Diese unterliegen aufgrund ihrer Schutzwürdigkeit einer besonderen Geheimhaltungspflicht und dürfen nur einem eng begrenzten Personenkreis und auch nur im unbedingt erforderlichen Umfang zur Kenntnis gegeben werden.

Ein mittlerweile aufgehobenes Urteil ist weder für die Durchführung noch für eine mögliche Beendigung des Arbeitsverhältnisses erforderlich. Dessen Weiterleitung bzw. Nutzung war daher unzulässig.

Etwas anderes gilt dagegen für die erteilten Abmahnungen. Nach Sozialgesetzbuch IX (SGB IX) schaltet der Arbeitgeber bei Eintreten von personen-, verhaltens- oder betriebsbedingten Schwierigkeiten im Beschäftigungsverhältnis, die dessen Bestand gefährden können, möglichst frühzeitig die Schwerbehindertenvertretung und die im Sozialgesetzbuch IX genannten Vertretungen sowie das Integrationsamt ein.[183] Er soll mit ihnen alle Möglichkeiten und alle zur Verfügung stehenden Hilfen zur Beratung und mögliche finanzielle Leistungen erörtern, mit denen die Schwierigkeiten beseitigt werden können, um das Arbeits- oder sonstige Beschäftigungsverhältnis möglichst dauerhaft fortzusetzen.[184]

Im Zusammenhang mit diesem sog. Präventionsverfahren spielen bereits erteilte Abmahnungen durch den DGB an die Petentin eine wichtige Rolle, da sie konkrete Hinweise auf verhaltensbedingte Störungen des Arbeitsverhältnisses und Nachweise für bereits aufgezeigte und festgestellte Pflichtverstöße der Beschäftigten geben. Ihre Nutzung war daher erforderlich und zulässig. Da die Abmahnungen nur der Vorsitzenden des Betriebsrats und dem Vorsitzenden der Gesamtschwerbehindertenvertretung übersandt wurden, ist dem Gebot der Datensparsamkeit und der Vertraulichkeit hinreichend Rechnung getragen worden.

182 Siehe § 32 Abs. 1 BDSG
183 § 84 Abs. 1 SGB IX
184 § 93 SGB IX

Die Weiterleitung der Abmahnungen an das Integrationsamt war zur (möglichen) Beendigung des Beschäftigungsverhältnisses ebenfalls in gewissem Umfang erforderlich.[185]

Das Präventionsverfahren dient der Prüfung möglicher Mittel und Wege zur Fortsetzung eines Beschäftigungsverhältnisses.[186] Diese Prüfung ist nur dann möglich, wenn entsprechende Daten der Beschäftigten vorliegen, weil die individuellen Umstände des Einzelfalls berücksichtigt werden müssen. Da es sich beim Integrationsamt zwar um einen Beteiligten im Rahmen eines besonderen Verfahrens handelt, jedoch um eine Stelle außerhalb des DGB, ist die Weitergabe von Personalaktendaten besonders sorgfältig zu prüfen.[187] Die Tatsache, dass es in der Vergangenheit bereits zu Störungen im Beschäftigungsverhältnis gekommen war, ist im Rahmen dieser Prüfung nicht unerheblich. Ob es jedoch tunlich war, die Abmahnungen selbst in Kopie an das Integrationsamt zu versenden, bleibt dennoch fraglich. Ausreichend und vorzugswürdig wäre gewesen, dem Integrationsamt, insbesondere im Hinblick auf das Gebot der Datenvermeidung und Datensparsamkeit, in einem ersten Schritt zunächst nur eine kurze Beschreibung der konkreten Situation zu geben.[188]

Die Nutzung und Übersendung eines aufgehobenen Urteils an die Personalvertretungen und an das Integrationsamt waren nicht erforderlich und damit rechtswidrig.

## 8.5 Zugriff auf Krankenakte durch Arbeitgeber

Aus der Praxis

Eine Beschäftigte eines Unternehmens, das medizinische Geräte und Dienstleistungen für Krankenhäuser anbietet, wandte sich mit der Beschwerde an uns, ihre Vorgesetzte habe Zugriff auf ihre Krankenakte genommen, als die Petentin als Patientin in einem von ihrem Arbeitgeber betreuten Krankenhaus stationär behan-

185 § 32 Abs. 1 BDSG i. V. m. § 84 Abs. 1 SGB IX
186 § 84 Abs. 1 SGB IX
187 Siehe § 84 Abs. 1 SGB IX
188 § 3a BDSG

delt wurde. Vor der Untersuchung unterschrieb die Petentin die vom Krankenhaus zur Verfügung gestellte Patienteninformation sowie eine Einwilligungserklärung. Dadurch erklärte sich die Petentin auch mit der Einsichtnahme des mit der Abrechnung der Leistungen betrauten Personals ihres Arbeitgebers in ihre Gesundheitsdaten einverstanden.

Das Unternehmen hatte auch solchen Beschäftigten den Zugriff auf Behandlungsdaten eingeräumt, die an der jeweiligen Behandlung nicht beteiligt waren. Darüber hinaus hatte es nicht Sorge dafür getragen, dass festgestellt werden kann, wer tatsächlich in die Daten Einsicht genommen hat. So war es dem Unternehmen auf Nachfrage auch nicht möglich zu ermitteln, ob tatsächlich ein Zugriff durch die von der Petentin benannte Vorgesetzte erfolgt war. Und schließlich standen dem Arbeitgeber der Patientin über einen direkten und uneingeschränkten Zugriff auf die elektronischen Patientenakten im Krankenhaus auch noch weit mehr Informationen zur Verfügung, als er sie für die ihm übertragene Tätigkeit benötigte.

Hierdurch wurden die Rechte der Patientin in doppelter Hinsicht verletzt: Ihre Daten wurden unbefugten Personen offengelegt, zumal solchen, die in einer Position waren, die Informationen in einer für die Patientin nachteiligen Weise zu nutzen. Und zum Zweiten wurde die Patientin daran gehindert, eine solch unberechtigte Einsichtnahme festzustellen und mögliche Ansprüche auf Schadensersatz geltend zu machen.

Im gegebenen Fall konnte lediglich festgestellt werden, dass irgendeine Beschäftigte des Arbeitgebers Einsicht in die Akten der Patientin genommen hatte, aber nicht wer. Zur Begründung für den Zugriff führte das Unternehmen an, dass es infolge einer Störung der Datenübertragung eine Nacherhebung vornehmen musste.

Formal lag zwar ein Einverständnis der Petentin vor, doch war dies in zweifacher Hinsicht problematisch. Erstens war die Einwilligung Voraussetzung für eine sachgerechte Behandlung und daher nicht freiwillig. Zum anderen schloss sie eine Offenlegung an Personen ein, zu denen die Patientin in einem Abhängigkeitsverhältnis stand. Damit ist die Einwilligung unwirksam. Selbst wenn man jedoch von einer Wirksamkeit ausginge, würde sie sich nicht auf Zugriffe erstrecken, die nicht erforderlich sind. Denn die Kenntnis des Arbeitgebers von Gesundheitsdaten

seiner Beschäftigten hat sich auf das absolut Notwendige zu beschränken. Dazu gehört keinesfalls die gesamte Krankenakte. Schließlich wollte die Petentin ganz sicher nicht ihrer Vorgesetzten Einblick in ihre Krankenakte gewähren.

Es lag daher ein Datenschutzverstoß durch den Arbeitgeber der Petentin vor. Die Nutzung der Personal- bzw. Gesundheitsdaten der Petentin erfolgte entgegen den Vorgaben des Bundesdatenschutzgesetzes ohne Rechtsgrundlage.[189]

Ferner lag ein Verstoß gegen die Pflicht vor, angemessene technisch-organisatorische Maßnahmen zu ergreifen. Das Unternehmen hatte keine ausreichenden Maßnahmen getroffen, um zu gewährleisten, dass Beschäftigte nur befugt personenbezogene Daten von Patientinnen und Patienten lesen und unbefugte Einsichtnahmen namentlich festgestellt werden können.[190]

Auf unsere Intervention hin wurde die Möglichkeit des direkten Zugriffs auf die Patientenakten des Krankenhauses beendet. Die Geschäftsführung teilte zudem mit, dass das Unternehmen zukünftig ein Berechtigungskonzept im eigenen Informationssystem umsetzen werde, das Zugriffsmöglichkeiten außerhalb der zugewiesenen Aufgaben ausschließe. Jede beschäftigte Person, die einen Zugriff auf Daten benötigt, soll für diesen Zugriff eine eigene Kennung benutzen. Die Nutzung dieser Kennung muss nachvollzogen werden können.

Sind Beschäftigte zugleich Patienten von Beschäftigungsstellen, so sind beide Verhältnisse strikt voneinander zu trennen, um die Persönlichkeitsrechte der Betroffenen zu wahren.

189 § 4 Abs. 1
190 § 9 BDSG Anlage Nr. 3

# 8.6 Unberechtigte Einsichtnahme in Arbeitnehmer- und Personalvertretungsdaten



Eine Bereichsleiterin hatte bei der IT-Abteilung die Erweiterung ihrer Zugriffsrechte beantragt, um sich zur Einarbeitung einen Überblick über die relevanten Informationen ihres Fachbereichs zu verschaffen. Nach telefonischer Beantragung über die sog. IT-Hotline wurde dem Antrag ohne Einhaltung des vorgeschriebenen Verfahrens (z. B. Ausfüllung eines entsprechenden Antragsformulars) entsprochen. Da auf dem betreffenden Laufwerk auch das Verzeichnis des Personalrats des Fachbereichs gespeichert war, konnte die Bereichsleitung auch auf dieses zugreifen. Aus diesem Verzeichnis öffnete sie mindestens ein Dokument und druckte es aus. In dem betreffenden Verzeichnis waren auch die Daten der Schwerbehindertenvertretung sowie der Frauenvertretung abgelegt. Der Vorfall wurde im System zudem nicht protokolliert.

Bei Daten der Personalvertretungen[191] handelt es sich um vertrauliche Personaldaten, aber auch um sensitive Personalaktendaten. Diese dürfen für Zwecke des Beschäftigungsverhältnisses nur verwendet oder genutzt werden, wenn dies erforderlich ist. Gleiches gilt für den Umgang mit Personalaktendaten.

Im vorliegenden Fall konnte die Bereichsleiterin wegen unzulässiger Einräumung des Zugriffsrechts auf sensible Personaldaten zugreifen und diese verwenden. Die Verwendung oder Nutzung der Daten war nicht erforderlich. Sowohl die Daten des Personalrats als auch die der Schwerbehinderten- und Frauenvertretung dürfen nur für diese Gremien abrufbar sein, sofern die betreffenden Personalvertretungen einem Zugriff durch andere Stellen nicht explizit zugestimmt haben.

Im Übrigen ist allein der Umstand, dass auf dem betreffenden Laufwerk auch die Verzeichnisse des Personalrats, der Frauenvertretung und der Schwerbehindertenvertretung gespeichert waren, rechtswidrig. Denn bereits die Möglichkeit eines jederzeitigen Zugriffs auf diese Verzeichnisse war nicht vom Gesetz gedeckt.

191 § 2 Abs. 2 BlnDSG i. V. m. § 32 Abs. 1 BDSG und § 84 Abs. 1 LBG

Da der Vorfall nicht im System protokolliert wurde, kann nicht ausgeschlossen werden, dass auch auf andere Arbeitnehmerdaten, wie z. B. Angaben über mögliche Beförderungen etc., zugegriffen wurde. Insoweit lag ein erheblicher Mangel in der Datenschutzorganisation des Unternehmens vor.

Zudem war es dem IT-Mitarbeiter offensichtlich möglich, ohne Einhaltung des vorgeschriebenen Verfahrens und ohne jegliche Kontrolle den Zugriff auf sensible personenbezogene Daten einzuräumen. Demnach muss davon ausgegangen werden, dass es sich nicht um ein bloßes Mitarbeiterversehen handelte, sondern strukturelle Probleme in der Gestaltung der Datenverarbeitungssysteme vorlagen bzw. vorliegen.

Die BVG räumte sowohl eine Lücke im Genehmigungsprozess als auch mangelndes Problembewusstsein der Beteiligten ein und sicherte eine zügige Aufklärung und Behebung der Datenschutzmängel zu.

Daten der Personalvertretungen sind besonders sensibel und schützenswert. Allein die Möglichkeit des unbefugten Zugriffs auf diese Daten stellt einen erheblichen Datenschutzmangel dar. IT-Systeme sind daher stets daraufhin zu überprüfen, ob es zu solchen Datenschutzproblemen kommen kann. Die Vertraulichkeit derartiger Daten muss stets gewahrt bleiben.

# 9 Wirtschaft

## 9.1 Bankgeheimnis im Zivilprozess



Eine Kundin verklagte ihre Bank auf Rückabwicklung eines Kreditvertrages. Sie behauptete, sie sei zum Widerruf des Vertrags berechtigt, da sie ihn als Verbraucherin abgeschlossen habe und dieser aufgrund ihrer Unerfahrenheit in finanziellen Dingen unwirksam sei. Die Bank hielt dem entgegen, es liege ein Geschäfts- und kein Verbraucherkredit vor; als Geschäftsführerin einer GmbH verfüge die Kundin im Übrigen über erhebliche Erfahrungen in finanziellen Angelegenheiten. Ein Widerruf des Kreditvertrages sei somit nicht möglich. Als Anlage zu der Klageerwiderung übersandte die Bank die anlässlich des Kreditvertrags erhaltene Selbstauskunft einschließlich der eingereichten Gehaltsabrechnungen und steuerlichen Unterlagen an das Gericht. Die Kundin sieht hierin einen Verstoß gegen das Bankgeheimnis.

Banken sind ihren Kundinnen und Kunden aufgrund des Bankvertrags zur umfassenden Geheimhaltung des Geschäftsverkehrs verpflichtet. Dies ist eine besondere Ausprägung der allgemeinen Pflicht der Bank, die Vermögensinteressen der Betroffenen zu schützen.

Das Bankgeheimnis gilt jedoch im Zivilprozess nicht uneingeschränkt, vielmehr besteht in diesem Zusammenhang Raum für eine Interessenabwägung, sodass eine Weitergabe von personenbezogenen Daten durch die Bank im Einzelfall durchaus gerechtfertigt sein kann. Der Rechtsgedanke der Wahrnehmung berechtigter Interessen[192] erlaubt es einer Bank, das Bankgeheimnis zu brechen, soweit bei ihr dafür ein überwiegendes Interesse besteht. Dieses ist anzuerkennen, wenn sich eine Bank in einem Prozess nicht sachgerecht verteidigen kann, ohne ihr anvertraute Geheimnisse aufzudecken. Die Offenlegung der Information muss also erforderlich sein, damit die Bank den Prozess erfolgreich führen kann. Ist die Bank zum Bruch des Bankgeheimnisses berechtigt, ist die Übermittlung

192 § 193 StGB

der Daten an das Gericht zur Rechtsverteidigung auch datenschutzrechtlich nicht zu beanstanden.[193]

Vorliegend war die Bank grundsätzlich berechtigt, entscheidungserhebliche Unterlagen, die etwa die fehlende Verbrauchereigenschaft nachweisen, dem Gericht vorzulegen. Nach einer genauen Durchsicht aller dem Gericht zugesandten Unterlagen haben wir der Bank allerdings empfohlen, in zukünftigen Fällen noch genauer zu prüfen, in welchem Umfang eine Datenübermittlung erforderlich ist.

Soweit es zur Rechtsverteidigung erforderlich ist, darf eine Bank dem Gericht personenbezogene Daten zuleiten, die dem Bankgeheimnis unterliegen.

## 9.2 Anforderung von Steuerdaten bei einer Kreditvergabe

Aus der Praxis

Ein Kunde beantragte bei seiner Bank einen Kredit für eine Immobilie. Zur Beurteilung seiner Kreditwürdigkeit forderte die Bank neben einer SCHUFA-Auskunft diverse Unterlagen an, insbesondere den letzten Einkommenssteuerbescheid und die aktuelle Einkommenssteuererklärung. Der Petent wollte von uns wissen, ob die Bank berechtigt sei, dem Steuergeheimnis unterliegende Daten zu erheben.

Eine Bank darf einen sog. Immobiliar-Verbraucherdarlehensvertrag nur abschließen, wenn es wahrscheinlich ist, dass der Betroffene das Darlehen vertragsgemäß zurückzahlen kann.[194] Die Bank hat die Kreditwürdigkeit des Betroffenen auf der Grundlage notwendiger, ausreichender und angemessener Informationen zu Einkommen, Ausgaben sowie anderen finanziellen und wirtschaftlichen Umständen eingehend zu prüfen.[195] Bei dem Abschluss eines Kreditvertrages gehören zu den erforderlichen Daten ausreichende Bonitätsinformationen, die es dem Darlehensgeber gestatten, das Risiko des Kredits zu analysieren. Diese Daten dürfen von der Bank erhoben und verarbeitet werden.[196]

193 Siehe § 28 Abs. 1 Satz 1 Nr. 2 BDSG
194 Siehe § 505a Abs. 1 Satz 2 BGB
195 Siehe § 505b Abs. 2 Satz 1 BGB
196 Siehe § 28 Abs.1 Satz 1 Nr. 1 BDSG

Welche Unterlagen im Einzelnen von der Bank angefordert werden dürfen, ist eine Frage des Einzelfalls. Wenn die Bonität des Betroffenen bereits auf der Grundlage von Gehaltsnachweisen verifizierbar ist, ist es nicht mehr erforderlich, weitere Unterlagen wie Steuererklärungen oder Steuerbescheide anzufordern. Bestehen aber Zweifel und sind für die Feststellung der Bonität mehrere Einkommensarten relevant, dürfen Steuerdaten angefordert werden. Da gerade die Einkommensteuererklärung aber Daten enthalten kann, die für die Bank nicht relevant sind, sollte diese in gewissem Umfang Schwärzungen akzeptieren.

Soweit es zur Überprüfung der Bonität erforderlich ist, darf die Bank bei einem Immobilienkredit Steuerdaten anfordern.

## 9.3 Ohne Einsichtnahme in Online-Konto kein Kredit?



Immer mehr Finanzdienstleister wie etwa eine Online-Bank, ein Kreditportal oder ein Zwischenfinanzierer bestehender Forderungen verlangen von ihren Kundinnen und Kunden die Preisgabe ihrer Kontozugangsdaten. Anhand der Kontobewegungen der letzten 90 Tage untersuchen die Finanzdienstleister die Zahlungsfähigkeit der Betroffenen. Die Datenverarbeitung wird von einigen Finanzdienstleitern auf eine Einwilligung gestützt. Besonders problematisch erscheint, dass Kontodaten zum Teil sensitive Daten enthalten (Arztrechnung, Gewerkschaftsbeitrag), auch enthält der Kontoauszug häufig Daten Dritter (Ehefrau, Kinder).

Ursprünglich haben die Banken ihren Kundinnen und Kunden die Preisgabe der Kontozugangsdaten in ihren Allgemeinen Geschäftsbedingungen verboten. Dies ist sowohl kartellrechtlich[197] als auch nach den Vorgaben der Zweiten Zahlungsdienste-Richtlinie (PSG II)[198] nicht mehr möglich.

Von den Aufsichtsbehörden sind die verschiedenen Geschäftsmodelle noch nicht abschließend bewertet worden. Für nicht sensitive Daten gibt es bei Vorhanden-

197 Beschluss Bundeskartellamt B 4 – 71/10

198 Amtsblatt der Europäischen Union – L337/35 vom 23. Dezember 2015

sein eines Kreditausfallrisikos Rechtsvorschriften für die Kontoauswertung.[199] Diese Normen rechtfertigen aber nicht die Auswertung von sensitiven Daten oder Daten Dritter. Die Speicherung dieser Daten erscheint nur dann hinnehmbar, wenn sie von dem Unternehmen nur zwischengelagert werden und technisch sichergestellt ist, dass sie nicht ausgewertet werden und der gesamte Datensatz nach der Auswertung in einer Weise zusammengefasst wird, dass ein Personenbezug nicht mehr herstellbar ist. Das technische Verfahren müsste sicherstellen, dass die o. g. problematischen Daten keiner natürlichen Person zur Kenntnis gegeben und nach der Auswertung unverzüglich gelöscht werden. Nach der Erhebung der Kontodaten sollten die Kontozugangsdaten ebenfalls unverzüglich gelöscht werden.

Die Überprüfung der Zahlungsfähigkeit durch Zugriff auf Kontodaten ist problematisch und rechtlich noch nicht abschließend geklärt.

## 9.4 411 Numbers Limited: Keine Löschung unter dieser Adresse!

Aus der Praxis

Der Betreiber eines Online-Telefonbuchs, abrufbar unter www.411numbers.de, nutzte das Löschen von personenbezogenen Daten aus seinem Verzeichnis als Einnahmequelle. Mehrere Betroffene berichteten uns, dass sie versucht hatten, Telefon- und Adresseinträge, die über die Suchfunktion auf der Webseite abrufbar waren, löschen zu lassen. Dabei konnten sie „wählen" zwischen einer schnellen kostenpflichtigen Löschung der Daten oder einer kostenlosen Variante, die bis zu vier Wochen dauern sollte und weitere Nachweise erforderlich gemacht hätte. Für die kostenlose Variante wurde von den Betroffenen verlangt, einen Identifikationsnachweis in Form der Kopie einer Rechnung des Telefonanbieters oder Stromversorgers vorzulegen. Für die kostenpflichtige Löschung waren nach den Angaben auf der Webseite hingegen keine Nachweise der Identität erforderlich.

Mit den Datenschutzrechten der Betroffenen auf Auskunft, Berichtigung und Löschung dürfen keine Geschäfte gemacht werden. Sie dürfen nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. Wird die Löschung von per-

199 Siehe § 28 Abs. 1 Satz 1 Nr. 1, 28b BDSG

sonenbezogenen Daten davon abhängig gemacht, dass z. B. wie im vorliegenden Fall weitere Nachweise über die Identität zu erbringen sind, obwohl diese – wie auch die kostenpflichtige Variante zeigt – offensichtlich nicht erforderlich sind, oder werden sonstige Nachteile an eine kostenlose Bearbeitung geknüpft, so liegt eine unzulässige Beschränkung der Rechte vor.

Die Durchsetzung der Rechte der Betroffenen gestaltete sich im vorliegenden Fall allerdings schwierig: Auf sämtlichen 411 Numbers-Webseiten wurde als Kontakt die 411 Numbers Limited mit einer Adresse in Berlin angegeben. Da wir auf unsere schriftlichen Anfragen auf Auskunft keine Antworten erhielten, versuchten wir die Betreiberin vor Ort aufzusuchen. Leider ohne Erfolg: Die 411 Numbers Limited war unter der angegebenen Adresse weder ansässig noch fanden wir dort Geschäftsräume des Unternehmens vor. Vor Ort konnten wir allerdings feststellen, dass die 411 Numbers Limited die Dienstleistung eines Unternehmens in Anspruch genommen hatte, welches die eigene Adresse als Geschäftsadresse für andere Unternehmen zur Verfügung stellt. Der Dienstleister bietet überdies an, die Post entgegenzunehmen, zu scannen und an seine Kunden weiterzuleiten.

Das Öffnen und Digitalisieren der Briefe führte der Dienstleister als Auftragsdatenverarbeiter durch. Wir baten ihn daher um die Vorlage eines entsprechenden Vertrags. Der Dienstleister sah sich zunächst nicht verpflichtet, uns Auskunft zu erteilen, und argumentierte, dass das Datenschutzrecht nicht anwendbar sei. Wir erläuterten daraufhin, dass die Briefe der Petenten an die 411 Numbers Limited mit der Bitte um Löschung der eigenen Daten personenbezogene Daten enthalten hatten. Diese sind durch das Öffnen und Digitalisieren der Briefe auch in die Hände des Dienstleisters geraten und dürfen dort nur zum Zwecke der Erbringung der Dienstleistung verarbeitet werden. Schließlich sagte der Dienstleister zu, die Vorgaben der Auftragsdatenverarbeitung in den Dienstleistungsverträgen nachzubessern, und teilte uns mit, dass er die Post der 411 Numbers Limited an eine Adresse in Kanada weiterleite.

Wir haben die Kollegen der zuständigen kanadischen Aufsichtsbehörde, denen das Unternehmen bereits bekannt war, über unsere Fälle informiert. Die Kanadier verwiesen auf eine eigene Untersuchung der Praktiken dieser Organisation, die noch nicht abgeschlossen sei. Sie sagten zu, uns über die Ermittlungen und das Ergebnis auf dem Laufenden zu halten, so dass wir unsere Petenten informieren

können. Gleichzeitig haben wir das Bezirksamt, das für die Überwachung der Impressumspflicht zuständig ist, über den Vorgang in Kenntnis gesetzt. Zwischenzeitlich hat 411 Numbers Limited den Löschprozess jedenfalls so umgestaltet, dass die schnelle kostenpflichtige Löschung nicht mehr angeboten wird.

Es zeigt sich, dass verantwortliche Stellen sich nicht hinter ihren Dienstleistern verstecken können, wenn personenbezogene Daten verarbeitet werden. Die Vorgabe, die Verarbeitung dieser Daten vertraglich zu regeln, zwingt sie letztlich dazu, als Vertragspartner in Erscheinung zu treten.

## 9.5 Wenn Kundendaten umziehen …

Aus der Praxis

Es wandte sich eine in Berlin bekannte und populäre Autovermietung an uns. Die Geschäftsführer sahen sich aus Altersgründen gezwungen, die Autovermietung entweder zu schließen oder an ein konkurrierendes Unternehmen zu verkaufen. Es stellte sich heraus, dass der Autovermieter nur Kaufinteressenten finden konnte, wenn die Daten der Kundinnen und Kunden mit übergeben würden. Es drohten Massenentlassungen.

Bei einer Neuanmietung eines Fahrzeuges bei der Autovermietung müssen eine Vielzahl an personenbezogenen Daten[200] zeitaufwendig erhoben und in die Datenbank eingetragen werden. Das veräußernde Unternehmen wollte die Daten der Kundinnen und Kunden ursprünglich nur eingeschränkt an das erwerbende Unternehmen übergeben. Dem erwerbenden Unternehmen ging es jedoch vor allem um die vollständige Übergabe aller bereits vorhandenen Daten, um eine Neuanlegung des Datensatzes und die damit verbundene Bearbeitungszeit zu vermeiden.

Bei einer Übermittlung von Kundendaten beim Unternehmenskauf ist Vorsicht geboten.[201] Auf unsere Veranlassung hin hatte das veräußernde Unternehmen deshalb mit dem erwerbenden Unternehmen zunächst einen Auftragsdatenver-

200 Z. B. Name, Anschrift, Ausweisnummer (inkl. ausstellende Behörde und Ausstellungsdatum), Führerscheinnummer (inkl. ausstellende Behörde und Ausstellungsdatum), Geburtsdatum und -ort, Sperrvermerke und Historie der Mietverträge

201 Siehe JB 2016, 8.5

arbeitungsvertrag zur Verwaltung der Kundendaten[202] streng nach Weisung durch das veräußernde Unternehmen geschlossen. Sollten Altkundinnen und Altkunden einen neuen Mietvertrag bei dem erwerbenden Unternehmen unterzeichnen wollen, müssen sie unter Angabe ihres Namens, ihrer Anschrift und ihres Geburtsjahres (um die Kundinnen und Kunden in der Datenbank aufzufinden) zunächst eine Einwilligungserklärung zur Übermittlung der weiteren Daten an das erwerbende Unternehmen unterzeichnen. Wird diese Einwilligung erteilt, erhält der Datensatz einen Zeitstempel zur Dokumentation. Ab diesem Moment werden alle Daten freigeschaltet und der komplette Datensatz der Altkundschaft geht an das erwerbende Unternehmen zur eigenen Speicherung und Nutzung über.

In dem Vertrag mit dem erwerbenden Unternehmen, welches die Daten „treuhänderisch" speichert, wurde zudem eine Vertragsstrafe festgesetzt, damit das erwerbende Unternehmen die Daten nicht abredewidrig für eigene Zwecke nutzt, sofern eine Einwilligung der Kundinnen bzw. der Kunden nicht erteilt wurde. Auf dieses Verfahren ließ sich das erwerbende Unternehmen ein, sodass der Geschäftsbetrieb wie gewohnt – nun durch das erwerbende Unternehmen – fortgesetzt werden konnte.

Zudem wurden die Genehmigungen der Beschäftigten zur Übermittlung ihrer Daten an das erwerbende Unternehmen eingeholt, sodass alle Arbeitsplätze erhalten werden konnten.

Es ist erfreulich, dass unsere Empfehlungen beim Unternehmensverkauf dazu beigetragen haben, dass Arbeitsplätze in Berlin erhalten blieben.

202 § 11 BDSG

## 9.6 Lange Speicherdauer bei Online-Essenslieferdienst

Aus der Praxis

Es erreichten uns einige Beschwerden von Bürgerinnen und Bürgern, die von einem Online-Essenslieferdienst Gutscheine per E-Mail erhalten hatten. Die Betroffenen konnten sich jedoch nicht daran erinnern, dort jemals etwas bestellt zu haben.

Durch eine Datenauskunft konnten die Betroffenen in Erfahrung bringen, dass die Daten im Zusammenhang mit Essensbestellungen gespeichert wurden, die bis zu zehn Jahre zurücklagen.

Die Bestellungen waren ursprünglich zum Teil bei einem anderen Lieferdienst aufgegeben worden. Die dabei gespeicherten Daten wurden dann im Zuge einer Rechtsnachfolge an die jetzige GmbH übertragen. Eine genaue Aufklärung war aufgrund des Zeitablaufs durch den Lieferdienst nicht mehr möglich. Generell war festzustellen, dass die Daten zu lange aufbewahrt wurden. Denn es besteht eine Pflicht zur Löschung von Daten, wenn diese für die Erfüllung des jeweiligen Speicherzwecks nicht mehr erforderlich sind.[203] Der Lieferdienst hat bei inaktiven Kundenkonten in seinem Löschkonzept eine Löschung der Daten nach maximal drei Jahren vorgesehen, was auch schon eine eher zu lange Speicherdauer darstellt. Selbst diese Löschvorgabe hat das Unternehmen jedoch nicht umgesetzt.

Unsere Sanktionsstelle wird daher ein Ordnungswidrigkeitenverfahren wegen unbefugter Speicherung personenbezogener Daten einleiten.

Hinzu kommt, dass der Lieferdienst für die von Betroffenen gewünschte Löschung der Daten einen Identitätsnachweis verlangt hat. Diese Anforderung war jedoch nicht zulässig, weil die Übermittlung der Ausweiskopien für die Löschung nicht erforderlich war – insbesondere vor dem Hintergrund, dass z. B. für die Registrierung, welche bei Missbrauch mehr Schaden verursachen kann, eine Identifizierung nicht vorgenommen wird. Der Lieferdienst folgte unserer Empfehlung und verzichtet zukünftig auf die Anforderung einer Kopie des Personalausweises.

203 Siehe § 35 Abs. 2 Satz 1 Nr. 3 BDSG

Personenbezogene Daten dürfen nicht unbegrenzt gespeichert werden. Es müssen daher Löschroutinen implementiert werden. Bei Nichteinhaltung der Löschfristen drohen Strafen.

## 9.7 Datenschutz auf zwei Rädern



Neben Leihfahrrädern und -autos erfreuen sich anmietbare E-Roller immer größerer Beliebtheit. Für die Verifizierung der Anmeldung sollte per Videochat über die App der Personalausweis oder der Führerschein vorgezeigt werden.

Da es unzulässig ist, Fahrzeuge Personen zu überlassen, die keine entsprechende Fahrerlaubnis haben,[204] muss das Vorliegen der Fahrerlaubnis vorher geprüft werden. Um die Identität der Mietinteressentinnen und -interessenten zu überprüfen, setzt der Anbieter ein foto-basiertes Verfahren ein. Über die App werden die an der Anmietung interessierten Personen aufgefordert, ihren Personalausweis und ihren Führerschein zu fotografieren. Zudem müssen sie ein Foto von sich selbst mit den Dokumenten machen, damit überprüft werden kann, ob ihnen die vorgezeigten Dokumente gehören. Diese Dokumente müssen dann im Rahmen der Anmeldung hochgeladen werden.

Bei diesem Verfahren sind vor allem die Vorgaben des Personalausweisgesetzes[205] zu beachten. Insbesondere ist eine Einwilligung der Ausweisinhaberin oder des Ausweisinhabers erforderlich, wenn durch die Ablichtung, wozu auch ein Scan zählt,[206] personenbezogene Daten erhoben oder verarbeitet werden.

Darüber hinaus dürfen nur diejenigen Daten erhoben, verarbeitet und genutzt werden, die für die Begründung, Durchführung oder Beendigung eines Rechtsgeschäfts erforderlich sind.[207] Hier war festzustellen, dass einige Angaben wie die Personalausweisnummer, die Körpergröße oder die Augenfarbe für den Zweck

204 Siehe § 21 Abs. 2 StVG

205 § 20 Abs. 2 PAuswG

206 Siehe Gesetzesbegründung zum Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises, BT-Drs. 18/11279, S. 27

207 § 28 Abs. 1 Satz 1 Nr. 1 BDSG

der Identifizierung der anfragenden Person und damit für die Vertragsdurchführung nicht erforderlich sind und eine Mitteilungspflicht gegenüber dem Anbieter daher nicht besteht. Der Einwilligungsvorbehalt zugunsten der Ausweisinhaberin bzw. des Ausweisinhabers beinhaltet daher auch das Recht, diejenigen personenbezogenen Daten unkenntlich zu machen (z. B. zu schwärzen), die die betreffende Person nicht preisgeben will.[208] Der Anbieter des Leihdienstes hatte bisher im Registrierungsprozess nicht vorgesehen, die Interessentinnen und Interessenten auf die Möglichkeit der Schwärzung hinzuweisen. Er sagte uns nunmehr zu, einen entsprechenden Hinweis im Registrierungsprozess und in die Datenschutzerklärung aufzunehmen.

Nicht alle Daten auf Ausweisdokumenten sind bei der Identifizierung erforderlich. Daher ist auf die Schwärzung von nicht erforderlichen Daten bereits im Registrierungsvorgang transparent hinzuweisen.

## 9.8 Werbe-E-Mails – Was kann ich tun?

Aus der Praxis

Wir bekommen täglich mehrere Anfragen zum Thema unerlaubte 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“.

Grundsätzlich ist die Verarbeitung personenbezogener Daten – z. B. die E-Mail-Adresse – nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder die Adressatin oder der Adressat der E-Mail in die Verarbeitung eingewilligt hat, hier also vor der Zusendung von Werbe-E-Mails ihre oder seine Zustimmung gegeben hat.[209] Hierbei darf das Einverständnis nicht im „Kleingedruckten“ – z. B. in den AGB – versteckt werden.

208 Siehe Gesetzesbegründung zum Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises, BT-Drs. 18/11279, S. 28

209 § 4 Abs. 1 BDSG

Die Einwilligung muss bestimmten Formvorschriften entsprechen.[210] Oft mangelt es insbesondere an der Freiwilligkeit. Teilweise fordern wir das Unternehmen auf, die Einwilligung auf der Webseite so umzugestalten, dass Nutzende diese freiwillig abgeben können, beispielsweise durch ein nicht voreingestelltes Markierungsfeld. Auch darf die Erbringung einer Dienstleistung in der Regel nicht an die Einwilligung in den Erhalt von Werbung gekoppelt werden.[211] Zudem muss es sich um eine informierte Einwilligung handeln, d. h. Nutzungszweck und eine eventuelle Weitergabe an Dritte müssen verständlich dargelegt sein. Eine unbeschränkte Einwilligung in die Zusendung von E-Mail-Werbung ohne enge Themenbegrenzung wie z. B. Produktkategorien und Beschränkung des Absenderkreises wäre unzulässig. Eine Verbindung mit anderen Erklärungen, wie z. B. die Zustimmung zu den AGB oder zur Datenschutzerklärung, wäre ebenso unzulässig, wenn hierdurch die Freiwilligkeit der Einwilligung eingeschränkt würde. Im Zweifelsfall muss der Versender der Werbe-E-Mail die Einwilligung des Empfängers nachweisen können, was meist nur bei Verwendung des sog. „Double-Opt-In"-Verfahrens möglich ist. Hierbei erhält die Empfängerin oder der Empfänger zunächst eine E-Mail mit einem Aktivierungslink. Nur wenn anschließend dieser Link bestätigt wird und dies revisionssicher protokolliert wird, ist die ausdrückliche Zustimmung erteilt und die E-Mail-Adresse darf bis zu einem Widerspruch für Werbe-E-Mails verwendet werden.

Zudem fordern wir betroffene Unternehmen im Beschwerdefall auf, die jeweiligen Daten im Einzelfall endgültig aus den Werbe- oder Newsletter-Verteilern zu löschen und die Adresse in eine Sperrliste aufzunehmen.

Verbraucherinnen und Verbraucher können folgende Maßnahmen ergreifen, um von lästigen Webe-E-Mails verschont zu bleiben bzw. um der Flut von Werbe-E-Mails wieder zu entkommen:

- Vorsicht beim Bestellvorgang im Internet. Eventuell erlaubt eine bereits vorab mit Zustimmungshäkchen versehene Einwilligungserklärung die Zusendung von Werbe-E-Mails.

210 Eine wirksame Einwilligung setzt eine freiwillige Erklärung voraus, die unmissverständlich und in Kenntnis des Verwendungszwecks der Daten zum Ausdruck gebracht wird.

211 § 28 Abs. 3b Satz 1 BDSG

- Prüfen Sie, ob ein günstig erscheinendes Angebot an die Preisgabe Ihrer personenbezogenen Daten gebunden ist und ob es Ihnen das wert ist. Insbesondere kostenlose Gewinnspiele fallen hier regelmäßig negativ auf.

- Antworten Sie nicht auf Ihnen unbekannte Spam-E-Mails. Oft werden in Werbe-E-Mails E-Mail-Adressen angegeben, an die ein Widerspruch gerichtet werden kann. Auch kann ein Link existieren, durch dessen Anklicken z. B. ein Abmelden von einem Newsletter möglich ist. Meist handelt es sich jedoch nur um einen Trick, um die E-Mail-Adresse zu verifizieren, d. h. durch das Anklicken kann festgestellt werden, dass es sich hier um eine „echte" E-Mail-Adresse handelt, die dann z. B. für Werbe-E-Mails missbraucht werden kann.

- Sowohl E-Mail-Programme als auch der E-Mail-Provider können Filterfunktionen bereitstellen, die bei entsprechender Einstellung das E-Mail-Postfach vor unerwünschten Werbe-E-Mails schützen.

- Richten Sie ggf. spezielle E-Mail-Adressen ein oder nutzen Sie Wegwerf-E-Mail-Adressen[212], wenn Sie nicht sicher sind, dass es sich um ein seriöses Angebot handelt, bei welchem Sie die jeweilige E-Mail-Adresse angeben.

- Sollten Sie bereits E-Mail-Werbung erhalten, so können Sie einen Widerspruch an das Unternehmen senden. Der Widerspruch kann jederzeit abgeschickt werden, es gibt keine Fristen. Sie sollten das Unternehmen darauf hinweisen, dass dieses unaufgefordert und unverlangt Werbe-E-Mails versendet. Hinzufügen sollten Sie einen Hinweis, dass diese E-Mails eine Belästigung darstellen. Folgende Angaben sollte das Widerspruchsschreiben enthalten:
  - Absenderadresse bzw. die betroffene E-Mail-Adresse
  - Adresse des Unternehmens
  - Überschrift mit dem Titel Werbewiderspruch bzw. Widerspruch
  - Im Text sollten Sie der Verarbeitung oder Nutzung Ihrer Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung gegenüber allen pri-

212 Über Wegwerf-E-Mail-Dienste wie trashmail.com erzeugte Adressen leiten E-Mails nur kurze Zeit an die eigene E-Mail-Adresse weiter. Gewöhnliche Webmail-Dienste bieten zudem meist die Möglichkeit, weitere E-Mail-Adressen (sog. „Alias-Adressen") einzurichten und jederzeit wieder zu löschen, wenn zu viele Spam-E-Mails empfangen werden.

vaten Stellen, die Ihre Daten gespeichert haben, nach § 28 Abs. 4 BDSG widersprechen.

- Aufforderung zur Unterlassung weiterer unaufgeforderter Zusendungen.

- Sollte der Widerspruch beim Unternehmen nicht zum Erfolg führen, können Sie die zuständige Aufsichtsbehörde für den Datenschutz im jeweiligen Bundesland unterrichten. Welches die zuständige Aufsichtsbehörde ist, ergibt sich aus dem Sitz des Unternehmens. Die jeweilige Aufsichtsbehörde kann ggf. rechtliche Schritte einleiten bis hin zur Verhängung von Bußgeldern.

Gegen die Zusendung unerwünschter Werbe-E-Mails gibt es Mittel und Wege. Sollte der Widerspruch durch die oder den Betroffenen nicht zum Erfolg führen, so kann die zuständige Aufsichtsbehörde eingeschaltet werden.

## 9.9 Eintreibung von Rundfunkgebühren durch ein beauftragtes Unternehmen

Wir prüften von Amts wegen die Datensicherheit bei der Creditreform Mainz[213], die als Auftragnehmer für den Rundfunk Berlin-Brandenburg für den Beitragsservice eingesetzt wird.

Die Creditreform Mainz Alberts & Naujoks KG ist durch die Landesrundfunkanstalten als Verwaltungshelfer beauftragt, rückständige Rundfunkgebühren gegenüber den Rundfunkteilnehmern geltend zu machen. Die Verträge sind jeweils mit den einzelnen Rundfunkanstalten geschlossen worden. Die Gebühreneinzugszentrale (heute: Beitragsservice) beauftragt die Creditreform Mainz Alberts & Naujoks KG im Auftrag der Landesrundfunkanstalten mit der Bearbeitung offener Rundfunkgebührenforderungen, wenn die zuständige Vollstreckungsbehörde des jeweiligen Bundeslandes die ausstehende Forderung nicht beitreiben kann und eine Pfändung erfolglos verläuft. Dabei sollen in Abstimmung mit den Rundfunkteilnehmerinnen und -teilnehmern Möglichkeiten für die Begleichung der offe-

213 Die Unternehmensgruppe Creditreform agiert als Wirtschaftsauskunftei und Inkassodienstleister.

nen Rechnungen ermittelt werden. Dies erfolgt für einen zeitlich eingeschränkten Zeitraum.

Gegenstand unserer Kontrolle war die Überprüfung der Einhaltung der Vorschriften zur Datensicherheit. Die Kontrolle wurde zusammen mit den Aufsichtsbehörden für den Datenschutz in Hessen, Bremen und Brandenburg durchgeführt.

Trotz mehrfacher Aufforderung standen anfangs keine Unterlagen in ausreichender Qualität zur Verfügung. Da wir jedoch Anstrengungen für die Gewährleistung der Vertraulichkeit und Integrität der Daten erkennen konnten, haben wir bei zwei Vorortterminen die Gegebenheiten geprüft und im direkten Gespräch den Verantwortlichen der Creditreform Mainz die Anforderungen an den Nachweis der Informationssicherheit erläutert. Die bereitgestellten Dokumente wurden von uns bewertet und wir konnten erreichen, dass sie stufenweise näher an die datenschutzrechtlichen und sicherheitstechnischen Anforderungen herangeführt wurden. Hinsichtlich weiterhin bestehender problematischer Aspekte haben wir die Intendanzen der Rundfunkanstalten zur Abhilfe aufgefordert.

Die Intendanz des Rundfunk Berlin-Brandenburg teilte im Nachgang mit, dass diverse notwendige Sicherheitsmaßnahmen bereits umgesetzt worden seien und die weitere Umsetzung bis spätestens August 2018 erfolgen solle. Wir werden diesen Zeitpunkt zum Anlass nehmen, den aktuellen Stand der Informationssicherheit und ggf. weitere Bereiche zu überprüfen.

Wenn Aufgaben der öffentlichen Verwaltung an private Unternehmen ausgelagert werden, muss die Sicherheit der Daten in gleichem Maße wie bei den Auftraggebern selbst gewährleistet sein.

## 9.10 Start-up-Sprechstunde: Erster Erfahrungsbericht

Im März 2017 ging unsere Sprechstunde für Start-ups an den Start. Seitdem bieten wir Berliner Start-ups jeden ersten und dritten Mittwoch im Monat in der Zeit zwischen 14:00 und 16:00 Uhr die Möglichkeit, sich bei uns beraten zu lassen.

Der Zuspruch war enorm: Unsere Sprechstunden waren überwiegend ausgebucht, sodass wir in der zweiten Jahreshälfte dazu übergehen mussten, die Sprechzeiten pro Start-up auf 30-45 Minuten zu begrenzen, um allen Ratsuchenden die Möglichkeit für eine Erörterung ihrer Belange zu ermöglichen.

Viele Beratungsanfragen drehten sich um die anstehende Reform des Datenschutzes durch die europäische Datenschutz-Grundverordnung. Auch Fragen zur internen Organisation des Datenschutzes, zur Bestellung von Datenschutzbeauftragten und zur Erstellung von Datenschutzinformationen wurden häufig thematisiert.

Vielfach kamen die Ratsuchenden allerdings auch mit konkreten Problemstellungen. Ein wiederkehrendes Thema ist die Verwertung von personenbezogenen Daten zu einem anderen als dem ursprünglichen Zweck, insbesondere zur Optimierung der eigenen Dienste. Eine ebenfalls häufig diskutierte Frage war, ob die Start-ups personenbezogene Daten als Auftragsdatenverarbeiter oder aber als verantwortliche Stelle verarbeiten. Hieran schlossen sich häufig Folgefragen an, die z. B. mit der Verarbeitung von Daten zu eigenen Zwecken zu tun hatten, die bei der Auftragsdatenverarbeitung ausgeschlossen ist. Darüber hinaus war die Frage, ab wann Daten als anonym gelten und welche Verfahren eine Anonymisierung von Daten sicherstellen, ein bestimmendes Thema in den Sprechstunden. Häufig spielte auch die Verarbeitung von besonderen Arten personenbezogener Daten, insbesondere Gesundheitsdaten, eine Rolle.

Die Start-ups kamen aus den verschiedensten Branchen, z. B. aus dem Bereich der Wohnungsverwaltung, der Pflege, der Reisevermittlung, der Bewerbungsplattformen, um nur einige zu nennen. Aber auch klassische Tech-Start-ups waren unter den Ratsuchenden.

Die Erfahrungen aus der Sprechstunde zeigen, wie viel Beratungsbedarf bei kleinen und mittelständischen Unternehmen gegeben ist, insbesondere im Hinblick auf die Datenschutz-Grundverordnung. Dabei war für uns eindrucksvoll, das jedenfalls bei den Start-ups, die den Weg in unsere Sprechstunde gefunden haben, eine hohe Sensibilität für Datenschutzfragen und eine große Bereitschaft besteht, die rechtlichen Vorgaben umzusetzen.

# 10 Politische Parteien und Gesellschaft

## 10.1 Wahlkampf auf die smarte Art

Aus der Praxis

Im Bundestagswahlkampf haben die politischen Parteien versucht, ihr Marketing durch moderne Technik zu optimieren. Auch die traditionelle Art des Haustürwahlkampfs wurde „smart" modernisiert. Vorreiter war hier die CDU mit der Smartphone-App „connect17 – Die Unterstützer". Die App dient vor allem als elektronisches Werkzeug der Wahlkampfhelferinnen und -helfer zur Protokollierung von Wählerdaten und ermöglicht den Aufbau einer gebietsbezogenen Datenbank. In dieser wird systematisch erfasst, welche Zustimmungsrate die CDU in einzelnen Stadtgebieten erzielt. Auf Basis der gesammelten Informationen kann eine Mobilisierung potenzieller Wählerinnen und Wähler effektiver gestaltet werden. Um die Motivation der Wahlkampfhelferinnen und -helfer zu steigern, werden ihre App-Eingaben mit Punkten bewertet und in einer internen connect17-Rangliste veröffentlicht („sog. Gamification"[214]).

Wir haben geprüft, ob der Einsatz der App datenschutzkonform ist. Problematisch war die Einwilligungserklärung. So wurden Wahlkampfhelferinnen und Wahlkampfhelfer nicht ausreichend darüber aufgeklärt, dass bei ihrer Registrierung über Facebook („Facebook-connect") die App personenbezogene Daten (die Tatsache der Registrierung) an Facebook übermittelt. Die Nutzung der App von connect17 offenbart damit, dass die Betroffenen offenbar politisch der Partei der CDU nahestehen. Damit werden also Informationen preisgegeben, die Rückschlüsse auf die politische Meinung der Betroffenen zulassen, bei der es sich um

214 Als Gamification (von engl. game für „Spiel") bezeichnet man den Einsatz von spieletypischen Elementen zur Motivationssteigerung und Verhaltensänderung bei Anwenderinnen und Anwendern.

ein sensitives Datum handelt, das unter besonderem Schutz steht.[215] Soweit derartige sensitive Daten erhoben, verarbeitet oder genutzt werden, muss sich eine Einwilligung auch ausdrücklich auf diese Daten beziehen.[216] Dies war hier nicht der Fall, weshalb die Einwilligung zur Datenübermittlung unwirksam war.

Die Wahlkampfhelferinnen und -helfer werden auch nicht ausreichend darüber aufgeklärt, dass – einmal registriert – ihr Nutzungsprofil (Nutzungsname und Punktestand) in dem für alle Nutzerinnen und Nutzer einsehbaren Unterstützer-Ranking angezeigt wird. Auch insofern ist die Einwilligungserklärung mangels ausdrücklichem Hinweis auf die Veröffentlichung der sensitiven Daten unwirksam.[217] Verstärkt wird die Problematik noch dadurch, dass ein nachträglicher Widerspruch gegen die Veröffentlichung im Ranking ebenfalls nicht möglich ist.

Darüber hinaus bestehen aber auch datenschutzrechtliche Probleme hinsichtlich der Speicherung von Daten der befragten Bürgerinnen und Bürger. Die App sieht vor, dass nach einem Gespräch mit Bürgerinnen und Bürgern an der Haustür Daten in ein App-Formular eingegeben werden. Dabei werden Geschlecht und Alter gespeichert (Schätzung in 10er Schritten), außerdem wird festgehalten, ob die Haustür geöffnet wurde und wie die Meinung der Person zur Partei zu bewerten ist (durch die Smileys „positiv" „neutral", „negativ"). Über eine Google-Funktion werden die GPS-basierten Standortdaten zu Straße und PLZ automatisch in das Eingabeformular übermittelt. Um sicherzustellen, dass im Zusammenhang mit der Speicherung zeitlicher Sequenzen (Zeitstempel) kein Personenbezug hergestellt wird, haben wir veranlasst, dass die App keine konkreten Zeitangaben, sondern nur die Angabe „valid"/„invalid" (übliche/unübliche Zeit) speichert. In Gebieten, wo mangels unzureichender Möglichkeiten der Anonymisierung die Gefahr eines Personenbezugs bestehen blieb, also beispielsweise bei Straßen mit geringer Häuseranzahl und wenigen Anwohnern, haben wir darauf hingewirkt, dass die dort erfassten Daten noch vor einer Auswertung gelöscht wurden.

215 § 3 Abs. 9 BDSG definiert sensitive Daten als besondere Arten personenbezogener Daten, die Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben enthalten.

216 § 4a Abs. 3 BDSG

217 §§ 4a Abs. 1 i. V. m. Abs. 3 BDSG

Auch andere politische Parteien haben derartige Apps im Bundestagswahlkampf 2017 eingesetzt. Nach unseren Recherchen waren diese im Hinblick auf den Umfang der Datenverarbeitungen jedoch nicht mit connect17 vergleichbar. Gleichwohl werden wir die Fortentwicklung bei den „smarten Helfern" und deren Einsatz im Blick behalten.

Parteien müssen sich vergegenwärtigen, dass die von ihnen verarbeiteten personenbezogenen Daten in der Regel Rückschlüsse auf politische Meinungen zulassen. Diese sensitiven Daten dürfen grundsätzlich nur mit Einwilligung verarbeitet werden.

## 10.2 Mit Kinderfotos Wahlkampf machen



Im Rahmen einer im Jahr 2015 in einer Grundschule in Berlin-Mitte stattfindenden Veranstaltung ließ sich ein Abgeordneter von Bündnis 90/Die Grünen mit Schulkindern ablichten. Zuvor hatte der Politiker die Eltern in einem Brief an die Schule darüber informiert, dass er die Fotos nur im Kontext seiner Teilnahme an der Veranstaltung, z. B. in seinem Newsletter, veröffentlichen wolle.

Im Bundestagswahlkampf 2017 verwandte Bündnis 90/Die Grünen eines der 2015 in der Schule aufgenommenen Fotos für einen Postwurf-Flyer. Dieser wurde an Haushalte im Bezirk Berlin-Mitte und an diversen öffentlichen Orten verteilt. Mehrere Eltern der abgebildeten Schüler haben sich hierüber beschwert. Man habe sie zu keinem Zeitpunkt darüber informiert, dass die Partei das Foto auch für Wahlwerbung verwenden wolle.

Die Zulässigkeit der Fotonutzung steht infrage, da jedenfalls für eine Verwendung im Wahlkampf keine Einwilligung[218] der Eltern vorlag und dies auch nicht durch eine sonstige Rechtgrundlage erlaubt war.[219] Die Überprüfung ist bei uns noch nicht abgeschlossen.

218 Siehe § 4a Abs. 1 i. V. m. Abs. 3 BDSG
219 §§ 22, 23 KunstUrhG

Nicht nur Parteien sollten nicht zu sorglos mit derartigen Fotos und damit mit dem Persönlichkeitsrecht von Kindern umgehen, weil durch einen solchen Umgang nicht zuletzt auch Vertrauen zerstört wird.

Wer mit Kinderfotos Wahlkampf macht, sollte über eine wirksame Einwilligung der Erziehungsberechtigten verfügen.

# 11 Aus der Arbeit der Sanktionsstelle

## 11.1 Bußgeldverfahren

Wir haben 16 Buß- und Verwarnungsgelder in Höhe von insgesamt 10.350,00 Euro festgesetzt. In 24 Fällen haben wir einen Strafantrag gestellt.

In einigen Fällen beschäftigte sich die Sanktionsstelle mit dem Thema GPS-Sender.[220] Diese Fälle bekommen wir meist von der Polizei übermittelt, an die sich Betroffene wenden, wenn sie solche Ortungssysteme an ihren Fahrzeugen entdeckt haben.[221]

Klassische Fallkonstellationen sind die Überwachung durch die Beschäftigungsstelle, z. B. zur Kontrolle von Fehlzeiten, oder durch nahestehende Personen, etwa aus Eifersucht oder im Zusammenhang mit Familienstreitigkeiten. In Beschäftigungsverhältnissen ist der Einsatz von GPS-Geräten nur in Ausnahmefällen zulässig.[222] Grundsätzlich kann der Einsatz solcher Geräte ohne Kenntnis der Betroffenen sogar eine Straftrat darstellen.

Der Tatnachweis ist in den meisten Fällen jedoch schwer zu erbringen. Häufig mangelt es sowohl an einer der Tat verdächtigen Person als auch an konkreten Anhaltspunkten dafür, dass diese (unbekannte) Person sich zielgerichtet Standort- bzw. Bewegungsdaten einer anderen Person über einen bestimmten Zeitraum verschafft und dabei in eigen- oder fremdnütziger Bereicherungsabsicht gehandelt hat. Dementsprechend gering sind die Aussichten, eine solche Tat erfolgreich zu ahnden. Leider mussten wir einige Verfahren deshalb auch abschließen, ohne die Täterin oder den Täter ermittelt zu haben.

220 Globales Positionsbestimmungssystem; siehe z. B. unten Ziff. 11.2.2
221 Siehe 11.2.2
222 JB 2015, 9.4

Wir beobachten das erhöhte Anzeigeaufkommen im Bereich unbefugter GPS-Ortung mit Sorge und werden nachgewiesene Verstöße in diesem Zusammenhang auch künftig konsequent mit empfindlichen Bußgeldern ahnden bzw. die strafrechtliche Verfolgung beantragen.

### 11.1.1 Nachbarschaftliches Ausspähen



Gegen zwei Mieterinnen haben wir Bescheide über Bußgelder in vierstelliger Höhe erlassen, weil sie im Zuge eines Nachbarschaftsstreits unbefugt Videoaufnahmen von der Terrasse ihrer Nachbarn erstellt und daraus generiertes Bildmaterial an den Hausverwalter übermittelt hatten.[223]

Die Beschuldigten hatten ihren Nachbarn vorgeworfen, entgegen gesetzlicher Bestimmungen Füchse zu füttern und dadurch vermehrt wilde Tiere auf das gemeinsam bewohnte Grundstück zu locken. Um diesen Vorwurf gegenüber der gemeinsamen Hausverwaltung zu bekräftigen, hatten sie die Terrasse ihrer Nachbarn mit einer Videokamera überwacht. Einige Ausschnitte dieser Aufzeichnungen, auf denen die Terrasse sowie Menschen – augenscheinlich bei der Fuchsfütterung – erkennbar waren, schickten sie an die Hausverwaltung.

Ob und inwieweit die gefilmten Nachbarn tatsächlich in unzulässiger Weise wilde Tiere gefüttert hatten, spielte für die datenschutzrechtliche Bewertung dieses Sachverhalts keine Rolle. Die Terrasse gehört zum Wohnraum und damit zum ganz persönlichen Lebensbereich der Betroffenen. Dieser Raum ist besonders schützenswert, weshalb eine Überwachung durch die Nachbarinnen mittels Kamera auch dann nicht gerechtfertigt wäre, wenn eine verbotene Wildfütterung tatsächlich stattgefunden hätte.[224] Entgegen der Auffassung des Verteidigers der Beschuldigten lag auch kein rechtfertigender Notstand[225] vor, der das Filmen der Terrasse gerechtfertigt hätte. Denn die dafür erforderliche gegenwärtige Gefahr war durch die vermeintliche Fuchsfütterung nicht gegeben. Das Land Berlin informiert Bürgerinnen und Bürger auf den Seiten der Senatsverwaltung für Umwelt,

223 § 43 Abs. 2 Nr. 1 BDSG
224 § 28 Abs. 1 Nr. 2 BDSG, § 28 Abs. 2 Nr. 2b BDSG
225 § 34 StGB

Verkehr und Klimaschutz zum Thema Füchse und stuft dort die Gefahren durch Tollwut oder Fuchsbandwurm als unwahrscheinlich und sehr gering ein.[226] Darüber hinaus wären die Erstellung des Videomaterials und deren Übermittlung an die Hausverwaltung nicht das geeignete Mittel gewesen, um eine potenzielle Gefahr zu beheben. Stattdessen hätten sich die Beschuldigten unverzüglich an die zuständigen Behörden wenden können.

Die Mieterinnen haben Einspruch gegen unsere Bußgeldbescheide eingelegt. In einem ersten Verfahren wurde eine der Mieterinnen vom Amtsgericht verurteilt. Das zweite Verfahren wurde aus Ermessensgründen eingestellt.

Ohne Einwilligung der Betroffenen ist es auch dann nicht zulässig, Grundstücke und zur Wohnung gehörende Bereiche der Nachbarinnen und Nachbarn zu filmen, wenn diese sich dort rechtswidrig verhalten.

## 11.1.2 Unerwünschte Kooperation mit dem Jobcenter



Ein Bußgeld in vierstelliger Höhe setzten wir gegen eine Genossenschaft fest, deren Vorstandsvorsitzender die Unterlagen eines Bewerbers, der sich initiativ bei der Genossenschaft um eine Stelle beworben hatte, unbefugt an das Jobcenter Reinickendorf weitergeleitet hat.[227]

Der Vorstandsvorsitzende war aufgrund des Inhalts der Bewerbung zu der Auffassung gelangt, der Bewerber sei an einer Stelle gar nicht interessiert, sondern wolle sich mit einer Scheinbewerbung lediglich einen „Stempel" für das Jobcenter abholen. Diese Auffassung begründete der Vorsitzende in seiner E-Mail an das Jobcenter u. a. damit, dass der Bewerber eine Lesebestätigung für seine Bewerbung angefordert hatte und sich eigens für Bewerbungen eine E-Mail-Adresse eingerichtet und diese als Kontaktadresse in den Bewerbungsunterlagen angegeben hatte. Unter den Bewerbungsunterlagen befanden sich neben einem Lebenslauf mit Lichtbild auch diverse Zeugniskopien des Bewerbers. All diese Unterla-

226 Siehe http://www.stadtentwicklung.berlin.de/forsten/wildtiere/de/fuchs.shtml
227 § 47 Abs. 2 Satz 1 OWiG

gen wurden ohne das Einverständnis und ohne Kenntnis des Bewerbers an das Jobcenter weitergeleitet.

Tatsächlich bezog der geschädigte Bewerber keine Geldleistungen vom Jobcenter und hatte diese auch nicht beantragt. Dessen ungeachtet wäre eine Übermittlung der Daten durch die Genossenschaft aber auch dann nicht gerechtfertigt gewesen, wenn der Bewerber tatsächlich Leistungen nach dem Sozialgesetzbuch bezogen hätte. Denn personenbezogene Daten aus Bewerbungsunterlagen dürfen grundsätzlich nur für die Entscheidung über das Zustandekommen eines Beschäftigungsverhältnisses verarbeitet und genutzt werden.[228]

Die Genossenschaft äußerte sich im Rahmen des Bußgeldverfahrens nicht zu den Vorwürfen. Gegen unseren Bußgeldbescheid legte sie Einspruch ein, sodass wir den Vorgang zur Entscheidung an das Amtsgericht Tiergarten abgegeben haben.

Bewerbungsunterlagen enthalten detaillierte Informationen über Bewerberinnen und Bewerber. Sie dürfen ohne deren Zustimmung grundsätzlich nicht an Dritte weitergegeben werden.

## 11.2 Strafanträge

Verstöße gegen materielle Bußgeldvorschriften des Bundesdatenschutzgesetzes können auch Straftaten darstellen, wenn sie gegen Entgelt oder mit einer Bereicherungs- oder Schädigungsabsicht begangen wurden.[229] Eine Schädigung muss nicht zwangsläufig finanzieller Natur sein. Auch immaterielle Schädigungen wie etwa eine Ehrverletzung oder eine Bloßstellung können einen datenschutzrechtlichen Verstoß strafrechtlich relevant machen.

Auch das Berliner Datenschutzgesetz (BlnDSG) enthält Strafvorschriften.[230] Davon sind Mitarbeiterinnen und Mitarbeiter des öffentlichen Dienstes betroffen, die im

228 Siehe § 32 Abs. 1 BDSG
229 § 43 Abs. 2 i. V. m. § 44 BDSG
230 § 32 Abs. 1 BlnDSG

Rahmen ihrer dienstlichen Tätigkeit z. B. unbefugt auf Daten zugreifen oder diese an Dritte weitergeben.

Bei den datenschutzrechtlichen Straftatbeständen handelt es sich um sog. Antragsdelikte, d. h. diese werden nur dann strafrechtlich verfolgt, wenn die Geschädigten oder dazu berechtigte Behörden einen entsprechenden Antrag stellen. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit ist strafantragsberechtigt und kann auch gegen den Willen der Geschädigten von Amts wegen Strafanträge bei den Strafverfolgungsbehörden stellen, wenn sie Kenntnis von Verstößen erlangt und ein öffentliches Interesse an der strafrechtlichen Verfolgung bejaht.

### 11.2.1 Rache kann strafbar sein



Gegen einen Nutzer der Online-Plattform eBay Kleinanzeigen stellten wir Strafantrag, weil er aus Rache Daten einer anderen Nutzerin auf der Plattform veröffentlicht hatte.[231]

Der Beschuldigte hatte zuvor Konzertkarten in der Rubrik „zu verschenken" bei eBay angeboten. Die Anzeigeerstatterin hatte auf diese Annonce hin ihr Interesse an den Karten bekundet und sie sich zurücklegen lassen, es dann jedoch versäumt, sich erneut zu melden und die Karten abzuholen. Daraufhin hatte der Anbieter der Konzertkarten ihr mehrfach erbost geschrieben und indirekt mit Rache gedroht.

An einem der nachfolgenden Tage erhielt die Geschädigte ca. 200 Anrufe von Personen, die Interesse an einem zu verschenkenden iPhone 6 hatten. Sie stellte fest, dass der Nutzer, dessen Konzertkarten sie zuvor nicht abgeholt hatte, eine Kleinanzeige mit dem Titel „iPhone 6 zu verschenken" auf der Plattform geschaltet und darin ihren Vor- und Zunamen sowie ihre Handynummer angegeben hatte. Diese Daten waren öffentlich abrufbar und wurden erst auf die Beschwerde der Geschädigten hin vom eBay-Kundendienst gelöscht.

231 § 43 Abs. 2 Nr. 1 i. V. m. § 44 Abs. 1 BDSG

Da in diesem Fall unzweifelhaft war, dass der Täter in der Absicht gehandelt hatte, die Betroffene zu schädigen, haben wir bei der Staatsanwaltschaft Berlin einen Antrag auf Strafverfolgung gestellt.

Wer aus Rachegefühlen nicht allgemein zugängliche personenbezogene Daten einer anderen Person im Internet oder auf sonstige Weise veröffentlicht, kann sich strafbar machen. Dabei muss es sich nicht um intime Informationen handeln. Auch einfache Kontaktdaten dürfen nicht unbefugt veröffentlicht werden.

## 11.2.2 Vertrauen ist gut, Kontrolle nicht immer



Gegen eine unbekannte Person haben wir Strafantrag bei der Staatsanwaltschaft Berlin gestellt, weil sie einen GPS-Sender an dem PKW des Anzeigeerstatters befestigt und über einen unbekannten Zeitraum dessen Bewegungsdaten erhoben und verarbeitet hat.

Der Anzeigeerstatter war von seiner Autowerkstatt darüber informiert worden, dass bei einer Inspektion an der Unterseite seines Autos ein magnetisch befestigter GPS-Sender entdeckt worden war. Aufgrund der Beschriftung des Geräts lag der Verdacht nahe, dass das befestigte GPS-Gerät einem gewerblichen Dienstleister, z. B. einer Detektei, gehört. Zunächst hatte der Anzeigeerstatter keine Idee, wer ein Interesse daran haben könnte, ihn auszuspähen. Einige Tage nach Anzeigeerstattung wandte er sich jedoch erneut an die Polizei und legte ein Schreiben seiner Krankenversicherung vor, in dem ihm sein Krankentagegeldtarif als Teil einer Krankheitskostenvollversicherung außerordentlich gekündigt wurde. Zur Begründung wurde angeführt, die Versicherung habe aus „zuverlässiger Quelle" erfahren, dass der Anzeigeerstatter – im Widerspruch zu einer ärztlich attestierten Arbeitsunfähigkeit und dem in diesem Zusammenhang beanspruchten Krankentagegeld – seiner beruflichen Tätigkeit als selbstständiger Kaufmann nachgehe.

Da konkrete Anhaltspunkte dafür gegeben waren, dass eine Detektei das GPS-Gerät gegen Entgelt für das Versicherungsunternehmen an dem Fahrzeug befestigt hatte, war eine Bereicherungsabsicht durch die potenziellen Täter zu bejahen. Wir haben deshalb einen Strafantrag gestellt.

Das Anbringen von GPS-Technik an einem Fahrzeug, um unbefugt personenbezogene und nicht allgemein zugängliche Daten zu erheben, ist nach einer Entscheidung des Bundesgerichtshofs aus dem Jahr 2013 grundsätzlich strafbar.[232] Ausnahmen sind danach nur in notwehrähnlichen Situationen denkbar, die im vorliegenden Fall nicht erkennbar waren.

## 11.2.3 Auch Familienangehörige haben ein Recht auf Privatsphäre



Gegen einen Polizeibeamten haben wir Strafantrag gestellt, weil dieser ohne dienstliche Veranlassung Daten über Personen aus seinem Familien- und Bekanntenkreis aus den polizeilichen Informationssystemen erhoben hatte.

Die Polizei hatte uns über den Vorfall informiert, der dort durch die Anzeige des Schwiegersohns des Beschuldigten bekannt geworden war. Dieser hatte bei der Internetwache der Polizei angefragt, ob es erlaubt sei, ohne Grund Anfragen zu Personen in den Polizeisystemen zu stellen, wie es sein Schwiegervater regelmäßig tue. Aufgrund dieses Hinweises wurde durch die interne Revision der Polizei eine Protokolldatenauswertung veranlasst. Dabei stellte sich heraus, dass der beschuldigte Polizist in einem Zeitraum von zwei Jahren in mindestens 84 Fällen personenbezogene Daten aus den polizeilichen Informationssystemen abgerufen hatte, ohne dass eine dienstliche Notwendigkeit vorlag. Die geschädigten Personen stammten zum Großteil aus dem Familien- und Bekanntenkreis des Beschuldigten. Neben Daten über seinen Schwiegersohn hatte er z. B. auch Daten über seine Tochter, seine Ehefrau sowie über seine Nachbarn abgefragt.

Da der Beschuldigte sich zu den Vorwürfen nicht geäußert hat, konnte seine Motivation für diese Straftaten nicht abschließend ermittelt werden. Wir nehmen an, dass er in den meisten Fällen aus reiner Neugierde gehandelt hat. Gleichwohl bejahten wir das öffentliche Interesse an einer Strafverfolgung allein aufgrund der hohen Anzahl der unbefugten Datenabrufe, die erkennen ließ, dass es dem Beschuldigten offenbar gänzlich an Unrechtsbewusstsein mangelte.

232 BGH, Urteil vom 4. Juni 2013 – 1 StR 32/13

Bedienstete der Polizei werden in regelmäßigen Abständen über datenschutzrechtliche Vorschriften informiert. Per Geschäftsanweisung ist es ihnen ausdrücklich untersagt, Daten aus POLIKS und anderen polizeilichen Informationssystemen für private Zwecke oder aus privatem Interesse abzurufen. Tun sie es dennoch, kann das nicht nur disziplinarrechtliche Konsequenzen haben, sondern muss auch strafrechtlich verfolgt werden.

# 12 Informationspflicht bei Datenlecks

Wir erhielten insgesamt 53 Mitteilungen zu Datenlecks[233], also zu Fällen, in denen personenbezogene Daten von datenverarbeitenden Stellen unplanmäßig an Unberechtigte gelangt sind. In 46 Fällen handelte es sich um Meldungen aus dem nicht öffentlichen Bereich. In den übrigen sieben Fällen haben uns öffentliche Stellen über einen Datenvorfall informiert.

## 12.1 Probleme im Schulbereich

Aus der Praxis

Mehrere Meldungen betrafen Datendiebstähle nach Einbrüchen in öffentlichen Schulen. In einer Grundschule wurde in die Büros und in das Lehrerzimmer eingebrochen. Es wurde vermutet, dass dabei personenbezogene Daten von Schülerinnen und Schülern in Papierform entwendet bzw. abfotografiert wurden. Es handelte sich um Namen, Anschriften und Geburtsdaten der Kinder. Auch konnten Zeugnisse und Gesprächsnotizen, Protokolle oder Briefe entwendet worden sein. An einem Gymnasium wurde bei einem Einbruch die Schulverwaltungsfestplatte gestohlen. Dort waren alle von der Schule verwalteten Daten sowohl des pädagogischen Personals als auch der Schülerinnen und Schüler sowie deren Eltern gespeichert. Es handelte sich um die Namen, Adressen, Telefonnummern, aber auch um Zensuren und um Vermerke über die Teilnahme am Religionsunterricht oder am Lernmittelfonds.

Das Berliner Datenschutzgesetz normiert eine Informationspflicht für alle öffentlichen Stellen des Landes Berlin bei unrechtmäßiger Kenntniserlangung durch Dritte.[234] Wird demnach einer datenverarbeitenden Stelle bekannt, dass bei ihr

233 § 42a BDSG, § 18a BlnDSG
234 § 18a BlnDSG

gespeicherte personenbezogene Daten unrechtmäßig übermittelt wurden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, so hat sie dies unverzüglich den Betroffenen und unserer Behörde mitzuteilen. Diese Pflichten haben beide Schulen erfüllt. Die Grundschule hat angekündigt, für die Aufbewahrung von personenbezogenen Daten künftig einen abgeschlossenen Stahlschrank in einem separaten Raum mit Spezialschlüsseln zu verwenden. Dem Gymnasium haben wir mitgeteilt, dass den Betroffenen auch noch die konkreten personenbezogenen Daten benannt werden müssen, die mit der Festplatte abhandengekommen sind. Für die Zukunft haben wir empfohlen, neben der vom Gymnasium in Aussicht gestellten Datenverschlüsselung auch die Festplatte selbst zu verschlüsseln.



Von einer Schule außerhalb Berlins erhielten wir den Hinweis auf einen sicherheitskritischen Vorfall bei der Nutzung der Schulsoftware „DAVINCI". Infolge einer Sicherheitslücke soll es möglich gewesen sein, personenbezogene Daten der Schülerinnen und Schüler sowie des Lehrpersonals mit Namen sowie Angaben zu den Unterrichtsfächern, Unterrichtszeiten und Stundenausfällen aufgrund von Krankheit schulübergreifend einzusehen. Da das entwickelnde Unternehmen seinen Sitz in Berlin hat, haben wir es um Auskunft gebeten, ob und wie die Sicherheitslücke geschlossen wurde, welche Schulen in Berlin von der Schutzlücke betroffen sein könnten und ob das Unternehmen diese Schulen informiert hat oder dies beabsichtigt.

Das Unternehmen teilte uns die Namen von sieben betroffenen öffentlichen und privaten Schulen in Berlin mit. Wir haben darauf gedrungen, dass mit einem Software-Update zusätzliche sicherheitsrelevante Maßnahmen implementiert wurden. Dazu gehörte der komplette Verzicht auf schülerrelevante Daten wie Schüler-IDs. Den betroffenen Schulen wurde mit der Empfehlung, das neue Update einzuspielen, eine Handlungsanweisung zur Behebung der Schwachstelle des DAVINCI-Infoservers geschickt. Keine der sieben Einrichtungen hat uns über die Möglichkeit der unrechtmäßigen Kenntniserlangung von Daten durch Dritte informiert.

In Schulen werden über Jahre, oft über ein ganzes Schulleben hinweg, personenbezogene, auch sensible Daten von Schülerinnen und Schülern sowie des Lehrpersonals verarbeitet. Jede Einrichtung ist gehalten, technische bzw. or-

ganisatorische Sicherheitsvorkehrungen zu treffen, um unberechtigte Zugriffe auf die Daten – nicht nur im Fall eines Diebstahls – zu vermeiden. Sollte es dennoch dazu kommen, empfehlen wir unsere Hinweise zur Informationspflicht bei Datenlecks im öffentlichen Bereich.[235]

## 12.2 Probleme im Gesundheitsbereich



Auch in diesem Jahr erhielten wir Meldungen über Fälle, in denen Patientendaten Dritten unrechtmäßig zur Kenntnis gelangt sind. In einem Fall wurden nicht ordnungsgemäß geschredderte Patientenunterlagen von einem Arzt im Hausmüll entsorgt. In einem anderen Fall hat ein Arzt die Praxis aufgegeben und die Patientenunterlagen in Säcken verstaut im Keller zurückgelassen. In einem weiteren Fall meldete uns eine Psychotherapeutin den Diebstahl ihres Praxislaptops. Schließlich informierte uns ein Krankenhaus darüber, dass einem Mitglied der Schwerbehindertenvertretung die Aktentasche mit Unterlagen über zu betreuende Beschäftigte aus dem Pkw gestohlen wurde.

In allen diesen Fällen konnten besonders geschützte personenbezogene Daten[236], nämlich Gesundheitsdaten, Dritten unrechtmäßig zur Kenntnis gelangen. Die betroffenen Patientinnen und Patienten wurden von der jeweiligen verantwortlichen Stelle über das Datenleck ebenso informiert wie unsere Behörde.[237] Lediglich im Hinblick auf die im Keller zurückgelassenen Patientenunterlagen konnten wir die Informationspflicht gegenüber dem verantwortlichen Arzt nicht durchsetzen, weil sein Aufenthaltsort nicht ermittelbar war.

Wer beruflich mit Patientendaten umgeht, sollte sich ständig vor Augen führen, dass es sich um sensitive Daten handelt, die vor einer unbefugten Kenntnis-

235 FAQs zur Informationspflicht bei unrechtmäßiger Kenntniserlangung von Dritten nach § 18a BlnDSG, Stand: August 2017, abrufbar unter www.datenschutz-berlin.de/meldung-datenleck.html

236 Dazu zählen nach § 3 Abs. 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

237 § 42a Satz 1 Nr. 1 und 2 BDSG

nahme durch Dritte besonders zu schützen sind. Deshalb sollte es selbstverständlich sein, dass Patientenunterlagen nicht über das Fahrtende hinaus im Auto gelassen, nicht mehr benötigte Daten fachgerecht entsorgt und Festplatten von mobilen Geräten wie Laptops verschlüsselt werden. Im (zu vermeidenden) Ernstfall sollten unsere Hinweise zur Informationspflicht bei Datenlecks im nichtöffentlichen Bereich beachtet werden.[238]

238 FAQs zur Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a BDSG, Stand: August 2017, abrufbar unter www.datenschutz-berlin.de/meldung-datenleck.html

# 13 Telekommunikation und Medien

## 13.1 Nachbar-Netzwerk

Aus der Praxis

Bei nebenan.de handelt es sich um ein Online-Portal, das in Nachbarschaft wohnenden Personen ermöglicht, sich miteinander virtuell zu verschiedenen Zwecken (Information, gegenseitige Hilfe, Kontaktaufnahme etc.) auszutauschen. Wir erhielten eine Beschwerde zu dem Nachbarschaftsnetzwerk, da die Nutzerinnen und Nutzer aufgefordert wurden, zur Überprüfung ihrer Anmeldung die abgelichtete Personalausweisrückseite bzw. ein offizielles Schreiben mit Namen und Anschrift (z. B. eine Rechnung) hochzuladen.

Eine neue Online-„Nachbarschaft" wird im Regelfall nicht durch das Unternehmen selbst, sondern durch registrierte Nutzerinnen oder Nutzer ins Leben gerufen. Für die Initiatorin oder den Initiator erstellt und verteilt das Unternehmen entsprechende Einladungsschreiben in Papierform. Durch den im Briefkasten befindlichen Handzettel werden die Anwohnerinnen und Anwohner über die Gründung und das Zugangspasswort zur neuen Gruppe informiert. Anders als bei sozialen Netzwerken üblich ist hier eine Beteiligung nur für Personen möglich, die in einem durch das Unternehmen geografisch abgesteckten Gebiet wohnen. Die Erfüllung der Teilnahmevoraussetzungen und ihre Identität können sie durch verschiedene Arten verifizieren.

Das Hochladen von offiziellen Dokumenten wie beispielsweise Rechnungen birgt die Gefahr, dass nicht erforderliche Informationen erfasst werden.[239] Die Betreiber waren auf unseren Hinweis hin unmittelbar bereit, die Informationen für die Nutzerinnen und Nutzer zu ergänzen und darauf hinzuwirken, dass nicht erforderliche Inhalte dieser Dokumente vor dem Hochladen geschwärzt werden können.

239 Siehe § 3a BDSG

Bei der Anforderung von Dokumenten, die personenbezogene Daten enthalten, ist auf die Möglichkeit hinzuweisen, dass nicht benötigte Daten geschwärzt werden können.

## 13.2 „Sag mir, wie mein Richter tickt“



Ein Richter beschwerte sich bei uns darüber, dass auf dem Bewertungsportal „Richterscore“ zu ihm ein Profil erstellt und seine richterliche Tätigkeit bewertet wurde. Nach Angaben der Betreiber dient die Webseite als berufliches Austauschforum für zugelassene Rechtsanwälte. Sie sollen sich anhand von Einträgen ihrer Kolleginnen und Kollegen vor Gerichtsverfahren über die jeweiligen Richterinnen und Richter ein Bild machen können. Für die Richterinnen und Richter blieb das Forum allerdings verschlossen, sie erhielten keinen Zugang zur Plattform. Auch ohne Registrierung konnte jedoch eingesehen werden, ob ein Profil für den gesuchten Namen besteht.

Die Bewertung der Richterinnen und Richter erfolgt durch die Vergabe von Sternen (1-5) für fünf festgelegte Eigenschaften (u. a. Schnelligkeit, Rechtskenntnis) und durch eine Freitextkommentarfunktion. Über ein Eingabefeld kann man unsachliche Kritik melden. Bei Stichproben haben wir jedoch unsachliche, teils beleidigende Kommentare festgestellt. Entgegen den Regelungen des Bundesdatenschutzgesetzes werden die betroffenen Richterinnen und Richter bislang nicht durch die Betreiber über die Existenz eines zu ihrer Person angelegten Profils benachrichtigt.[240]

Die Rechtsprechung zu Bewertungsportalen anderer Berufsgruppen (wie z. B. für Ärzte oder Lehrer) hat u. a. im sog. „spickmich-Urteil“[241] Kriterien für deren Rechtmäßigkeit aufgestellt. Danach sind derartige Portale rechtmäßig, wenn sich die Bewertung allein auf das berufliche Verhalten bezieht und anhand sachlicher Kriterien erfolgt. Eine Pranger-Wirkung durch Beleidigungen oder Schmähungen

240 Gemäß § 33 Abs. 1 BDSG ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, der Verarbeitung oder Nutzung sowie von der Identität der verantwortlichen Stelle zu benachrichtigen.

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

muss ausgeschlossen sein. Bei missbräuchlichen Bewertungen ist sicherzustellen, dass entsprechende Beiträge gelöscht werden. – Nichts anderes darf für die Bewertung von Richterinnen und Richtern gelten. Jedoch haben die Betreiber der Plattform bisher keine zufriedenstellenden Vorschläge für die Umsetzung der Benachrichtigungspflicht und die Kontrolle der Sachlichkeit der Kommentare unterbreitet. Die Prüfung ist noch nicht abgeschlossen.

Bewertungsportale sollen sachlich und für die Betroffenen transparent sein.

## 13.3 Alternativen zu WhatsApp

Aus der Praxis

Der Kommunikationsdienst WhatsApp ist zwar sehr populär, steht jedoch auch seit Jahren wegen Datenschutzmängeln und einer intransparenten Verarbeitung von Nutzerdaten in der Kritik. Wir haben aus diesem Anlass verstärkt Alternativen zu WhatsApp geprüft.

Bei jedem Start von WhatsApp wird das Adressbuch der Nutzerin oder des Nutzers vom verwendeten Smartphone auf die Server von WhatsApp hochgeladen, um auf diesem Wege abzugleichen, welche der eigenen Kontakte ebenfalls WhatsApp nutzen. Die Nutzerin oder der Nutzer kann dies zwar inzwischen untersagen, das hat aber zur Folge, dass WhatsApp keine Kontakte zur Verfügung hat, was die Nutzung erheblich einschränkt. Der daher von den Nutzenden üblicherweise gewährte Zugriff mag komfortabel sein, lässt jedoch völlig außer Acht, dass dadurch auch Daten Dritter ohne deren Einwilligung weitergegeben werden.

Die Übertragung des Adressbuchs auf den Server erfolgt nicht in lesbarem Text. Vielmehr werden eindeutige Prüfwerte[242] berechnet, die zum Server übermittelt und verglichen werden. Da es nur eine begrenzte Anzahl von Telefonnummern gibt, könnten diese selbst von durchschnittlichen PCs in kurzer Zeit durchprobiert und jeweils mit den Prüfwerten verglichen werden. Damit könnte in der Praxis aus dem Prüfwert auf eine Telefonnummer geschlossen werden.

242 Der Prüfwert wird mittels einer unumkehrbaren kryptografischen Hashfunktion aus der Telefonnummer berechnet.

Die von der Weitergabe ihrer Daten aus dem Adressverzeichnis betroffenen Personen können sich dagegen kaum zur Wehr setzen. Eine Funktion zum manuellen Hinzufügen von Kontakten außerhalb des Adressbuchs direkt in der App, wie sie andere Messenger-Dienste mitunter anbieten, fehlt bei WhatsApp. WhatsApp ist daher ohne Hochladen des Adressbuchs so gut wie nicht nutzbar. Darüber hinaus ist auch seit Jahren unklar, wie WhatsApp bzw. die Mutterfirma Facebook mit den erhaltenen Nutzerdaten umgehen.[243] WhatsApp und Facebook hüllen sich zu diesem Thema weitestgehend in Schweigen: Die Informationen auf der Homepage von WhatsApp[244] liefern nur allgemeine Aussagen, ohne konkret zu benennen, wie lange die Daten gespeichert oder ob sie ggf. auch für andere Zwecke als zur Erbringung der konkreten Dienstleistung genutzt werden.

Nachgebessert hat WhatsApp inzwischen hingegen bei der Verschlüsselung. Nachdem andere Anbieter wie „Threema" schon frühzeitig eine Ende-zu-Ende-Verschlüsselung angeboten haben – dies bedeutet, dass der Inhalt der gesamten Kommunikation zwischen Absender und Empfänger verschlüsselt übertragen wird, sodass unbefugte Dritte diese nicht mitlesen können –, nutzt WhatsApp diese sichere Art der Verschlüsselung seit dem Jahr 2016 ebenfalls standardmäßig.

Dennoch ist die Anwendung aus Datenschutzsicht kritisch zu sehen: So berufen sich Facebook und WhatsApp auch weiterhin auf das aktuell aus ihrer Sicht für sie ausnahmslos gültige Recht der USA, wodurch die Nutzenden in Deutschland praktisch schlechter geschützt sind, weil sie sich mit Beschwerden an das US-Unternehmen oder an amerikanische Behörden wenden müssen. Mit Inkrafttreten der EU-Datenschutz-Grundverordnung wird hier eine Verbesserung eintreten, weil diese dann für die europäischen Nutzerinnen und Nutzer durch das sog. Marktortprinzip mit allen Schutzrechten auch gegenüber amerikanischen Unternehmen wie WhatsApp gilt. Das jeweilige Unternehmen muss dann zudem eine Kontaktadresse innerhalb der EU bereitstellen. Allerdings können sich bei Sanktionen dennoch Vollstreckungsprobleme ergeben.

243 Seit 2014 gehört WhatsApp zur Firma Facebook Incorporated, welche u. a. das soziale Netzwerk Facebook betreibt.

244 Siehe https://faq.whatsapp.com/de/general/20971813/?category=5245250

Zunehmend – insbesondere seit der Übernahme von WhatsApp durch Facebook – äußern sich Nutzerinnen und Nutzer zudem besorgt über den mangelnden Datenschutz bei WhatsApp und den Datenaustausch mit dem Mutterkonzern Facebook. Damit einhergehend steigt auch das Interesse an Alternativen, welche ebenso leicht zu bedienen sind, gleichzeitig jedoch ein höheres Niveau an Datenschutz und Datensicherheit bieten.

Positiv fallen hierbei insbesondere die Anbieter Threema, Wire und Signal – vormals TextSecure – auf. Der Anbieter Threema gilt als Vorreiter in punkto Datenschutz und legt den Schwerpunkt außerdem vor allem auf Sicherheitsaspekte. Nutzerinnen und Nutzer können sich gegenseitig in einem dreistufigen Verfahren authentifizieren, um sicherzustellen, dass es sich tatsächlich um die Person handelt, die sich als Absender bzw. Urheber einer Nachricht ausgibt. Die Kommunikation innerhalb der App erfolgt stets verschlüsselt (Ende-zu-Ende-Verschlüsselung). Das Adressbuch kann ebenso wie bei anderen Kurznachrichtendiensten zum Finden neuer Kontakte genutzt werden. Im Unterschied zu WhatsApp ist eine Nutzung von Threema auch ohne Hochladen des Adressbuches auf einen Server des Anbieters möglich, erfordert aber, dass Kommunikationspartner sich treffen und gegenseitig die Threema-internen Teilnahmekennungen – Nutzungsnamen – eingeben bzw. einscannen. Die Verschlüsselungslösung der App wurde von Experten im Jahr 2015 im Rahmen einer Kontrolle überprüft und für gut befunden. Auch die Stiftung Warentest lobte Threema im Februar 2014 im Rahmen eines Schnelltests für seinen Datenschutz. Da sich der Unternehmenssitz und der Serverstandort von Threema in der Schweiz befinden, ist hier gemäß dem Schweizer Bundesgesetz über den Datenschutz auch rechtlich ein hohes Datenschutzniveau des Anbieters verpflichtend vorgeschrieben. Seit dem Ende des Jahres 2016 veröffentlicht die Threema GmbH auch einen regelmäßig aktualisierten Transparenzbericht, in welchem Behördenanfragen offengelegt werden.[245] Zu beachten ist, dass die App nicht kostenfrei verfügbar ist, sondern einmalig gegen eine jedoch nur geringe Gebühr erworben werden muss.

Ebenfalls positiv ist uns der Anbieter „Wire" von der Wire Swiss GmbH bei einer Überprüfung aufgefallen. Die Gesellschaft hat ihren Sitz in der Schweiz, betreibt die technische Fortentwicklung des Programms jedoch durch ein eigenes Ent-

245 Siehe https://threema.ch/de/transparencyreport

wicklerteam in Berlin. Das Programm ist kostenlos verfügbar und Nutzerinnen und Nutzer können sich gegenseitig anhand eines Sicherheitscodes authentifizieren, um die wahre Identität der Kommunikationspartner zu bestätigen. Die Kommunikation erfolgt ebenfalls gesichert durch eine Ende-zu-Ende-Verschlüsselung. Einmal versandte Nachrichten, Bilder und Videos können später auch wieder aus den entsprechenden Chats gelöscht werden. Dieser Löschvorgang kann sowohl auf dem eigenen Gerät als auch auf den Geräten aller Chatteilnehmerinnen und -teilnehmer ausgeführt werden. Eine ähnliche Funktion wurde inzwischen auch von WhatsApp in seinem Angebot implementiert. Wire zeichnet sich zudem durch ein hohes Maß an Transparenz aus, da sowohl der Quelltext der App als auch größere Teile des Serverquellcodes öffentlich verfügbar sind und somit von jedermann eingesehen werden können.[246] Darüber hinaus wurden die Sicherheit der verwendeten kryptografischen Lösung und deren Implementierung im Jahr 2016 von externen IT-Sicherheitsfirmen überprüft und für gut befunden. Die dabei gefundenen Schwachstellen wurden von Wire schrittweise behoben.[247]

Eine weitere Alternative zu WhatsApp stellt Signal dar. Das Programm der Firma Open Whisper Systems ist kostenlos für verschiedene Plattformen verfügbar und die Kommunikation erfolgt auch hier per Ende-zu-Ende-Verschlüsselung. Nachrichten können nach dem Eingang wieder gelöscht werden, entweder durch einen Fernlöschbefehl des Absenders oder durch Selbstlöschung nach festgelegter Zeit. Darüber hinaus verhindert das Programm standardmäßig, Bildschirmfotos von Unterhaltungen zu erstellen. Der Programmcode für die Serverplattform ist öffentlich zugänglich[248] und kann somit analysiert werden. Damit können potenzielle Sicherheitsrisiken überprüft werden. Der Quellcode des Programms wurde bereits mehrfach durch unabhängige wissenschaftliche Institutionen geprüft, u. a. 2014 durch die Ruhr-Universität Bochum[249] sowie 2016 durch ein Team der University of Oxford, der Queensland University of Technology und der McMaster University, und insgesamt für sicher befunden. Bei der Überprüfung gefundene Schwachstellen wurden vom Anbieter behoben.

246 Siehe https://github.com/wireapp

247 Siehe Report unter https://medium.com/@wireapp/wires-independent-security-review-61f37a1762a8

248 Siehe https://github.com/whispersystems/TextSecure-Server/

249 Siehe https://eprint.iacr.org/2014/904.pdf

Eine aus Datenschutzsicht relevante Frage – die Nutzende für sich selbst entscheiden müssen – ist die nach dem Ort der Datenverarbeitung und unter wessen Kontrolle diese geschieht. Trotz der Verschlüsselung fallen auf den Servern der Betreiberfirmen zwangsläufig Daten darüber an, wer mit wem in welchen Zeiträumen kommuniziert hat.[250] Bei WhatsApp und Signal erfolgt die Datenverarbeitung in den USA. Wire verarbeitet Daten für Privatnutzer derzeit in europäischen Rechenzentren eines internationalen Cloud-Dienstes mit Sitz in den USA, Firmenkunden können eigene Server betreiben. Die Server von Threema befinden sich in der Schweiz und unter alleiniger Kontrolle der schweizerischen Firma.

Wir haben dieses Jahr verschiedene Kommunikationsdienste überprüft, welche alternativ zu WhatsApp genutzt werden können. Wichtig waren für uns hierbei insbesondere ein hohes Maß an Datenschutz sowie eine transparente Verarbeitung und Speicherung von Nutzerdaten. Hierbei haben sich insbesondere die Anbieter Threema, Wire und Signal positiv hervorgetan. Aus Datenschutzsicht sollte jedoch auch der Ort der Datenverarbeitung bewertet werden.

## 13.4 Aus der Arbeit der „Berlin Group“

Die unter dem Vorsitz der Berliner Beauftragten für Datenschutz und Informationsfreiheit tagende internationale Arbeitsgruppe für Datenschutz in der Telekommunikation (die sog. Berlin Group) hat sich im vergangenen Jahr neu organisiert. Aufgrund der Größe, die die Arbeitsgruppe in den letzten Jahren erreicht hat, musste ein neuer Ansatz entwickelt werden, der die finanziellen Aufwendungen und Ressourcen auf mehrere „Schultern“ verteilt und gleichzeitig die Produktivität und den Nutzen der Arbeit der Gruppe erhält bzw. steigert.

Auf der Frühjahrskonferenz am 24./25. April in Washington D. C. wurde auf eindringlichen Wunsch der Teilnehmerinnen und Teilnehmer u. a. vereinbart, dass die Gruppe weiterhin zweimal jährlich tagt, die Herbstsitzungen jedoch nicht mehr ausschließlich in Berlin stattfinden, sondern ebenso wie die Frühjahrssitzungen an wechselnden Orten, sodass auch hinsichtlich der Sitzungsorganisation eine

250 Sog. Metadaten

Lastenverteilung stattfindet. Für die Herbstsitzungen haben sich mehrere Datenschutzaufsichtsbehörden bereit erklärt, einen „Pool“ zu bilden und auf einer Rotationsbasis die Treffen im Wechsel auszurichten. Dieser regelmäßige Rhythmus ermöglicht für die Betroffenen eine langfristige Planung. Die Ausrichtung der Frühjahrssitzungen steht allen Teilnehmerländern offen. Neben der örtlichen Verteilung der Verantwortlichkeiten wurden auf unseren Vorschlag hin auch die Aufgaben und Verantwortlichkeiten zwischen dem auch weiterhin in Berlin geführten Sekretariat der Berlin Group und den gastgebenden Aufsichtsbehörden neu aufgeteilt. Schon von diesen rein organisatorischen Änderungen erhoffen wir uns eine spürbare Entlastung unserer Behörde.

Aber auch bei der Organisation der inhaltlichen Arbeit wurden auf unseren Vorschlag hin Neuerungen beschlossen: Die Rolle der Berichterstatterinnen und Berichterstatter für die zu behandelnden Themen wurde neu definiert und gestärkt, außerdem einigten sich die Mitglieder auf angemessene Fristen für die Einreichung der Entwürfe von Dokumenten, die in den Sitzungen erörtert werden sollen. Es zeigt sich jetzt bereits, dass auch diese inhaltliche Verteilung von Verantwortlichkeiten und die Schaffung klarer zeitlicher Abläufe zu einer effizienteren und das Berliner Büro entlastenden Arbeitsweise führt. Zur Auswertung der Änderungen ist eine Evaluierung nach Ablauf von zwei Jahren vorgesehen.

Inhaltlich hat die Berlin Group 2017 insgesamt vier Arbeitspapiere verabschiedet.[251]

In der 61. Sitzung der Berlin Group in Washington einigten sich die Mitglieder auf das **„Arbeitspapier zum Thema E-Learning-Plattformen“**, das ein höchst aktuelles Thema aufgreift. E-Learning Plattformen kommen an Schulen und Universitäten weltweit immer häufiger zum Einsatz. Dadurch werden stetig mehr personenbezogene Daten über Schülerinnen und Schüler sowie über deren Verhalten und Leistung digital erhoben. Sind solche Daten erst einmal vorhanden, wächst auch schnell die Nachfrage, diese für weitere Bildungszwecke, z. B. für sog. Learning

251 Abrufbar, auch in deutscher Übersetzung, auf unserer Internetseite unter www.datenschutz-berlin.de/working-paper.html

Analytics,[252] zu nutzen. Das Arbeitspapier zeigt Datenschutzrisiken für Schülerinnen und Schüler beim Einsatz solcher Plattformen auf, die z. B. dadurch entstehen, dass über Noten automatisiert entschieden wird, ohne das die Lehrerinnen und Lehrer sich in die Prozesse bestimmend einbringen können und ohne dass für Eltern, Schülerinnen und Schüler der Prozess der Entscheidungsfindung und die zugrundegelegten Daten transparent wären. Darüber hinaus besteht ein hohes Risiko, dass Daten über Schülerinnen und Schüler weiterverwertet werden, indem sie beispielsweise über die eigentlichen Bildungszwecke hinaus für kommerzielle Zwecke genutzt werden. Neben naheliegenden Werbezwecken besteht aber auch die Gefahr, dass solche Daten auch für existentielle Entscheidungen, z. B. mit Blick auf die Karriere, den Hauskauf oder eine Kreditbewilligung, herangezogen werden. Das Arbeitspapier enthält konkrete Empfehlungen für Bildungseinrichtungen, Betreiberinnen und Betreiber von E-Learning-Plattformen und Datenschutzaufsichtsbehörden für einen datenschutzgerechten Einsatz solcher Plattformen.

Ebenfalls in Washington verabschiedete die Arbeitsgruppe das **„Arbeitspapier zu internationalen Grundsätzen oder Instrumenten zur Regulierung der nachrichtendienstlichen Informationsbeschaffung“**, welches an die Enthüllungen von Edward Snowden im Jahr 2013 und an das Spannungsfeld zwischen Sicherheit und dem Recht auf Privatsphäre anknüpft. Das Arbeitspapier skizziert die aktuelle Diskussion und die Forderungen nach international verbindlichen Standards im Zusammenhang mit der Überwachung von Kommunikationsinhalten durch Nachrichtendienste. Dabei spricht es Empfehlungen für Datenschutzbehörden aus, wie sie einen Beitrag zur Entwicklung solcher Grundprinzipien leisten können.

In der 62. Sitzung der Berlin Group, die am 27./28. November 2017 bei der CNIL[253] in Paris stattfand, verabschiedete die Arbeitsgruppe insgesamt zwei Papiere:

252 Als „Learning Analytics“ kann nach George Siemens („Learning and Analytics“, 5. August 2011, abrufbar unter www.learningandanalytics.net/?p=131) bezeichnet werden „das Messen, Sammeln, Analysieren und Auswerten von Daten über Lernende und ihren Kontext mit dem Ziel, das Lernen und die Lernumgebung zu verstehen und zu optimieren“.

253 Commission Nationale de l'Informatique et des Libertés, die französische Datenschutzaufsichtsbehörde

Das **„Arbeitspapier zu Fragen der Privatsphäre und des Datenschutzes in Bezug auf die Daten von Registranten und das WHOIS-Verzeichnis bei ICANN“** thematisiert insbesondere die Offenlegung von Daten im sog. WHOIS-Verzeichnis[254], in dem die im Zusammenhang mit der Registrierung von Webseiten nach den Regularien der ICANN[255] erhobenen Daten zwingend veröffentlicht werden. Da es dabei regelmäßig auch um personenbezogene Daten geht, wird deren Veröffentlichung im Arbeitspapier als nicht verhältnismäßig kritisiert und darauf hingewiesen, dass dieses Verfahren gegen die Datenschutzgrundsätze sowie die Datenschutzgesetze in vielen Ländern verstößt. Im Arbeitspapier wird zudem darauf hingewiesen, dass ein mehrstufiger Zugriff[256] nach wie vor nicht realisiert ist, sodass das Verzeichnis in der Konsequenz als eine vollständig und anonym unbeschränkt zugängliche und frei durchsuchbare Datenbank weitergeführt wird. Neben anderen kritischen Aspekten, die das Arbeitspapier aufzeigt, werden konkrete Empfehlungen für ICANN formuliert, sich dringend mit bestimmten Datenschutzaspekten (u. a. Zweckfestlegung, Erforderlichkeitsprinzip) zu befassen, sowie insbesondere Richtlinien zu entwickeln, die mit den Anforderungen der bestehenden Datenschutzgesetze und mit international anerkannten Datenschutzprinzipien und -standards vereinbar sind.

Darüber hinaus verabschiedete die Berlin Group in Paris das **„Arbeitspapier zu Firmware-Updates eingebetteter Systeme im Internet der Dinge“.** Das Arbeitspapier befasst sich mit der Frage, was unter Firmware[257] zu verstehen ist und warum hierfür Aktualisierungen notwendig sind bzw. wie diese realisiert werden könnten. Dabei geht es insbesondere auch um die Gefahren, die durch schwache kryptografische Algorithmen sowie durch Fehler in der Software entstehen und die die Geräte von außen angreifbar machen können. Das Papier zeigt potenzielle Probleme der Aktualisierung von Firmware sowie Datenschutzrisiken auf und schließt mit

254 Verzeichnis der Inhaberinnen und Inhaber aller Webseiten weltweit

255 Internet Corporation for Assigned Names and Numbers, eine von verschiedenen Akteuren getragene Einrichtung mit Sitz in Kalifornien, USA, die gegründet wurde, um das Domain Name System (DNS) zu koordinieren, d. h. den Verzeichnisdienst, der die Namen für Webseiten im Internet vergibt und verwaltet

256 Zugriff auf die Daten in unterschiedlichem Umfang je nach Zugriffsberechtigung der zugreifenden Stelle

257 Die Firmware eines Geräts ist Software, die in elektronische Geräte eingebettet ist, um deren grundlegende Funktion zu gewährleisten. Sie ist funktional fest mit der Hardware verbunden, das eine ist ohne das andere nicht nutzbar.

konkreten Empfehlungen für Regulierungsbehörden, Gesetzgeber und Aufsichtsbehörden sowie für Gerätehersteller und Geräteinhaber.

Intensiv setzte sich die Arbeitsgruppe damit auseinander, dass Strafverfolgungsbehörden bei strafrechtlichen Ermittlungen zunehmend den Zugang zu elektronischem Beweismaterial suchen, das über nationale Grenzen hinaus z. B. auf Servern in anderen Zuständigkeitsbereichen aufbewahrt wird. Diese Datenanforderungen werfen schwierige Fragen im Hinblick auf die Einhaltung nationaler und internationaler Standards zum Datenschutz und zum Schutz der Privatsphäre auf. Ein entsprechendes Arbeitspapier zu Standards für den Datenschutz und den Schutz der Privatsphäre in den Bereichen grenzüberschreitender Datenanfragen zu Strafverfolgungszwecken wird voraussichtlich in der Frühjahrskonferenz 2018 erörtert.

# 14 Europäischer und internationaler Datenschutz

## 14.1 Neue Entwicklungen zum EU-US Privacy Shield



Wir haben im letzten Jahr über das sog. EU-US Privacy Shield als Nachfolgeabkommen zur „Safe Harbor"-Vereinbarung informiert.[258] Die zwischen der EU und den USA vereinbarten Neuregelungen für Übermittlungen personenbezogener Daten in die USA sind bereits seit August 2016 in Kraft.

Auf der Grundlage des neuen Abkommens können nunmehr personenbezogene Daten an US-Unternehmen übermittelt werden, die über eine gültige Zertifizierung im Privacy Shield verfügen. Die Zahlen in der im Internet abrufbaren Liste mit Zertifizierungen[259] haben sich in diesem Jahr gegenüber den Zahlen im Vorjahr auf 2602 Anmeldungen fast verdoppelt.[260] In Europa lebende Menschen haben gegenüber den zertifizierten US-Unternehmen eine Reihe individueller Rechte wie das Recht auf Information, auf Auskunft, Berichtigung und – unter bestimmten Umständen – auf Löschung sowie auf Garantien für den Fall einer Weiterübermittlung. Diese Rechte können von Betroffenen direkt gegenüber den zertifizierten US-Unternehmen geltend gemacht werden. Daneben ist es auch möglich, sich jederzeit an die zuständige nationale Datenschutzbehörde zu wenden. Um es Betroffenen zu erleichtern, sich zu informieren und ggf. eine Beschwerde einzureichen, haben wir allgemeine Informationen zum Privacy Shield sowie unter den EU-Datenschutzbehörden abgestimmte Beschwerdeformulare veröffentlicht.[261]

258 JB 2016, 1.1
259 www.privacyshield.gov
260 Stand: 29. Dezember 2017
261 www.datenschutz-berlin.de/eu-us-privacy-shield.html

Das Privacy Shield räumt europäischen Bürgerinnen und Bürgern erstmals auch eine Überprüfungsmöglichkeit ein, wenn sie Zugriffe von US-amerikanischen Sicherheitsbehörden oder Nachrichtendiensten auf ihre aus Europa übermittelten Daten unter Verstoß gegen geltende Bestimmungen befürchten. Für die Untersuchung solcher Anträge soll eine Ombudsperson im US-Außenministerium zuständig sein. Sie ist verpflichtet, Überprüfungsanträgen nachzugehen, die ihr von den europäischen Datenschutzbehörden zugeleitet wurden.

Ob und wie das Privacy Shield in der Praxis funktioniert, war im September Gegenstand einer ersten Evaluierung durch die Europäische Kommission. Diese ist verpflichtet, einmal pro Jahr zu überprüfen, ob ein angemessenes Datenschutzniveau weiterhin gewährleistet ist.

Dass die Position der Ombudsperson nach wie vor nicht besetzt ist, sondern nur kommissarisch wahrgenommen wird, ist nur einer der Punkte, den die Europäische Kommission nach zweitägigen Evaluierungsgesprächen mit der US-Seite in ihrem Prüfbericht kritisierte.[262] Daneben forderte die Kommission eine aktivere und regelmäßigere Kontrolle der Einhaltung der Datenschutzpflichten durch die beteiligten Unternehmen von Seiten des US-Handelsministeriums. Denn es gibt offenbar Firmen, die mit falschen Angaben eine Zertifizierung erreichen wollen. Besonders wachsam ist die Europäische Kommission im Hinblick auf die anstehende Reform des US-Gesetzes, das die Auslandsaufklärung und Spionageabwehr der Vereinigten Staaten regelt.[263] Sollten die dort bestehenden Beschränkungen bei der Überwachung von Nicht-US-Bürgerinnen und -Bürgern aufgehoben werden, wäre dies womöglich für die Europäische Kommission ein Grund, an dem Abkommen nicht festzuhalten. Im Ergebnis sieht die Kommission allerdings ein angemessenes Datenschutzniveau durch das Privacy Shield gewährleistet.

Obwohl mehrere europäische Datenschutzbehörden an der Evaluierung des Privacy Shields im September in den USA beteiligt waren, hatten sie keinen Einfluss auf die Erstellung des Kommissionsberichts. Deshalb verfasste die

262 Report from the Commission to the European Parliament and to the Council on the first annual review of the functioning of the EU-US Privacy Shield, Commission Staff Working Document, beides vom 18. Oktober 2017 und (in engl. Fass.) abrufbar unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

263 Foreign Intelligence Surveillance Act (FISA)

Gruppe nach Art. 29 Europäische Datenschutzrichtlinie[264] eine eigene Stellungnahme,[265] die weitaus kritischer ausfällt und aus der hier nur einige Punkte genannt werden:

In Bezug auf die kommerziellen Aspekte wurde die US-Seite aufgefordert, sowohl bei der Zertifizierung als auch im späteren Überprüfungsverlauf zu beachten, dass die US-Unternehmen personenbezogene Daten aus Europa in verschiedenen Rollen erhalten können, nämlich entweder als selbstverantwortlicher Eigenverarbeiter oder als Auftragsdatenverarbeiter. Unterschiedliche Vorstellungen herrschen auch im Hinblick auf die Interpretation und Handhabung von Beschäftigtendaten und Weiterübermittlungen von Daten. Hier hat die Art. 29-Gruppe der US-Seite angeboten, die Erarbeitung neuer Richtlinien beratend zu begleiten, um ein gemeinsames Verständnis der Prinzipien des Privacy Shields zu entwickeln und den Bedürfnissen der Wirtschaft auf beiden Seiten des Atlantiks Rechnung zu tragen.

In Bezug auf die angesprochene Reform des US-Rechts[266] regt die Art. 29-Gruppe an, nicht Überwachungsprogramme generell zu autorisieren, sondern die Überwachung von konkreten Kriterien wie etwa einem „begründeten Verdacht" abhängig zu machen sowie eine genaue Zielausrichtung vorzusehen. Diese sollte bestimmen, ob eine Einzelperson oder eine Gruppe von Personen Ziel der Überwachung sein soll, wobei bei Personen eine entsprechende Vorabprüfung durch eine unabhängige Behörde gefordert wird.

Wegen dieser und – auch nach den Feststellungen im letzten Jahr[267] – weiterer noch immer ungeklärter Kritikpunkte appellierte die Art. 29-Gruppe an die Europäische Kommission und an die zuständigen US-Behörden, unverzüglich einen Aktionsplan aufzustellen. Darin sollten nicht nur alle offenen Fragen formuliert, sondern ihre Klärung in einer bestimmten Rangfolge festgelegt werden. Zu einer der Prioritäten gehört beispielsweise die Einrichtung der unabhängigen Ombudsstelle unter Darlegung ihrer Befugnisse. Nach dem Willen der Art. 29-Gruppe

264 Die Art. 29-Gruppe hat beratende Funktion; alle europäischen Datenschutzbehörden sind Mitglieder.

265 WP 255 vom 28. November 2017, EU-US Privacy Shield – First annual Joint Review, abrufbar unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

266 Section 702 Foreign Intelligence Surveillance Act (FISA)

267 JB 2016, 1.1

sind alle vordringlichen Fragen bis zum Wirksamwerden der Europäischen Datenschutz-Grundverordnung am 25. Mai 2018 zu beantworten, alle übrigen Punkte spätestens bis zum nächsten gemeinsamen Prüfbericht im Herbst 2018. Sofern nach Ablauf dieser Fristen keine Abhilfe geschaffen werde, werden die Mitglieder der Art. 29-Gruppe angemessene Maßnahmen ergreifen, auch um ggf. eine gerichtliche Klärung in Bezug auf die erforderliche Angemessenheit des Privacy Shields zu erreichen.[268]

## 14.2 EuGH stoppt Fluggastdaten-Abkommen mit Kanada

Aus der Praxis

Der Gerichtshof der Europäischen Union (EuGH) hat erneut eine datenschutzfreundliche Entscheidung gefällt. Er vertrat in einem Gutachten die Auffassung, dass das geplante Fluggastdaten-Abkommen zwischen Kanada und der EU in weiten Teilen gegen die Grundrechte des Datenschutzes und der Achtung des Privatlebens verstößt.[269]

Die Übermittlung sog. PNR-Daten[270] soll die Bekämpfung terroristischer Straftaten und grenzüberschreitender schwerer Kriminalität ermöglichen. Dieser Zweck kann die Datenübermittlung zwar grundsätzlich rechtfertigen. Die Richter beanstandeten aber vor allem den Umfang der geplanten Datenspeicherung. Der Schutzzweck der öffentlichen Sicherheit in Kanada gestatte nicht die Übermittlung sensitiver Daten, aus denen etwa die rassische oder ethnische Herkunft, religiöse Überzeugungen oder Informationen zum Gesundheitszustand von Fluggästen hervorgehen. Der Übermittlungszweck rechtfertige auch nicht von vornherein die weitere Verwendung und Speicherung von Passagierdaten über den Aufenthalt in Kanada hinaus. Sofern sich während des Aufenthalts keine konkreten Anhalts-

268 Pressemitteilung zur Sitzung der Art. 29-Gruppe im November 2017, „First annual Joint Review of the Privacy Shield", abrufbar unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48781

269 EuGH, Gutachten 1/15 (Große Kammer) vom 26. Juli 2017, in: EuGRZ 2017, S. 535 ff.

270 PNR steht für Passenger Name Record. Das sind Fluggastdatensätze, zu denen neben Kontakt-, Reise- und Zahlungsinformationen auch Informationen zu Ernährungsgewohnheiten und zum Gesundheitszustand zählen können.

punkte für geplante terroristische oder andere schwere Straftaten ergeben hätten, sei eine weitere Speicherung der Daten nicht gerechtfertigt.

Der EuGH hat erneut einer anlasslosen Speicherung von personenbezogenen Daten auf Vorrat eine klare Absage erteilt. Es ist zu erwarten, dass die Europäische Kommission vor diesem Hintergrund bereits bestehende PNR-Abkommen mit Australien und den USA auf den Prüfstand stellt.

## 14.3 Grundsätzliche Rechtsfragen vor dem EuGH: Facebook-Fanpage-Verfahren[271]



Ein weiteres Kapitel offener Rechtsfragen bei der Verarbeitung der Daten von Nutzerinnen und Nutzern im Internet könnte erneut[272] durch die Rechtsprechung des Europäischen Gerichtshofs (EuGH) in naher Zukunft geschlossen werden. Es geht um die Frage, wer eine sog. verantwortliche Stelle ist. Ausgangspunkt ist ein Verfahren der schleswig-holsteinischen Datenschutzbehörde zu der Nutzung einer Facebook-Fanpage durch die dort ansässige Wirtschaftsakademie als Webseitenbetreiberin.

Fanpages sind Webauftritte von Unternehmen oder Privatpersonen bei dem sozialen Netzwerk Facebook, die dazu genutzt werden, mithilfe der Kommunikationsmittel des Netzwerks[273] die eigene Sichtbarkeit und Popularität zu steigern. Durch derartige Fanpages sind die jeweiligen Anbieter sowohl für die Nutzerinnen und Nutzer des Netzwerks erreichbar als auch für andere Personen, die Facebook nicht nutzen. Zugleich erhalten die Betreiberinnen und Betreiber der Webseiten statistische Informationen von Facebook zu den Besucherinnen und Besuchern der jeweiligen Fanpage.

271 Rechtssache C 210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein gegen Wirtschaftsakademie Schleswig-Holstein GmbH

272 Wie bereits kürzlich bei der Frage des Personenbezugs dynamischer IP-Adressen, vgl. EuGH, Urteil vom 19. Oktober 2016, C-582/14 und JB 2016, Einleitung

273 Nutzbar ist auf diesem Wege z. B. die Kommentarfunktion oder die Möglichkeit, durch die sog. „like"-Funktion für einen großen Personenkreis sichtbar für gut befunden zu werden.

Die Rechtsfragen, die im Rahmen des Rechtsstreits zu klären sind, lassen sich ohne Weiteres auf eine Vielzahl von Verarbeitungssituationen personenbezogener Daten im Zusammenhang mit der Nutzung elektronischer Kommunikation übertragen. In der Regel geht es darum, dass Organisationen, Unternehmen und Internetanbieter sich der Dienste und Infrastrukturen großer Dienstleister bedienen, deren Aktivitäten sie weder rechtlich noch technisch steuern bzw. kontrollieren können. Zumeist werden die vertraglichen Bedingungen, unter denen die Unternehmen die Dienste nutzen dürfen, von den Dienstleistern diktiert, denn häufig besitzen diese eine derartige Marktmacht, dass die angebotenen Dienste im Hinblick auf den Verbreitungsgrad fast alternativlos sind. Indem die Besucherinnen und Besucher z. B. die Profilseite oder das Benutzerkonto eines Unternehmens bei einem solchen Dienstleister aufrufen, werden Cookies[274] gesetzt, Pixel[275] geladen oder sonstige Daten von den Geräten durch die Dienstleister erhoben, die eine Identifikation ermöglichen. Diese Datenerhebungen und -verarbeitungen sind für die Besucherinnen und Besucher häufig nicht transparent und können von ihnen nicht wirksam verhindert werden. Die Unternehmen profitieren von der Nutzung dieser Dienste, indem sie ihre Wahrnehmbarkeit verbessern und Analysen zu ihren Besucherstrukturen erhalten. Für die Dienstleister geht es in der Regel zusätzlich um die Weiterverarbeitung der Daten, z. B. zum Zwecke des sog. Webtrackings, d. h. um die Beobachtung und Analyse der Nutzerinnen und Nutzer zu Geschäfts- und Marketingzwecken.

In dem angesprochenen, über mehrere Instanzen geführten Rechtsstreit bewog die Frage nach der datenschutzrechtlichen Verantwortlichkeit bei der Auswahl des Betreibers eines solchen Dienstes das Bundesverwaltungsgericht dazu, den EuGH anzurufen.[276] Das Bundesverwaltungsgericht ging zwar selbst nicht davon aus, dass die Webseitenbetreiberin verantwortliche Stelle ist.[277] Gleichwohl stellte

274 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, besuchte Webseiten und Zeitpunkte des Besuchs zugeordnet werden.

275 Kleine Grafiken auf Webseiten, die meist nur 1x1 Pixel messen und beim Aufruf einer Webseite von einem Server geladen werden. Das Herunterladen wird registriert und kann für Auswertungen im Bereich des Online-Marketings genutzt werden.

276 BVerwG, Beschluss vom 25. Februar 2016–1 C 28.14

277 BVerwG, Beschluss vom 25. Februar 2016–1 C 28.14, Rn. 27

es sich die Frage, ob es auch eine abgestufte Verantwortlichkeit geben kann und legte u. a. diese Frage dem EuGH zur Klärung vor.[278]

Der EuGH hat das letzte Wort noch nicht gesprochen. Allerdings liegen die Schlussanträge des Generalanwalts[279] vor, die anders als das Bundesverwaltungsgericht von einer gemeinsamen Verantwortlichkeit von Fanpage-Betreiber und Facebook für die Phase der Erhebung der Daten ausgehen. Zwar erhalte der Fanpage-Betreiber keinen Zugriff auf die erhobenen Daten, gleichwohl übe er einen „bestimmenden Einfluss auf das Auslösen der Verarbeitung personenbezogener Daten" der Besucherinnen und Besucher aus, und verfüge „über die Macht, diese Verarbeitung zu beenden, indem er die Fanpage schließt".[280] Zudem hätte der Fanpage-Betreiber die von Facebook diktierten Vertragsbedingungen freiwillig angenommen und damit die „volle Verantwortung für sie übernommen".[281] Diese Umstände führen nach Ansicht des Generalanwalts dazu, dass die Fanpage-Betreiber jedenfalls an der Bestimmung über die Mittel und Zwecke der Verarbeitung beteiligt waren, was nach der für diesen Fall anwendbaren Datenschutz-Richtlinie[282] für die Verantwortlichkeit maßgeblich ist. Der Generalanwalt vertritt demnach die Auffassung, dass sicherzustellen ist, dass diejenigen, „die einen Bereithaltungsdienst für ihre Internetseite in Anspruch nehmen" und sich darüber „vermarkten", sich „nicht der datenschutzrechtlichen Verantwortung entziehen können", indem sie sich den Vertragsbedingungen des Dienstleisters unterwerfen.[283]

Bemerkenswert ist, dass der Generalanwalt sich nicht darauf beschränkt, sich zu den Facebook-Fanpages zu äußern. Vielmehr macht er deutlich, dass seiner Ansicht nach kein Unterschied zu dem Fall besteht, in dem ein Betreiber einer Webseite „den Code eines Webtracking-Dienstleisters in seine Webseite einbindet und somit ohne Wissen des Internetnutzers die Übermittlung von Daten, das Setzen

278 BVerwG, Beschluss vom 25. Februar 2016–1 C 28.14, 1. Vorlagefrage

279 Schlussanträge des Generalanwalts Yves Bot vom 24. Oktober 2017 in der Rechtssache C 210/16

280 Schlussanträge des Generalanwalts in der Rechtssache C 210/16, Rn. 56

281 Schlussanträge des Generalanwalts in der Rechtssache C 210/16, Rn. 61

282 Richtlinie 95/46/EG

283 Schlussanträge des Generalanwalts in der Rechtssache C 210/16, Rn. 64

von Cookies und die Erhebung von Daten zugunsten des Webtracking-Dienstleisters unterstützt".[284]

Nun kommt es auf die Entscheidung des EuGH an. Wenn das Gericht der Auffassung des Generalanwalts folgt, was häufig vorkommt, sind nicht nur die Betreiberinnen und Betreiber von Fanpages betroffen. Die Entscheidung wird sich auf sämtliche Anbieter auswirken, ob öffentlicher oder nichtöffentlicher Natur, die soziale Netzwerke bzw. Mikroblogging[285] nutzen, Social-Plugins[286] verwenden oder auf andere Art und Weise Dienste Dritter einbinden, um sich selbst zu präsentieren. Sie alle müssen dafür sorgen, dass die Anforderungen eingehalten werden, die an die Rechtmäßigkeit der von ihnen veranlassten Datenerhebungen zu stellen sind.

284 Schlussanträge des Generalanwalts in der Rechtssache C 210/16, Rn. 69

285 Beim Mikroblogging werden kurze SMS-ähnliche Texte erstellt, die in einem Blog oder Kurznachrichtendienstes dargestellt werden.

286 Ein Programmcode, der in die Webseite eingebunden wird und den Browser der Benutzerin bzw. des Benutzers der Webseite dazu veranlasst, Inhalte von einem Dritten anzufordern und dazu Daten an diesen Dritten übermittelt, z. B. „Gefällt mir"-Button von Facebook, oder „Twitter"-Button

# 15 Informationsfreiheit

## 15.1 Informationsfreiheit in Deutschland

Das **Bundesverfassungsgericht** hat in einer Entscheidung grundlegende Aussagen zur Informationsfreiheit getroffen.[287] In dem Rechtsstreit ging es um Akten der Bundesregierung, die in den Besitz der Konrad-Adenauer-Stiftung und des Historischen Instituts der Deutschen Bank gelangt waren. Das Gericht hat nicht nur entschieden, dass die ursprünglich aktenführende Stelle aufgrund des Informationsfreiheitsgesetzes des Bundes verpflichtet ist, die Akten wiederzubeschaffen und antragsgemäß zugänglich zu machen. Es hat darüber hinaus festgestellt, dass sich der Verfassungsrang der Informationszugangsfreiheit aus dem Grundgesetz herleitet, jedenfalls soweit der Gesetzgeber eine einfachgesetzliche Regelung getroffen hat. Nach dem Grundgesetz hat jeder Mensch das Recht, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten.[288] Zu diesen Informationsquellen zählen alle amtlichen Informationen, die nach dem Informationsfreiheitsgesetz des Bundes oder eines Landes grundsätzlich Gegenstand eines Informationszugangsantrags sein können. Demzufolge erhalten die Informationszugangsbegehren von antragstellenden Personen künftig ein größeres Gewicht, weil bei einer Abwägung konkurrierender Grundrechte nunmehr die Informationsfreiheit auf Augenhöhe mit dem Recht auf Datenschutz[289] und dem Recht auf Eigentum[290] steht.

Ein neues Urteil des **Bundesverwaltungsgerichts** ist ebenfalls bedeutungsvoll: Das Gericht hat in Bezug auf Umweltinformationen klargestellt, dass sich eine Maßnahme oder Tätigkeit auf Umweltbestandteile wie Luft, Wasser und Boden oder auf Faktoren wie Lärm, Abfälle und Emissionen lediglich auswirken oder wahrscheinlich auswirken muss, um eine Umweltinformation nach § 2 Abs. 3 Um-

287 Beschluss vom 20. Juni 2017 – 1 BvR 1978/13

288 Art. 5 Abs. 1 Satz 1 GG

289 Das Recht auf informationelle Selbstbestimmung wird hergeleitet aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

290 Art. 14 Abs. 1 GG umfasst auch Betriebs-/Geschäftsgeheimnisse eines Unternehmens.

weltinformationsgesetz (UIG) zu sein.[291] Eines unmittelbaren Zusammenhangs der einzelnen Daten mit der Umwelt bedarf es dagegen nicht. Damit ist der sachliche Anwendungsbereich des Umweltinformationsgesetzes denkbar weit gefasst.

Ende 2016 hat die Bundesregierung die Teilnahme Deutschlands an der 2011 gegründeten sog. OGP-Initiative bekanntgegeben. OGP steht für **Open Government Partnership**,[292] ein Zusammenschluss von inzwischen 75 Staaten, die sich für ein offenes und modernes Regierungs- und Verwaltungshandeln einsetzen. Im Rahmen dieser Teilnahme beschloss die Bundesregierung nun den Ersten Nationalen Aktionsplan 2017-2019 und legte damit „Grundsteine für offenes Regierungs- und Verwaltungshandeln", die sie als Signal für die weitere Förderung von Open Government betrachtet.[293] In dem Aktionsplan werden 15 Verpflichtungen formuliert, zu denen zunächst die Schaffung von Rahmenbedingungen für die OGP-Teilnahme und die Umsetzung von Open Data in der Verwaltungspraxis gehören. Die hierfür zu erarbeitenden Leitfäden sind Teil der „messbaren Meilensteine".[294]

Etwa zeitgleich mit der Bekanntgabe dieses Aktionsplans ist auf Bundesebene das **Open-Data-Gesetz**[295] in Kraft getreten. Damit sollen digitale Daten der Bundesbehörden maschinenlesbar und entgeltfrei öffentlich zugänglich gemacht werden. Es sind auch Rohdaten wie Angaben über Herkunft, Struktur und Inhalt der Verwaltungsinformationen erfasst. Diese sollen über das bestehende Portal GovData[296] verfügbar sein, das einen inhaltlichen zentralen Zugang zu offenen Verwaltungsdaten aus Bund, Ländern und Kommunen bietet, die diese Daten in ihren jeweiligen Open Data-Portalen zugänglich gemacht haben. Anders als das Informationsfreiheitsgesetz des Bundes begründet das neue Gesetz allerdings keinen Individualanspruch, digitale Daten der Behörden zu erhalten. Ein gerichtlich durchsetzbares Recht besteht also nicht.

291 Urteil vom 23. Februar 2017 – VII C 3.15
292 www.opengovpartnership.org
293 www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/08/ogp-aktionsplan.html
294 Verpflichtung 1 Nr. 5 sowie Verpflichtung 2 Nr. 5 des Ersten Nationalen Aktionsplans
295 Erstes Gesetz zur Änderung des E-Government-Gesetzes, BGBl. I, S. 2206
296 www.govdata.de

Leider blieb der Appell der Informationsfreiheitsbeauftragten der Länder im Deutschen Bundestag ungehört. Sie hatten angesichts der Auswirkungen auf die Landesgesetzgebung gefordert, anstelle der Verabschiedung eines Open-Data-Gesetzes die Weiterentwicklung des Informationsfreiheitsgesetzes des Bundes zu einem umfassenden Transparenzgesetz zu betreiben.[297]

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)** hat angesichts immer häufiger auftauchender sog. „Fake-News", also bewusst gestreuter Fehlinformationen, an alle öffentliche Stellen in Deutschland appelliert, durch größtmögliche Transparenz die Menschen in ihrer politischen Meinungs- und Willensbildung zu unterstützen.[298] Je mehr staatliche Informationen aktiv zur Verfügung gestellt werden, desto eher werden Menschen in die Lage versetzt, Falschmeldungen von richtigen Nachrichten zu unterscheiden. Darüber hinaus haben die Landesbeauftragten für die Informationsfreiheit Grundsatzpositionen formuliert und an die nach der Bundestagswahl im September zu bildende neue Bundesregierung gerichtet.[299] Dazu gehört die Forderung, die Informationsfreiheit in die Verfassungen aufzunehmen und – zur Vermeidung von „Rechtszersplitterung" – Informationszugangsansprüche in verschiedenen Gesetzen in nur einem Gesetz zusammenzufassen und diese zu Transparenzgesetzen weiterzuentwickeln.

297 Entschließung vom 24. April 2017: „Open Data: Gesetzentwurf der Bundesregierung greift zu kurz!", www.datenschutz.rlp.de/de/service/Infothek/entschliessungen-der-informationsfreiheitskonferenz

298 Entschließung vom 13. Juni 2017: „Mit Transparenz gegen ‚Fake-News'", www.datenschutz.rlp.de/de/service/Infothek/entschliessungen-der-informationsfreiheitskonferenz

299 www.datenschutz-berlin.de/national.html

## 15.2 Informationsfreiheit in Berlin

### 15.2.1 Verweigerungshaltung bei der Senatsverwaltung für Finanzen

Aus der Praxis

Ein Bürger beantragte bei der Senatsverwaltung für Finanzen die Bekanntgabe der sog. AO-Kartei Berlin Vollstreckung (VO-Kartei). Dabei handelt es sich um Anordnungen der Steuerverwaltung für die Durchführung von Verwaltungsvollstreckungsmaßnahmen in den Finanzämtern. Nach der Mitteilung der Senatsverwaltung für Finanzen, dass die Kartei aus ca. 3000 Dateien bestehe und für den Informationszugang mit einer Gebühr von 1.500 Euro zu rechnen sei, beschränkte der Petent seinen Antrag auf die Bekanntgabe der letzten der Kartei zugefügten Datei. Diesen Antrag wies die Senatsverwaltung für Finanzen ebenso zurück wie den hiergegen erhobenen Widerspruch. Zur Begründung wurde insbesondere angeführt, dass die VO-Kartei Anordnungen für die Durchführung bestimmter Verwaltungsvollstreckungsmaßnahmen unterschiedlicher Fallgestaltungen enthalte, wodurch der gesetzliche Auftrag der Beitreibung von Rückständen gewährleistet werde. Diese Regelungen seien deshalb nur für den Dienstgebrauch. Eine Veröffentlichung von Inhalten der VO-Kartei würde Vollstreckungsschuldnern ermöglichen, sich auf bestimmte Verwaltungsmaßnahmen zur Vollstreckung einzustellen und eine erfolgreiche Beitreibung zu vereiteln. Damit wäre die gesetzliche Aufgabenerfüllung gefährdet. Zur Begründung dieser Auffassung berief sich die Senatsverwaltung auf § 9 Abs. 1 IFG.

Nach der angeführten Vorschrift besteht das Recht auf Akteneinsicht oder Aktenauskunft nicht, soweit und solange durch das vorzeitige Bekanntwerden des Akteninhalts der Erfolg bevorstehender behördlicher Maßnahmen, insbesondere von Überwachungs- und Aufsichtsmaßnahmen, ordnungsbehördlichen Anordnungen und Maßnahmen der Verwaltungsvollstreckung, vereitelt wird oder ein vorzeitiges Bekanntwerden des Akteninhalts nach der besonderen Art der Verwaltungstätigkeit mit einer ordnungsgemäßen Aufgabenerfüllung unvereinbar ist. Sowohl der Wortlaut („soweit und solange“) als auch die in § 9 Abs. 2 IFG vorgesehene Befristung der Verweigerung auf bis zu drei Monate sprechen gegen einen generellen Charakter der Regelung, sodass der pauschale Hinweis der Finanzverwaltung auf

die Gefährdung der Aufgabenerfüllung bei Bekanntgabe der Datei nicht greifen konnte. Vielmehr müssen die gesetzlichen Voraussetzungen im Einzelfall, also in Bezug auf eine konkrete Vollstreckungsmaßnahme erfüllt sein.

Das aber war hier nicht der Fall. Aus welchem Grund die AO-Kartei Berlin-Vollstreckung „bundeseinheitlich abgestimmt" und deshalb mangels alleiniger Verfügungsbefugnis ohne Zustimmung der anderen Landesverwaltungen nicht zugänglich gemacht werden dürfte,[300] wurde nicht weiter begründet. Der Bürger hat angekündigt, die Auffassungen der Senatsverwaltung für Finanzen vom Verwaltungsgericht Berlin klären zu lassen.

Die gesetzlichen Ausnahmetatbestände im Berliner Informationsfreiheitsgesetz sind eng auszulegen. Deshalb ist die generelle Berufung auf einen Ablehnungsgrund wie § 9 Abs. 1 IFG – ohne Berücksichtigung der Umstände des Einzelfalls – unzulässig.

## 15.2.2 Kein Informationszugang bei der BIM – leider!

Erneut erreichten uns Beschwerden, weil die Berliner Immobilien Management GmbH (BIM) den Informationszugang zu dort vorhandenen Unterlagen abgelehnt hatte. In einem Fall ging es um undurchsichtige Mietverhältnisse bei der Nutzung des Palais am Festungsgraben, in einem anderen um eine vermutete Vertragsverletzung wegen baulicher Veränderungen auf einem Zehlendorfer Grundstück.



In beiden Fällen mussten wir den Petenten mitteilen, dass die BIM, obwohl sie eine landeseigene Gesellschaft ist, nicht dem Berliner Informationsfreiheitsgesetz unterfällt. Denn dieses Gesetz regelt die Informationsrechte gegenüber den Behörden und sonstigen öffentlichen Stellen (insbesondere den nicht rechtsfähigen Anstalten, Krankenhausbetrieben, Eigenbetrieben und Gerichten) des Landes Berlin, den landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und gegenüber Privaten, die mit der Ausübung hoheitlicher Befugnisse betraut sind (öffentliche Stellen).[301] Bei der BIM handelt es sich je-

300 § 10 Abs. 3 Nr. 2 IFG
301 § 2 Abs. 1 Satz 1 IFG

doch weder um eine Behörde noch um eine sonstige öffentliche Stelle des Landes Berlin, sondern um eine juristische Person des Privatrechts. Auch ist die BIM nicht mit der Ausübung hoheitlicher Befugnisse betraut. Vielmehr ist sie nur für die Vermietung, Bewirtschaftung, Optimierung und den Verkauf der landeseigenen Grundstücke zuständig und wird insoweit rein privatrechtlich tätig. An dieser Rechtslage ändert auch der Umstand nichts, dass es sich bei der BIM um ein landeseigenes Unternehmen handelt, denn das Informationsfreiheitsgesetz trifft keine Sonderregelungen für landeseigene Unternehmen. Diese unterfallen also selbst dann nicht diesem Gesetz, wenn sie sich vollständig in der Hand des Landes Berlin befinden und alle unternehmerischen Entscheidungen gänzlich vom Land Berlin getroffen werden.

Hierbei handelt es sich um eine gesetzliche Regelungslücke, die wir in der Vergangenheit stets kritisiert haben.[302] Auch die Konferenz der Informationsfreiheitsbeauftragten in Deutschland hatte moniert, dass durch Verlagerung von öffentlichen Aufgaben auf Private eine Flucht ins Privatrecht stattfindet, die es zu vermeiden gilt.[303] Unsere Bestrebungen, eine entsprechende Anpassung des Berliner Informationsfreiheitsgesetzes zu erreichen, waren bislang erfolglos.[304] Auch vor dem Hintergrund weiterer Absichten des Landes Berlin, öffentliche Aufgaben wie z. B. die Schulsanierungen auf juristische Personen des Privatrechts zu übertragen, sollte der Anwendungsbereich dieses Gesetzes auf (mehrheitlich) landeseigene Unternehmen erweitert werden.

Dass die Zusammenarbeit von Staat und Privatwirtschaft die Informationsfreiheit nicht gefährden darf, hat auch die 10. Internationale Konferenz der Informationsfreiheitsbeauftragten in Manchester in ihrer jüngsten Entschließung herausgestellt.[305] Informationsfreiheitsgesetze seien weiterzuentwickeln, um auch bei der Vergabe von öffentlichen Dienstleistungen an Unternehmen der Privatwirtschaft

302 JB 2011, 13.3

303 Entschließung vom 17. Juni 2014: „Keine Flucht vor der Informationsfreiheit ins Privatrecht!", siehe Dokumentenband 2014, S. 147

304 Inhaltsprotokoll der 18. Sitzung des Ausschusses für Digitale Verwaltung, Datenschutz und Informationsfreiheit am 10. Dezember 2012, TOP 3b), S. 12ff, abrufbar unter http://www.parlament-berlin.de/ados/17/itdat/protokoll/it17-018-ip.pdf

305 Entschließung vom 20./21. September 2017: „Right of access to information and accountability of public services", abrufbar unter www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2017/16_ICIC_Manchester.html

die staatliche Rechenschaftspflicht über öffentliche Mittel zu gewährleisten. Eine neue Arbeitsgruppe soll Beispiele für angemessenen Informationszugang in diesen Bereichen zusammentragen.

Die Flucht ins Privatrecht führt dazu, dass – ausgerechnet in Bezug auf kostenträchtige öffentliche Aufgaben – die eigentlich bestehende Informationspflicht des Staates zulasten der Steuerzahlenden eingeschränkt wird.

### 15.2.3 Unterlagen zu gerichtlichen Verfahren der Ausländerbehörde



Ein Bürger beschwerte sich darüber, dass die Ausländerbehörde im Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) den Informationszugang zu behördeneigenen Prozessakten über ein abgeschlossenes verwaltungsgerichtliches Verfahren abgelehnt habe. Gegenstand des über zwei Instanzen geführten Prozesses war die Frage, ob den Eltern eines Flüchtlingskindes in Berlin ein Visum zur Einreise in die Bundesrepublik zwecks Familienzusammenführung erteilt werden muss. Das Informationsinteresse des Antragstellers war allein darauf gerichtet, zu erfahren, wie die Koalitionsvereinbarung des Senats, das Aufenthaltsgesetz möglichst großzügig im humanitären Sinne anzuwenden, in der Praxis umgesetzt wird. An personenbezogenen Daten war ihm nicht gelegen.

Die Ausländerbehörde hat den Antrag vollständig abgelehnt, maßgeblich unter Berufung darauf, dass der Versagungsgrund des § 10 Abs. 4 IFG (Schutz des behördlichen Entscheidungsprozesses) der Einsichtnahme in die Prozessakten entgegenstehe. Angesichts der übrigen Erwägungen zur Auslegung des Berliner Informationsfreiheitsgesetzes, z. B. zu unmöglichen Teilanonymisierungen der Akten, sahen wir uns zu einer Ortsprüfung veranlasst. Bei dem ausführlichen Gespräch und nach Sichtung der Prozessakten zu beiden Instanzen mit insgesamt ca. 100 Seiten haben wir folgende Hinweise zur Erstellung des Widerspruchsbescheids gegeben: Prozessakten der Ausländerbehörde sind nicht von vornherein vom Informationszugang durch Dritte ausgenommen.[306] Die Daten von Amtsträ-

306 § 9 IFG

gern sind nicht geheimhaltungsbedürftig,[307] auch nicht die Namen der beteiligten Rechtsanwältinnen,[308] wohl aber deren Kontodaten, die zu schwärzen sind. Die Namen der Richter sind bereits mit den Urteilen im Internet offengelegt und daher ebenfalls nicht zu schwärzen. Sofern in den Akten Unterlagen von Bundesbehörden wie dem Auswärtigen Amt enthalten sind, ist deren Zustimmung zur Offenlegung einzuholen.[309] Beim Schutz des behördlichen Entscheidungsprozesses nach § 10 Abs. 4 IFG ist die ständige verwaltungsgerichtliche Rechtsprechung zu beachten. Danach ist nur der eigentliche Vorgang der behördlichen Entscheidungsfindung, d. h. die Besprechung, Beratschlagung und Abwägung, mithin der eigentliche Vorgang des Überlegens geschützt, nicht aber die Tatsachengrundlage, die Grundlagen der Willensbildung und das Ergebnis der Willensbildung.[310] Nach § 17 Abs. 4 IFG sind die Vorschriften des Sozialgesetzbuchs VIII über den Schutz von Sozialdaten vorrangig zu beachten, diese also – unter Umständen in einzelnen Absätzen und Sätzen – zu schwärzen.

Hinsichtlich des Verfahrens haben wir empfohlen, die beiden Vorgänge, die uns bei der Ortsprüfung als Ausdruck aus der elektronischen Akte vorgelegt wurden, zu paginieren und auf einem Vorblatt die nicht offenzulegenden Seiten bzw. Absätze oder Sätze mit dem jeweiligen Ausschlussgrund zu benennen. Das LABO hat auf dieser Grundlage den Antrag auf Akteneinsicht erneut geprüft und ihm schließlich unter Aufhebung des ursprünglichen Bescheides stattgegeben.

In diesem erfreulichen Fall wurden alle unsere Empfehlungen umgesetzt.

## 15.2.4 Feuerstättenschau im Bezirk Mitte

Ein Bürger beschwerte sich darüber, dass der vom Bezirksamt Mitte beauftragte Schornsteinfeger die Einsichtnahme in das Ergebnis der Feuerstättenschau abgelehnt habe. Begründet habe er dies damit, dass die Einsicht in die Hausakten nur dem Grundstückseigentümer gemäß Schornsteinfeger-Handwerksgesetz vorbe-



307 § 6 Abs. 2 Satz 1 Ziff. 2 IFG
308 § 6 Abs. 2 Satz 1 Ziff. 1a IFG
309 § 10 Abs. 3 Nr. 2 IFG
310 VG Berlin, Urteil vom 5. Mai 2011 – 2 K 132.10

halten sei. Der Petent meinte, der Informationsanspruch ergebe sich aus dem Berliner Informationsfreiheitsgesetz (IFG).

Nach § 14 a Abs. 1 Satz 1 Schornsteinfeger-Handwerksgesetz (SchfHwG) ist der Feuerstättenbescheid gegenüber der Eigentümerin oder dem Eigentümer zu erlassen. Es bestand kein Anspruch auf Herausgabe der begehrten Informationen auf der Grundlage des IFG. Nach diesem Gesetz hat jeder Mensch zwar grundsätzlich einen Anspruch auf (u. U. gebührenpflichtige) Auskunft oder Einsicht in die bei öffentlichen Stellen vorhandenen Akten.[311] Da Bezirksschornsteinfeger nach dem Schornsteinfeger-Handwerksgesetz hoheitlich tätig sind, gelten auch sie als öffentliche Stellen im Sinne von. § 2 Abs. 1 Satz 1 IFG und unterliegen damit grundsätzlich dem Anwendungsbereich des Gesetzes. Allerdings sieht das IFG auch vor, dass auf Bundesrecht beruhende Geheimhaltungspflichten unberührt bleiben[312] und daher vorrangig zu beachten sind. Solche Pflichten sind in § 19 Abs. 5 SchfHwG normiert. Danach dürfen personenbezogene Daten aus dem sog. Kehrbuch, zu denen auch Datum und Ergebnis der letzten beiden Feuerstättenschauen zählen,[313] unter engen Voraussetzungen – u. a. bei Vorliegen eines rechtlichen Interesses – an nichtöffentliche Stellen (also auch an Privatpersonen) übermittelt werden. Insofern war hier kein Raum für den voraussetzungslosen „Jedermanns-Anspruch" nach dem IFG.

Vor diesem Hintergrund haben wir dem Petenten empfohlen, dass er sich an seine Hausverwaltung wendet, bei der er einen Anspruch auf (gebührenfreie) Selbstauskunft auf der Grundlage des Bundesdatenschutzgesetzes geltend machen kann.[314] Seine personenbezogenen Daten dürften in dem Feuerstättenbescheid wenigstens insoweit enthalten sein, als die Wohnlage innerhalb des Hauses verzeichnet wird und zwecks Erreichbarkeit und Identifizierbarkeit dort auch der Name angegeben sein dürfte.

311 § 3 IFG
312 § 17 Abs. 4 IFG
313 § 19 Abs. 1 Satz 1 Nr. 4 SchfHwG
314 § 34 BDSG

Spezialgesetzliche Informationsansprüche sind gegenüber dem Informationsfreiheitsgesetz vorrangig. Ansprüche nach Datenschutzrecht sind für die Betroffenen günstiger als nach dem Informationsfreiheitsgesetz, da sie gebührenfrei sind.

# 16 Aus der Dienststelle

## 16.1 Entwicklungen

Der Berichtszeitraum stand – wie nicht anders zu erwarten – ganz im Fokus der Vorbereitungen auf die zum 25. Mai 2018 wirksam werdende neue EU-Datenschutz-Grundverordnung (DS-GVO). Da die Umsetzung der DS-GVO in die (Rechts-) Praxis in vielen Bereichen zum Teil sehr komplexe praktische und rechtliche Fragen aufwirft, waren intensive Abstimmungsprozesse zwischen den Datenschutzgremien auf Landes-, Bundes- und europäischer Ebene erforderlich. Um die berlinspezifischen Aspekte einzubringen, haben wir uns daran intensiv beteiligt und dazu beigetragen, Lösungen zu entwickeln. Die zeit- und arbeitsintensive Vor- und Nachbereitung sowie die Teilnahme an den nationalen (z. B. im Rahmen der DSK) und europäischen Sitzungen (z. B. in diversen Subgroups[315] der Artikel 29-Gruppe) wurde sowohl von der Leitung als auch von den Mitarbeiterinnen und Mitarbeitern neben dem „Alltagsgeschäft" geleistet. Dies hat die Dienststelle allgemein und die Dienstkräfte im Besonderen an die Grenzen ihrer (Arbeits-)Belastung gebracht.

Das Thema „Datenschutz-Grundverordnung" ist – nicht zuletzt unter dem Zeitdruck der Fristsetzung bis zum 25. Mai 2018 – mittlerweile auch in den Berliner Behörden und Unternehmen angekommen. Der große Bedarf an Informationen über die DS-GVO zeigt sich u. a. daran, dass unser Angebot von Sprechstunden für Start-Up-Unternehmen auf sehr große Resonanz stößt. Entsprechende Anfragen, aber auch die Beratungsersuchen aus anderen Bereichen der Wirtschaft, sind kaum zu bewältigen.

Die Auswirkungen der DS-GVO auf die internen Arbeitsprozesse der Dienststelle wurden von uns in regelmäßigen Sitzungen (Jour-Fix-Runden) analysiert und diskutiert. Konzepte und geeignete Instrumente zur Umsetzung der DS-GVO in unserer Dienststelle wurden entwickelt, dies reichte von der Neukonzeption von Zuständigkeiten bis hin zur Ausarbeitung von Formularen für eine möglichst leicht zugängliche Formulierung von Bürgereingaben im Internet. Die Optimierung der

315 Vorbereitende Arbeitsgruppen der Art. 29-Gruppe

Entscheidungsprozesse, die mit der Einführung einer Referatsstruktur bereits im vergangenen Jahr begann, hat die Entwicklung und Implementierung der neuen internen Vorgaben zur Umsetzung der DS-GVO erheblich erleichtert.

Die Presse- und Öffentlichkeitsarbeit sowie die Büroleitung der Berliner Beauftragten für Datenschutz und Informationsfreiheit wurden umorganisiert. Die Bildung einer „Servicestelle für Presse- und Gremienarbeit" hat dazu beigetragen, dass Themen, die für die Umsetzung der DS-GVO von besonderer öffentlicher Bedeutung sind, aktiv und zeitnah an interessierte Multiplikatoren transportiert werden können. In diesem Kontext steht auch die Überarbeitung unserer Homepage (www.datenschutz-berlin.de), die zum Abschluss gebracht werden konnte. Im neuen, modernen und übersichtlichen Layout bietet das Programm aktuelle Informationen rund um das Thema „Datenschutz und Informationsfreiheit". Es richtet sich vorrangig an die Bürgerinnen und Bürger in Berlin; aber auch dem Datenschutz in Wirtschaft und Verwaltung ist ein Schwerpunkt zugeordnet.

Im Rahmen der Vorbereitung auf die DS-GVO wurde sehr schnell deutlich, dass sich die Stellung, die Aufgaben und die Befugnisse der Berliner Beauftragten für Datenschutz und Informationsfreiheit als Berliner Aufsichtsbehörde für den Datenschutz grundlegend ändern werden. Um die Verarbeitung von Daten bei den Verantwortlichen wirkungsvoll zu kontrollieren, erhält die Behörde neue bzw. erweiterte Kontroll-, Anordnungs- und Sanktionsbefugnisse. Auch der Charakter der Behörde wird sich dadurch deutlich verändern. Sie wird von einer Petitionsbehörde zu einer echten Vollzugsbehörde. Um die europaweite Einheitlichkeit des Vollzugs der Verordnung zu erreichen, wird die Berliner Beauftragte für Datenschutz und Informationsfreiheit zudem durch ein kompliziertes Geflecht von Regelungen in der DS-GVO unmittelbar zu einer arbeitsintensiven unionsweiten Kooperation mit den anderen (nationalen und europäischen) Aufsichtsbehörden und dem neuen Europäischen Datenschutzausschuss (EDSA) verpflichtet. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit wird von einer Opportunitätsbehörde eines Bundeslandes zu einer Exekutivbehörde der Europäischen Union. Der grundsätzliche Wandel von einer Kontroll- und Beratungsstelle in eine mit weitreichenden Weisungs- und Verbotsbefugnissen ausgestattete Aufsichtsbehörde ist für die Berliner Beauftragte für Datenschutz und Informationsfreiheit nur möglich, wenn dafür die erforderlichen strukturellen und personellen Voraussetzungen geschaffen werden.

Die Bearbeitung von Eingaben, Beratungsersuchen von Behörden und Unternehmen, Prüfungen von Amts wegen und die Erledigung sonstiger Aufgaben war für die Dienststelle mit den vorhandenen (Personal-) Ressourcen bisher schon kaum noch zu bewältigen. Durch die neuen europäischen Regelungen zum Datenschutz verschärft sich die Situation extrem. Fest steht, dass die Umsetzung und Anwendung der DS-GVO – die ihre verbindliche Gültigkeit am 25. Mai 2018 erlangt – für die Dienststelle der Berliner Beauftragten für Datenschutz und Informationsfreiheit nur mit einem erheblichen Zuwachs an Personal und durch nachhaltige Veränderungen in der Struktur zu realisieren sein wird.

Neben der Einleitung notwendiger Strukturveränderungen in unserer Dienststelle haben wir daher für den Haushalt 2018/2019 einen Stellenmehrbedarf von 15 Stellen (davon 10 Stellen des höheren Dienstes und 4 Stellen des gehobenen Dienstes) sowie Stellenhebungen im höheren Dienst angemeldet – all dies im Zusammenhang mit einer insgesamt für notwendig erachteten Neujustierung der Behörde in der Behördenstruktur des Landes Berlin. Bewilligt wurden davon lediglich 5 Stellen des höheren und die 4 Stellen des gehobenen Dienstes sowie die Stelle einer Fremdsprachensekretärin. Ob die großen Herausforderungen, vor denen der Datenschutz im Land Berlin im Allgemeinen und die Dienststelle der Berliner Beauftragten für Datenschutz und Informationsfreiheit im Besonderen durch die Einführung der DS-GVO steht, mit derart begrenzten Personalressourcen bewältigt werden kann, ist zweifelhaft.

## 16.2 Zusammenarbeit mit dem Abgeordnetenhaus von Berlin

Der Unterausschuss für Datenschutz, Informationsfreiheit und zur Umsetzung von Art. 13 Abs. 6 Grundgesetz sowie § 25 Abs. 10 Allgemeines Sicherheits- und Ordnungsgesetz (UADat/G13)[316] sowie – nach Einrichtung eines eigenen Fachausschusses anstelle des Unterausschusses – der Ausschuss für Kommunikationstechnologie und Datenschutz (KTDat) tagten in insgesamt neun Sitzungen,

316 Aufgelöst am 4. Mai 2017, die Aufgaben wurden von dem neu eingesetzten Ausschuss für Kommunikationstechnologie und Datenschutz übernommen

in denen die Berliner Beauftragte für Datenschutz und Informationsfreiheit zu verschiedenen Themen Empfehlungen und Vorschläge abgeben konnte. Ein besonderer Fokus lag auf der Umsetzung der Datenschutz-Grundverordnung[317]. Darüber hinaus waren die IT-Sicherheit und der Datenschutz bei der Charité[318], das Service-Konto Berlin[319] sowie die Übermittlung von Meldedaten an den Beitragsservice[320] Gegenstand unserer Befassung.

## 16.3 Zusammenarbeit mit anderen Stellen

Die **Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)** tagte am 29./30. März in Göttingen und am 8./9. November in Oldenburg und fasste zahlreiche Entschließungen zu aktuellen Fragen des Datenschutzes.[321] Aufgrund notwendiger Beratungen zur bevorstehenden EU-Datenschutz-Grundverordnung und der Vorbereitung eines darauf abgestimmten neuen Bundesdatenschutzgesetzes fanden darüber hinaus am 24. Januar, 11. Mai, 21. Juni und 14. September in Hannover sowie am 24. Oktober in Wiesbaden insgesamt fünf Sondersitzungen der DSK statt.

Der **Düsseldorfer Kreis**, in dem die Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich zusammenarbeiten, tagte am 6./7. März und 12./13. Oktober in Düsseldorf.

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)** tagte am 13. Juni sowie am 14. November in Mainz und fasste Entschließungen zu Grundsatzpositionen zur Informationsfreiheit sowie zum Vorgehen gegen „Fake-News" durch Transparenz.[322]

317 Wortprotokoll UADat/G13 18/1 vom 13. Februar 2017, S. 2 ff.; Inhaltsprotokoll UADat/G13 18/2 vom 6. März 2017, S. 1 ff.; Inhaltsprotokoll KTDat 18/2 vom 3. Juli 2017, S. 2 ff.; Inhaltsprotokoll KTDat 18/6 vom 11. Dezember 2017, S. 2 f.

318 Wortprotokoll UADat/G13 18/3 vom 3. April 2017, S. 2 ff.

319 Siehe 2.1 und Inhaltsprotokoll KTDat 18/2 vom 3. Juli 2017, S. 12 ff.

320 Inhaltsprotokoll KTDat 18/2 vom 3. Juli 2017, S. 6 ff.

321 https://www.datenschutz-berlin.de/beschluesse.html

322 https://www.datenschutz-berlin.de/pdf/informationsfreiheit/BlnBDI_Grundsatzpositionen_der_Landesbeauftragten_Informationsfreiheit.pdf und https://www.datenschutz-berlin.de/pdf/pressemitteilungen/2017/14062017_Fake_News.pdf

Die **Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre (ICDPPC)** fand vom 25. bis 29. September in Hong Kong statt und fasste Entschließungen zum Datenschutz in automatisierten und vernetzten Fahrzeugen, zur Zusammenarbeit zwischen Datenschutz- und Verbraucherschutzbehörden sowie zur internationalen Zusammenarbeit bei der Durchsetzung von aufsichtsrechtlichen Maßnahmen.[323] Unser dort vorgetragener Bericht über die Arbeitsergebnisse sowie über die notwendige Umorganisation der sog. Berlin Group stieß auf großes Interesse und wird voraussichtlich zu einer intensivierten Zusammenarbeit auf internationaler Ebene führen.

Die **„Berlin Group" (IWGDPT)** tagte unter unserem Vorsitz am 24./25. April in Washington D.C. sowie am 27./28. November in Paris.[324]

Die **Internationale Konferenz der Informationsfreiheitsbeauftragten (ICIC)** tagte vom 19. bis 21. September in Manchester und fasste eine Entschließung zum Informationszugang gegenüber nicht öffentlichen Stellen, die öffentliche Aufgaben wahrnehmen.[325]

Wie schon in den Vorjahren besuchten uns verschiedene ausländische Delegationen, die sich mit uns zu politischen, rechtlichen und praktischen Fragen des Datenschutzes und der Informationsfreiheit austauschten. Hierzu gehörten neben Vertretern der israelischen Datenschutzaufsichtsbehörde[326] die für Informationsfreiheit zuständige aserbaidschanische Kommissarin für Menschenrechte sowie der Justizminister von Sambia.

323 https://icdppc.org/document-archive/adopted-resolutions/
324 Zu den Ergebnissen siehe 13.6
325 https://icic2017open.org/resolution/
326 Siehe 16.3.1

## 16.4 Besuch der israelischen Aufsichtsbehörde in Berlin

Der israelische Datenschutzbeauftragte und seine Abteilungsleiterinnen und Abteilungsleiter kamen zu einem einwöchigen Studienbesuch im Rahmen eines Programms der Europäischen Kommission in unsere Dienststelle. Ziel des Programms TAIEX[327] ist es, Informationen über europäisches Recht, europäische Politik und europäische Standards mit Nicht-EU-Ländern auszutauschen.

Per Beschluss vom 31. Januar 2011 hat die EU-Kommission festgestellt, dass der Staat Israel über ein angemessenes Schutzniveau für die Übermittlung personenbezogener Daten aus der Europäischen Union verfügt. Auch ein Drittland wie Israel muss sich auf die neuen Vorgaben der Datenschutz-Grundverordnung vorbereiten. Die israelischen Kollegen erhielten Gelegenheit, sich darüber zu informieren, wie sich in Deutschland Aufsichtsbehörden, Verwaltungen und Wirtschaft auf den 25. Mai 2018 (Wirksamwerden der Datenschutz-Grundverordnung) vorbereiten. Wie wir ist die israelische Aufsichtsbehörde der Auffassung, dass im Zeitalter der weltweiten Digitalisierung ein enger Austausch unter den Datenschutzbehörden erforderlich ist. Insgesamt wurden 24 Vorträge gehalten, in denen es u. a. um folgende Themen ging: Vorbereitung auf die Datenschutz-Grundverordnung, Rechtsdurchsetzung und Sanktionen, Aufbau unserer Servicestelle Bürgereingaben, Unabhängigkeit der Aufsichtsbehörde, Arbeit der Datenschutzstiftung und des Verbraucherschutzes für den Datenschutz sowie Fragen des Privacy Shields. Zum Abschluss des Besuchs fand ein Workshop statt, in dem Gemeinsamkeiten und Unterschiede des israelischen und europäischen Datenschutzrechts analysiert wurden.

Israel wird seine Aufsichtsbehörde für den Datenschutz und die datenschutzrechtlichen Rahmenbedingungen entsprechend den neuen Herausforderungen (EU-Datenschutz-Grundverordnung, weltweite Digitalisierung) anpassen. Wir konnten hierzu einige hilfreiche Anregungen geben.

327 Technical Assistance and Information Exchange

# 16.5 Presse- und Öffentlichkeitsarbeit

## 16.5.1 Pressearbeit

Im Jahr 2017 haben wir unsere Pressestelle neu strukturiert, um eine höhere Präsenz des Themas Datenschutz in der Öffentlichkeit zu erreichen und dessen Wichtigkeit für jede und jeden Einzelnen deutlich zu machen. Neben dem Ziel, möglichst viele Presseanfragen fundiert zu beantworten, möchten wir mit eigenen Pressemitteilungen künftig auch verstärkt aktiv über die Themen berichten, die uns wichtig sind.

In diesem Jahr haben wir 109 Presseanfragen beantwortet. Von besonderem Interesse für die Medien waren das Pilotprojekt zur biometrischen Gesichtserkennung, das im Sommer am Berliner S-Bahnhof Südkreuz gestartet ist, sowie die Wahlkampf-App einer Partei im Bundestagswahlkampf. Darüber hinaus waren wir jedoch auch mit vielen Anfragen zu alltäglichen Themen wie dem Umgang mit Kundendaten durch Essenslieferanten oder der Zulässigkeit von Videokameras in Umkleidekabinen befasst. In einigen Fällen nahmen wir Anfragen von Medienvertretern auch zum Anlass, um Datenverarbeitungsvorgänge aufsichtsrechtlich zu überprüfen, wie z. B. die Datenerhebung durch eine Partei im Rahmen der Akkreditierung von Journalisten für ihren Bundesparteitag.

Folgende Pressemitteilungen haben wir in diesem Jahr veröffentlicht:

- Neu ab März 2017: Extra-Sprechstunden für Start-ups ! (24. Februar 2017)
- Jahresbericht 2016 – Einladung zu einem Pressegespräch (31. März 2017)
- Biometrische Gesichtserkennung – eine Technik ohne Zukunft (23. Februar 2017)
- Arbeitspapier zu Biometrie in der Online-Authentifizierung verabschiedet (14. März 2017)
- Bundestagswahl und Volksentscheid am 24. September 2017 – Nur ein rechtzeitiger Widerspruch verhindert unerwünschte Werbung (22. Mai 2017)
- Beschneidung der Kontrollbefugnisse der Datenschutzaufsichtsbehörden nicht hinnehmbar! (4. Mai 2017)

- Bundestag beschließt schwere Grundrechtseingriffe im Hauruckverfahren (23. Juni 2017)
- Biometrische Gesichtserkennung – große Risiken für Individuen und Gesellschaft (31. Juli 2017)
- EU-US Privacy Shield: Informationen sowie Beschwerdeformulare für Betroffene veröffentlicht (14. August 2017)
- Veröffentlichte Arbeitspapiere „E-Learning Plattformen“ und „Internationale Grundsätze zur Regulierung der nachrichtendienstlichen Informationsbeschaffung“ (17. August 2017)
- Weil wir Datenschutz lieben: Anstehende Aufräumarbeiten bei der BVG (29. August 2017)
- Identitätsdiebstahl darf nicht als allgemeines Geschäftsrisiko hingenommen werden (8. September 2017)
- Bündnis für mehr Videoaufklärung – 10 Gründe, warum Sie nicht unterschreiben sollten (13. September 2017)

Alle Pressemitteilungen sind auf unserer Webseite unter https://www.datenschutz-berlin.de/pressemitteilungen.html abrufbar.

## 16.5.2 Öffentlichkeitsarbeit

### Neues Design/neue Webseite

Erklärtes Ziel war es, die Modernisierung und Umgestaltung der Außendarstellung der Dienststelle der Berliner Beauftragten für Datenschutz und Informationsfreiheit in diesem Jahr weitgehend umzusetzen. Die Ergebnisse können sich sehen lassen. Unsere Schreiben präsentieren sich im neuen modernen Design, wir haben neugestaltete Plakate und Aufsteller für Veranstaltungen und vor allem unsere Webseite wurde komplett überarbeitet. Auf das Ergebnis sind wir sehr stolz und wir haben bereits viel positive Resonanz für die neue Webseite bekommen. Sie sei modern, ansprechend, informativ und genüge allen Ansprüchen für eine zeitgemäße Präsentation und Benutzung.

### Veröffentlichungen

Neben dem Tätigkeitsbericht des vergangenen Berichtszeitraums und dem Band mit den Entschließungen der nationalen, europäischen und internationalen Datenschutzgremien haben wir zwei Flyer im neuen Design gestaltet und drucken lassen.

Der Flyer „Datenschutz in Berlin" hilft den Betroffenen, die richtigen Ansprechpartnerinnen oder -partner zu finden, wenn sie eine allgemeine Frage zum Datenschutz oder ein konkretes Problem im Umgang mit ihren personenbezogenen Daten haben. Die richtige Vorgehensweise wird dabei ausführlich beschrieben.

Der Flyer „EU-Datenschutz-Grundverordnung – Ihre Rechte" informiert die Bürgerinnen und Bürger über ihre Rechte bei der Speicherung und Verarbeitung der personenbezogenen Daten und stellt die wichtigsten Neuerungen vor.

Das Bürgerbündnis für mehr Videoaufklärung und mehr Datenschutz hat einen Gesetzesentwurf für ein „Artikel-Gesetz für mehr Sicherheit und mehr Datenschutz in Berlin" vorgestellt, über den in einem Volksbegehren entschieden werden soll. Wir raten davon ab, die Initiative zu unterstützen, und haben unseren Standpunkt im Rahmen der Presseerklärung „Bündnis für mehr Videoaufklärung – 10 Gründe, warum Sie nicht unterschreiben sollten" veröffentlicht.

Gemeinsam mit der Senatsverwaltung für Bildung, Jugend und Familie haben wir eine Broschüre unter dem Titel „Datenschutz bei Bild-, Ton- und Videoaufnahmen – Was ist in der Kindertageseinrichtung zu beachten?" herausgegeben.[328]

Aufgrund des unmittelbar bevorstehenden Wirksamwerdens der Europäischen Datenschutz-Grundverordnung (DS-GVO) haben sich die Aufsichtsbehörden von Bund und Ländern das ganze Jahr über sehr intensiv mit den kommenden neuen Rechtsgrundlagen und deren Anforderungen befasst, um untereinander eine möglichst einheitliche Sichtweise zu entwickeln. Erste Ergebnisse dieses Prozesses sind eine Reihe gemeinsamer Kurzpapiere zu zentralen Rechtsfragen der DS-GVO, die den Bürgerinnen und Bürgern in jeweils einem kurzen Überblick die wichtigsten Rechtsänderungen erläutern sollen. Diese Kurzpapiere werden von

328 Siehe auch 6.5

der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ab sofort veröffentlicht und sind auch auf unserer Webseite abrufbar.[329]

Auch alle übrigen Informationsmaterialien sind auf unserer Webseite abrufbar und teilweise auch in gedruckter Form erhältlich.

Derzeit nicht verfügbar sind beide Broschüren aus der Reihe Berliner Informationsgesetzbuch: Das Berliner Datenschutzgesetz und das Berliner Informationsfreiheitsgesetz. Die Gesetze werden zurzeit novelliert. Mit der Neuauflage der beiden Broschüren ist frühestens Mitte 2018 zu rechnen. Bis dahin sind die Gesetzestexte in der jeweils gültigen Fassung auf unserer Webseite abrufbar.

### Artikelreihe zur DS-GVO im Magazin „Berliner Wirtschaft" der IHK Berlin

Bis zum Inkrafttreten der DS-GVO soll regelmäßig ein Kurzartikel zu den wichtigsten Neuerungen der DSGVO in dem o. g. Magazin erscheinen. Bislang wurden zwei Beiträge veröffentlicht: der Einführungsbeitrag „Countdown für Umsetzung des neuen EU-Rechts läuft" im September, ein weiterer Beitrag „Werben nach europäischem Recht" im November. Der nächste Beitrag „Das neue Recht auf Datenübertragbarkeit (Datenportabilität)" erscheint in der Januar-Ausgabe.

### Veranstaltungen und Vorträge

Die diesjährige zentrale Veranstaltung aus Anlass des 11. Europäischen Datenschutztages wurde auf Einladung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 30. Januar im Abgeordnetenhaus von Berlin durchgeführt. Das Thema lautete „Diktatur der Daten? – Privatsphäre und Selbstbestimmung im Zeitalter von Big Data und Algorithmen".

Am 19. September fand der jährliche Gesundheitstag an der Freien Universität Berlin statt. Das Motto „Die Freie Universität ist mobil (lass uns noch 'ne Runde drehen)" eignete sich angesichts von Fragestellungen zu Gesundheitsapps und sog. Wearables in besonderer Weise als Ausgangspunkt für Informationen zum Datenschutz. Für den Ausstellungsstand der behördlichen Datenschutzbeauftragten der Freien Universität stellten wir eine Auswahl von Broschüren und Werbeartikeln mit Datenschutzbezug zur Verfügung.

329 www.datenschutz-berlin.de/kurzpapiere.html

Im Rahmen der mobilen Vorlesungsreihe der KinderUni Lichtenberg „KUL unterwegs“, einem Angebot für Schülerinnen und Schüler der 3. bis 8. Klassen in Lichtenberg und Buch, bieten wir regelmäßige Veranstaltungen zu den Themenbereichen Neue Medien und Kommunikation an. Derzeit ist ein Referent unserer Behörde dort mit drei Vorlesungen vertreten: „Check: WhatsApp – Möglichkeiten, Gefahren, Alternativen“, „Facebook, Twitter, WhatsApp & Co. – Soziale Netzwerke und Datenschutz“ und „OMG! – Fake News – Erkennen, einordnen, vermeiden“. Die Vorlesungen richten sich grundsätzlich an zwei oder mehr Klassen.[330]

Wie bereits seit mehreren Jahren wirkte eine Mitarbeiterin unserer Behörde auch in diesem Jahr am Schulungsangebot des Sozialpädagogischen Fortbildungsinstituts Berlin-Brandenburg (SFBB) mit, das in seinem Schulungsangebot unter anderem Veranstaltungen für pädagogische Fachkräfte in der Jugendhilfe im Strafverfahren anbietet. Die Kooperation verschiedener Stellen im Jugendstrafverfahren wirft immer wieder Datenschutzprobleme auf. Fragestellungen des Datenschutzes in Bezug auf die Weitergabe personenbezogener Daten sowie auf den Umgang mit der Schweigepflicht beim Zusammenwirken von Jugendhilfe und Polizei, Schule und Justiz sind daher Bestandteil der Fortbildung.

Zahlreiche weitere Vorträge wurden im Berichtszeitraum gehalten. Hier nur eine kleine Auswahl:

- Veranstaltungsreihe der KPMG Rechtsanwaltsgesellschaft mbH zum Thema „Datenschutz-Grundverordnung“; Vortrag „Schwerpunkte des Umsetzungsbedarfs – Kontrolltätigkeit der Aufsichtsbehörden nach der DS-GVO“ am 21. März

- 4. Fachtagung „Medienkompetenz verbindet – Medienbildung in Schule und Jugendarbeit“ am 30. März; Workshop 4 „Datenschutz und Medienkompetenz“

- Symposium der Direktorenkonferenz der Landesmedienanstalten (DLM) zum Thema „Die Werbung ist tot! Es lebe die Werbung! Leitlinien moderner Regulierung für die Vermarktungsmodelle von morgen“ am 23. März; Kurzstatement „Seid smart mit Euren Daten“

330 Ausführlicher zur Medienkompetenz siehe 6.7

- Verbandstag des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V. unter dem Titel „Datenschutz in Europa – Von der Theorie zur Praxis“ am 4. Mai; Vortrag „Wenn die Aufsichtsbehörde klingelt... Datenschutzkontrollen im nicht-öffentlichen Bereich – Die Aufsichtsbehörde als Ansprechpartner der Datenschutzbeauftragten?!“

- 18. Datenschutzkongress 2017 vom EUROFORUM zur Datenschutz-Grundverordnung am 17./18. Mai; Vortrag “In einem Jahr beginnt das neue europäische Datenschutzzeitalter, der Countdown für Gesetzgeber, Wirtschaft, Verwaltung und Aufsichtsbehörden läuft“

- Sitzung der Kommission Arbeit & Soziales des Bundesverbands mittelständische Wirtschaft am 13. Juni; Praxisbericht „Beschäftigtendatenschutz konkret“

- Kinderschutzkonferenz der Region 1/3 des Jugendamtes Treptow-Köpenick „Gelingende Netzwerke“ am 14. Juni; Vortrag zur Netzwerkarbeit im Kinderschutz

- Tagung des Erfa-Kreises der Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) am 7. September; Vortrag „Vorbereitung der Aufsichtsbehörde auf die Datenschutz-Grundverordnung“

- Vortrag auf der Informationsveranstaltung des Landesverbands Haus & Grund Berlin e. V. zum Thema „Datenschutz in Vereinen“ am 14. November

- Veranstaltung der Landesvereinigung Selbsthilfe Berlin e.V. „Pflege 4.0–digitale Versorgungsreform in der Pflege“ am 20. November; Vortrag „Transparenz, Einwirkungsmöglichkeiten, Schutz bei der Datenverarbeitung in der Pflege“

# Anhang

## Rede der Berliner Beauftragten für Datenschutz und Informationsfreiheit am 19. Oktober 2017 im Abgeordnetenhaus von Berlin zum Jahresbericht 2016

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

2016 war in datenschutzrechtlicher Hinsicht ein sehr ereignisreiches Jahr. Geprägt wurde es vor allem durch die Entwicklungen auf europäischer und internationaler Ebene, die jedoch unmittelbare Auswirkungen auf die Bürgerinnen und Bürger Berlins sowie auf die Berliner Wirtschaft haben werden.

Da ist zunächst die europäische Datenschutz-Grundverordnung, die nach vier Jahren zäher Verhandlungen im Mai 2016 in Kraft trat. Durch sie wird erstmals ein komplettes Rechtsgebiet für alle europäischen Mitgliedstaaten verbindlich und im Detail geregelt. Nach einem Übergangszeitraum von zwei Jahren wird sie ab Mai 2018 europaweit unmittelbar anwendbar sein, ohne dass es noch einer nationalen Umsetzung bedürfte. Dies ist ein wirklich epochaler Schritt, der das Grundrecht auf Datenschutz europaweit anerkennt und ihm eine optimale Geltung in einer globalisierten Welt verschaffen soll.

Die neuen Regelungen stärken die Rechte von Bürgerinnen und Bürgern durch erweiterte Auskunfts- und Löschrechte erheblich. Auch für Unternehmen bietet das neue Rechtssystem enorme praktische Vorteile, weil dadurch erstmals einheitliche Wettbewerbsbedingungen für alle im europäischen Raum tätigen Unternehmen geschaffen und einheitliche Ansprechpartner für sie definiert werden. Die Aufsichtsbehörden schließlich erhalten deutlich erweiterte Befugnisse, die einer möglichst effizienten Durchsetzung des Datenschutzes dienen sollen.

Für die Datenschutz-Aufsichtsbehörden hat mit dem Beschluss über die Einführung der Datenschutz-Grundverordnung eine Zeit intensivster Vorbereitungen auf

das neue Rechtssystem begonnen. Neue Verfahren der Zusammenarbeit mussten und müssen entwickelt und vorbereitet werden; das höchst komplizierte Rechtsgebiet muss in all seinen Anforderungen durchdrungen werden, um die notwendigen Vorbereitungen für die sehr komplexen neuen Verfahren treffen zu können.

Diverse Gesetzesanpassungen wurden intensiv begleitet – denn leider war festzustellen, dass auf Bundesebene verschiedene Versuche unternommen wurden, die auf europäischer Ebene gestärkten Datenschutzrechte auf nationaler Ebene wieder einzuschränken, was erhebliche verfassungsrechtliche Fragen aufwirft und Rechtsunsicherheit schafft. Insgesamt setzte zwischen den Datenschutzbehörden sowohl auf nationaler als auch auf europäischer Ebene eine intensive Diskussion um die Auslegung der neuen Regelungen ein, um ab Mai 2018 tatsächlich einigermaßen abgestimmt agieren zu können. Es ist eine riesige Herausforderung!

Zugleich haben wir alles in unserer Kraft Stehende versucht, um unser Beratungsangebot für die Berliner Bürgerinnen und Bürger, die Unternehmen und Verwaltungen zu verstärken. Nur als Beispiel möchte ich in diesem Zusammenhang unsere seit Beginn dieses Jahres regelmäßig stattfindende Start-Up-Sprechstunde hervorheben, in der wir Berliner Gründerinnen und Gründer individuell zu Datenschutzfragen beraten. Dieses Angebot wird sehr gut angenommen und vermittelt uns gleichzeitig einen Einblick in die Schwierigkeiten der Wirtschaftsunternehmen mit den neuen Anforderungen der Datenschutz-Grundverordnung.

Von enormer praktischer Bedeutung für die nationale Wirtschaft war die ebenfalls im Jahr 2016 getroffene Vereinbarung des sog. Privacy Shields zwischen der Europäischen Kommission und den USA. Dieses Abkommen ist datenschutzrechtlich zwar nach wie vor mit Fragezeichen versehen, bietet aber europäischen Unternehmen derzeit einen Rahmen zur Übermittlung personenbezogener Daten an zertifizierte US-Unternehmen. Auf der Webseite meiner Behörde sind detaillierte Informationen über das neue Abkommen zu finden.

Auf lokaler Ebene hatten wir mit einer großen Bandbreite datenschutzrechtlich relevanter Fragen zu tun. Natürlich ging es immer wieder um Fragen des Ausgleichs zwischen innerer Sicherheit und den Freiheitsrechten der Menschen, ob es sich nun um den Einsatz von Videoüberwachung, den Einsatz sogenannter stil-

ler SMS in strafrechtlichen Ermittlungsverfahren oder um das Wirken eines Vereins im Bereich der Deradikalisierung handelte.

Sehr großen Raum hat der Bereich Gesundheitsdatenschutz eingenommen, da nach wie vor erhebliche Mängel im Datenschutzmanagement und in der Datensicherheit sowohl in der öffentlichen Verwaltung als auch in den Krankenhäusern festzustellen sind. Gerade in diesem Bereich geht es aber um höchst sensitive Daten, die besonderen Schutzes bedürfen. Dieser Schutz fordert insbesondere in den großen Krankenhausbetrieben mit ihren komplexen Datenverarbeitungssystemen riesige Anstrengungen, die teilweise noch deutlich intensiviert werden müssen.

Im Übrigen ging es um Themen wie z. B. den Umgang von Wohnungsbaugesellschaften mit Kandidaturen für Mieterräte, die Gestaltung der Arbeit der Kinderambulanzen, die Zulässigkeit der Anforderung amtsärztlicher Diagnosen durch Arbeitgeber und vieles mehr. Fälle wie die Durchführung von Bewerbungsgesprächen über Skype oder der Einsatz von WhatsApp in Schulen zeigen, dass die sich immer weiter entwickelnde Digitalisierung der Gesellschaft auch zu immer neuen datenschutzrechtlichen Problemen führt.

Im Bereich der Informationsfreiheit hat sich ebenfalls vieles getan, seit das Berliner Informationsfreiheitsgesetz im Jahr 1999 in Kraft trat. Damals bedeutete es eine Abkehr vom traditionellen Prinzip des Amtsgeheimnisses. Die Informationsfreiheit hat sich jedoch in diesen vergangenen 18 Jahren stetig weiterentwickelt. Sie ist sozusagen erwachsen geworden.

Das spiegelt sich auch in den Eingaben zu diesem Bereich wider, die mein Haus erreichen. War in den Jahren zuvor noch ein regelmäßiger Anstieg zu verzeichnen, sind die Eingabezahlen im vorigen Jahr erstmals gefallen. Aber auch der Anteil an Eingaben, bei denen wir einen anderen Umgang mit dem Informationsfreiheitsgesetz anmahnen mussten, ist kontinuierlich zurückgegangen. Dies könnte darauf hindeuten, dass der Grundgedanke der Informationsfreiheit in der Verwaltung angekommen ist und auch ernstgenommen wird. Es bleibt abzuwarten, ob die künftige Entwicklung diese Annahme stützen wird.

Dennoch besteht weiterhin Handlungsbedarf. Die gesellschaftliche Entwicklung geht zur Fortentwicklung bestehender Informationsfreiheitsgesetze hin zu Trans-

parenzgesetzen. Mit Verabschiedung des E-Government-Gesetzes im vergangenen Jahr ist Berlin einen Schritt in die richtige Richtung gegangen. Allerdings muss die darin enthaltene Verpflichtung der Verwaltung zur proaktiven Veröffentlichung von Unterlagen noch konkretisiert und mit Leben erfüllt werden.

Meine Damen und Herren, das waren nur einige wenige Themen, mit denen mein Haus sich derzeit befasst. Die notwendigen Anpassungen aufgrund der Datenschutz-Grundverordnung stellen einen riesigen Kraftakt für meine Behörde dar. Ich möchte deshalb die Gelegenheit nutzen, meinen Mitarbeiterinnen und Mitarbeitern ausdrücklich für ihren steten und engagierten Einsatz zu danken, ohne den diese Umstellung nicht möglich wäre.

Vielen Dank für Ihre Aufmerksamkeit!

# Glossar

**2-Faktor-Authentifizierung**

Nachweis der Identität einer Person über zwei der drei folgenden Merkmale:

1. Besitz eines Gerätes, über das ausschließlich diese Person verfügt,
2. Kenntnis eines Geheimnisses (z. B. ein Passwort), das nur ihr bekannt ist,
3. biometrische Charakteristika der Person wie ihren Fingerabdruck.

**Anonym/Pseudonym**

Anonyme Daten können nicht mehr einer Person zugeordnet werden. Bei pseudonymen Daten ist dies einer bestimmten dritten Partei möglich unter vorab festgelegten Bedingungen.

**Art. 29-Gruppe**

Gruppe nach Art. 29 Europäische Datenschutzrichtlinie, die sich aus Vertreterinnen und Vertretern aller europäischen Datenschutzbehörden zusammensetzt. Sie hat beratende Funktion; vornehmlich gegenüber der Europäischen Kommission, aber auch gegenüber anderen Datenverarbeitern innerhalb der Europäischen Union.

**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.

**Cookies**

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.

| | |
|---|---|
| CRO | CRO steht für Clinical Research Organisation (Auftragsforschungsinstitut). Dabei handelt es sich um ein Dienstleistungsunternehmen für die Arzneimittel und Medizinprodukte produzierende Industrie, welches die Forschung und Entwicklung von Arzneimitteln bzw. Medizinprodukten im Zuge der Planung und Durchführung klinischer Studien unterstützt. |
| Double-Opt-In | Nutzende, die sich mit einer E-Mail-Adresse in einem Verteiler eingetragen haben, erhalten durch eine Bestätigungs-E-Mail die Möglichkeit, die Anmeldung zu bestätigen. Erst durch die Bestätigung wird die Anmeldung wirksam. |
| DS-GVO | Europäische Datenschutz-Grundverordnung – Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie 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, wird aber aufgrund einer zweijährigen Übergangsfrist erst am 25. Mai 2018 wirksam. Ab diesem Zeitpunkt ist sie in allen Mitgliedstaaten der Europäischen Union unmittelbar anwendbar. |
| 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 Anwenderinnen und Anwender nicht oder nur mit speziellen Mitteln bzw. Funktionen austauschbar. Firmware ist funktional fest mit der Hardware verbunden; das eine ist ohne das andere nicht nutzbar. |
| Gamification | Von engl. game für „Spiel" bezeichnet man den Einsatz von spieletypischen Elementen zur Motivationssteigerung und Verhaltensänderung bei Anwenderinnen und Anwendern. |
| GovData | Datenprotal für Deutschland, das einen zentralen und einheitlichen inhaltlichen Zugang zu Verwaltungsdaten aus Bund, Ländern und Kommunen bietet, die diese in ihren jeweiligen Open Data-Portalen zugänglich gemacht haben. |
| GPS / GPS-Sender | Global Positioning System; deutsch: Globales Positionsbestimmungssystem. |

| | |
|---|---|
| Hashfunktion | Bei einer kryptografischen Hashfunktion handelt es sich um eine mathematische Berechnungsvorschrift, die aus beliebigen Ausgangsdaten wie beispielsweise einem Dokument oder auch nur einem Wort bzw. einer Telefonnummer einen eindeutigen Prüfwert mit fester Länge berechnet. Diese Berechnung ist nicht umkehrbar – aus den Prüfwerten können die Ausgangsdaten nicht zurückberechnet werden. Bei wiederholter Berechnung mit gleichen Ausgangsdaten ergibt sich jedoch immer der gleiche Prüfwert. |
| Hashwert | Der Hashwert ist das Ergebnis (der Prüfwert) der Anwendung einer [obigen] kryptografischen Hashfunktion. Bei dieser handelt es sich um eine mathematische Berechnungsvorschrift, die aus beliebigen Ausgangsdaten wie beispielsweise einem Dokument oder auch nur einem Wort bzw. einer Telefonnummer einen eindeutigen Hashwert mit fester Länge berechnet. |
| Integrität | Unter der Wahrung der Integrität von Daten versteht man ihren Schutz vor unbeabsichtigtem Verlust oder unbeabsichtigter Verfälschung. |
| 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 (zum One-Stop-Verfahren siehe S. 206) kein Konsens zwischen den beteiligten Aufsichtsbehörden gefunden werden kann, trifft der Europäische Datenschutzausschuss im Rahmen des Kohärenzverfahrens verbindliche Beschlüsse. Darüber hinaus werden im Kohärenzverfahren mit dem Ziel der einheitlichen Anwendung der DS-GVO auch Stellungnahmen des Europäischen Datenschutzausschusses – etwa zur Festlegung von Standard-Datenschutzklauseln – abgestimmt.

**Link**

Verweis oder Sprung zu einem elektronischen Dokument.

**Marktortprinzip**

Die DS-GVO ist anwendbar, sobald ein Unternehmen Waren und Dienstleistungen für Personen in der Europäischen Union anbietet oder das Verhalten von Bürgerinnen und Bürgern beobachtet und in diesem Zusammenhang personenbezogene Daten verarbeitet. Der Anwendungsbereich der DS-GVO erfasst damit auch außereuropäische Unternehmen, die auf dem europäischen Markt aktiv sind, selbst wenn sie keine Niederlassung in der Europäischen Union haben. Durch das Marktortprinzip sollen einheitliche Wettbewerbsbedingungen für alle Unternehmen geschaffen werden, die auf dem europäischen Markt Waren und Dienstleistungen anbieten.

**Metadaten**

Die bei einer Datenübermittlung anfallenden Daten unterteilt man in Inhaltsdaten – beispielsweise der Text einer E-Mail – und alle anderen sog. Metadaten, die die Kommunikationsumstände betreffen, d. h. Zeitpunkt, Absender, Empfänger, Standorte bei mobilen Endgeräten sowie technische Adressen/Kennnummern der zur Kommunikation verwendeten Geräte.

| | |
|---|---|
| Mikroblogging | Beim Mikroblogging werden kurze SMS-ähnliche Texte erstellt, die in einem Blog oder 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. |
| 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. |
| OWASP 10-Kriterien | Kriterien, die durch das Open Web Application Security Project, eine global tätige Stiftung zur Förderung der Netzsicherheit, veröffentlicht wurden. |

| | |
|---|---|
| Pixel | Kleine Grafiken auf Webseiten, die meist nur 1x1 Pixel messen und beim Aufruf einer Webseite von einem Server geladen werden. Das Herunterladen wird registriert und kann für Auswertungen im Bereich des Online-Marketings genutzt werden. |
| PNR-Daten | PNR steht für Passenger Name Record. Das sind Fluggastdatensätze, zu denen neben Kontakt-, Reise- und Zahlungsinformationen auch Informationen zu Ernährungsgewohnheiten und zum Gesundheitszustand der Reisenden zählen können. |
| Pre-Recording-Funktion | Bezeichnet die Aufzeichnung und Speicherung eines vorgewährten Zeitbereichs in einer Endlosschleife, d. h., es handelt sich um eine Aufzeichnungsfunktion, bei der bereits wenige Sekunden vor Betätigen des Aufzeichnungsknopfes eine Speicherung der Daten erfolgt. |
| Privacy-by-Default | Produkte werden mit den datenschutzfreundlichsten Voreinstellungen ausgeliefert. |
| Privacy-by-Design | Die Hersteller berücksichtigen den Datenschutz bereits bei der Herstellung und Entwicklung von Produkten. |
| Profiling | Unter Profiling ist jede Art der automatisierten Bewertung bestimmter persönlicher Aspekte einer natürlichen Person zu verstehen. Zu diesen Aspekten können etwa die Arbeitsleistung, die wirtschaftliche Lage, die Gesundheit, persönliche Vorlieben, die Interessen, die Zuverlässigkeit, das Verhalten, der Aufenthaltsort oder mögliche Ortswechsel einer Person gehören. Ziel des Profilings ist es, diesbezüglich eine Analyse vorzunehmen bzw. eine Vorhersage zu treffen. Profiling kommt z. B. im Werbebereich und bei der Vertragsanbahnung zum Einsatz, aber etwa auch die Polizei setzt zunehmend auf entsprechende Vorhersageverfahren. |

| | |
|---|---|
| Prüfwert | Der Prüfwert wird mittels einer unumkehrbaren kryptografischen Hashfunktion aus der Telefonnummer berechnet. |
| pseudonymisieren | Pseudonymisieren ist das Ersetzen identifizierender Angaben wie Name, Adresse, Geburtsdatum oder anderer eindeutiger Kennzeichen bzw. Merkmale durch eine andere Bezeichnung (z. B. eine laufende Nummer) derart, dass ein Rückschluss auf die Person ohne Kenntnis der Zuordnungsregel nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. |
| Quellcode | Der Programmcode (technische Grundlage) einer Software. |
| Registrant | Person, die eine Webseiten-Registrierung bei einer Organisation durchführt, die Internet-Domains registriert (bei dem sog. Registrar). |
| Ringspeicherverfahren | Speichert Daten kontinuierlich in einem gewissen Zeitraum und überschreibt diese nach dem Ablaufen einer vorgegebenen Zeit wieder, um den Speicherplatz für neue Daten wieder freizugeben. |
| sensitive Daten | Besondere Arten personenbezogener Daten. Dazu gehören Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. |
| Social-Plugins | Ein Programmcode, der in die Webseite eingebunden wird und den Browser der Benutzerin bzw. des Benutzers der Webseite dazu veranlasst, Inhalte von einem Dritten anzufordern, und dazu Daten an diesen Dritten übermittelt, z. B. „Gefälltmir"-Button von Facebook oder „Twitter"-Button. |

| | |
|---|---|
| Tracking / Cookie Walls | Verhinderung der Nutzung einer Webseite bei Nichtakzeptieren von Cookies. |
| Wearable | Wearable Computer oder kurz Wearables sind Computer, die so klein sind, dass sie weder einen Raum ausfüllen noch einen Schreibtisch benötigen, sondern z. B. als Armband und Brille getragen oder in Kleidung eingearbeitet werden können. Während der Anwendung sind sie am Körper der Benutzenden befestigt und oftmals direkt mit dem Internet verbunden. So kann z. B. ein Blutdruckmessgerät, welches dauerhaft oder über einen längeren Zeitraum am Arm getragen wird, durchaus als Gerät aus dem Bereich Wearable Computing bezeichnet werden. |
| Webtracking | Die Beobachtung und Analyse der Nutzerinnen und Nutzer zu Geschäfts- und Marketingzwecken. |
| WiFi-Tracking | Eine Technik, mit der Bewegungsverläufe von Personen anhand von Standortdaten verfolgt werden können, die unter Rückgriff auf das Smartphone dieser Personen erfasst werden. |

# Stichwortverzeichnis

## E



## F



## G



## H / I



## J / K



## L



## M

## 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, Faltblätter/Broschüren 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.

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

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

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

Der Jahresbericht 2017 umfasst folgende Schwerpunkte:

Europäische Datenschutz-Grundverordnung: Betroffenenrechte, Verhaltensregeln und Risiken; Volksbegehren Videoüberwachung; Identitätsdiebstahl; Entwurf einer ePrivacy-Verordnung – Noch mehr Datenschutz made in Europe!

www.datenschutz-berlin.de

be Berlin