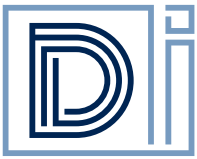

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Datenschutz und Informationsfreiheit

Jahresbericht 2016

Jahresbericht 2016

der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2016

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 23. März 2016 vorgelegten Jahresbericht 2015 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2016 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band (Dokumente 2016) veröffentlicht.

Beide Veröffentlichungen sind auf unserer Internetseite abrufbar, siehe unter: https://www.datenschutz-berlin.de

Impressum

Herausgeberin: Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin
Telefon: (0 30) + 138 89-0
Telefax: (0 30) 215 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Gestaltung: april agentur GbR

Satz: Layoutmanufaktur.Berlin

Druck: Druckerei Arnold

Inhalt

Einleitung

Am 28. Januar 2016 hat mich das Abgeordnetenhaus von Berlin für die Dauer von fünf Jahren zur Berliner Beauftragten für Datenschutz und Informationsfreiheit gewählt. Ich stehe in der Nachfolge von Dr. Alexander Dix, der das Amt über zehn Jahre innehatte und dem ich an dieser Stelle sehr herzlich für seine Arbeit danken möchte. Mein besonderer Dank gilt aber meinen Mitarbeiterinnen und Mitarbeitern. Ihr unermüdlicher und engagierter Einsatz für die Interessen des Datenschutzes und der Informationsfreiheit bildet die Grundlage für diesen Jahresbericht.

Die Vielfalt der Themen zeigt erneut, dass die Nutzung personenbezogener Daten inzwischen alle Bereiche unseres Lebens erfasst. Die schnell weiter voranschreitende Digitalisierung unseres Alltags sorgt für immer neue Fragestellungen und Herausforderungen sowohl im Datenschutz als auch in der Informationsfreiheit. Die Verarbeitung von Informationen ist zunehmend allgegenwärtig, weil diese inzwischen jederzeit und überall verfügbar sind. Fast alle Abläufe des täglichen Lebens können durch Digitalisierung unserer Alltagsumgebung, z. B. durch selbstfahrende Autos[1] und Smart Home-Lösungen[2], komfortabler gestaltet werden. Allerdings kann doch nur ein Haus, das die Privatsphäre seiner Bewohner achtet und damit die Wahrung eines zentralen Grundrechts berücksichtigt, wirklich als smart bezeichnet werden. Dieser Aspekt müsste bei der Entwicklung des sogenannten Internets der Dinge viel stärker berücksichtigt werden, um wirklich einen qualitativen Fortschritt zu erreichen. Bei der Entwicklung des digitalen Heims wird derzeit viel zu wenig im Bereich der IT-Sicherheit und des Datenschutzes geforscht.[3] Hier ist nicht die nutzende Person, sondern die Wirtschaft in der Ver-

1 Siehe 4.3

2 Siehe 4.4

3 So der Bericht der Gemeinsamen Forschungsstelle (Joint Research Center JRC) der Europäischen Kommission von Dezember 2016: Smart Grid Laboratories Inventory 2016, abrufbar (in englischer Fassung) unter https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/smart-grids-laboratories-inventory-2016

antwortung. Sie muss den Datenschutz als Wettbewerbsvorteil begreifen und die Produkte von vornherein datenschutzfreundlich gestalten.

Es sind diese technischen Anforderungen, die zusammen mit den rechtlichen Regelungen das Fundament für den Datenschutz bilden, der seit Inkrafttreten des Vertrags von Lissabon ein europäisches Grundrecht darstellt. Danach hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.[4]

Dass es dieses Grundrecht zu verteidigen gilt, hat der Europäische Gerichtshof in diesem Jahr erneut sehr deutlich gezeigt. So hat er die jahrelange Diskussion beendet und mit einem Grundsatzurteil entschieden, dass IP-Adressen[5] personenbezogene Daten darstellen.[6] Auch hat er sich erneut mit der Vorratsdatenspeicherung durch Telekommunikationsunternehmen befasst und anlässlich einer Auseinandersetzung mit den Gesetzen in Großbritannien und Schweden geurteilt, dass eine allgemeine und unterschiedslose Speicherung von Verkehrs- und Standortdaten unzulässig ist.[7] Zugleich hat er hohe Hürden für die Rechtmäßigkeit der Vorratsdatenspeicherung formuliert, die deutlich über die vom Bundesverfassungsgericht aufgestellten Anforderungen hinausgehen.[8] Es bleibt abzuwarten, ob die in Deutschland seit 2015 geltenden gesetzlichen Regelungen zur Speicherung von Verkehrsdaten[9] den Maßstäben des Europäischen Gerichtshofs genügen.

Diese Entscheidung des Europäischen Gerichtshofs dürfte auch auf andere Bereiche ausstrahlen, in denen personenbezogene Daten auf Vorrat gespeichert werden. So wird zu gegebener Zeit untersucht werden müssen, ob die europaweite Verarbeitung von Flugpassagierdaten auf der Grundlage der neuen PNR-Richt-

4 Artikel 8 Abs. 1 EU-Grundrechte-Charta

5 IP steht für Internetprotokoll. Die IP-Adressen sind Nummernfolgen, die an das Internet angeschlossenen Geräten zugewiesen werden, um die Kommunikation zwischen diesen zu ermöglichen.

6 Urteil vom 19. Oktober 2016, C-582/14

7 Urteil vom 21. Dezember 2016, C-203/15 und C-698/15

8 Siehe hierzu JB 2010, 13.1

9 Zum Hintergrund siehe JB 2015, 4.1

linie,[10] die nahezu unbemerkt von der Öffentlichkeit – zufällig oder nicht – am selben Tag verabschiedet wurde wie das EU-Datenschutz-Reformpaket,[11] den hohen Anforderungen des Gerichtshofs genügt. Denn es ist mehr als fraglich, ob die von den Fluggesellschaften erfassten Daten sämtlicher Reisenden in der EU überhaupt geeignet sind, schwere Straftaten zu verhindern bzw. aufzuklären.

Auch in Zukunft wird der Europäische Gerichtshof gefordert bleiben. Womöglich wird er sich vor dem Hintergrund der aktuellen Entwicklungen in den USA alsbald auch mit der Angemessenheitsentscheidung zum EU-US Privacy Shield[12] befassen müssen.

Der weltweite Terror mit islamistischem Hintergrund ist nun leider auch in Deutschland angekommen. Nicht zuletzt wegen des Lkw-Anschlags auf einen Berliner Weihnachtsmarkt hat die Debatte um mehr öffentliche Sicherheit eine neue Dimension erreicht. Obwohl die Umstände, die den Anschlag ermöglicht hatten, im Einzelnen noch ungeklärt waren, nahm die Diskussion um mögliche Gesetzesverschärfungen schnell ihren Lauf. Dazu gehörte – neben der Einführung der elektronischen Fußfessel zur Überwachung von „Gefährdern" durch Satellitenortung – erneut die Forderung, die Videoüberwachung auszuweiten. In Berlin wurde dies zusätzlich mit den Fahndungserfolgen in Bezug auf mehrere Gewaltdelikte in Bahnhöfen der Berliner Verkehrsbetriebe (BVG) begründet.

Bei der ganzen Diskussion darf jedoch nicht vergessen werden, dass mehr Videoüberwachung nicht automatisch auch zu mehr Sicherheit führt. Bislang ist nicht geklärt, welchen Beitrag Überwachung im öffentlichen Raum für die Sicherheit überhaupt leistet. Dass es angesichts neuer besonderer Gefährdungslagen zu einer Neujustierung bei der Abwägung zwischen den Sicherheitsbedürfnissen der Bevölkerung und den Freiheitsrechten der Betroffenen kommen kann, schließe auch ich nicht aus. Jedoch ist die Videoüberwachung kein Allheilmittel und es

10 Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. EU vom 4. Mai 2016, L 119/132

11 Siehe 1.2

12 Siehe 1.1

muss immer wieder daran erinnert werden, dass jeder Mensch das verfassungsrechtlich verbürgte Recht hat, sich unbeobachtet in der Öffentlichkeit zu bewegen. Eine umfassende Überwachung der Menschen darf es in unserer freiheitlich-demokratischen Grundordnung nicht geben.

Berlin, den 7. April 2017

Maja Smoltczyk
Berliner Beauftragte für Datenschutz und Informationsfreiheit

1 Schwerpunkte

1.1 Post-Safe Harbor: Das neue EU-US Privacy Shield

Was bisher geschah

Zur datenschutzrechtlichen Absicherung der Handelsbeziehungen zwischen den Vereinigten Staaten von Amerika und den Mitgliedstaaten der Europäischen Union hatte die EU-Kommission im Jahr 2000 die zuvor mit dem US-Handelsministerium verhandelten „Grundsätze des ‚sicheren Hafens' zum Datenschutz" (im Folgenden Safe Harbor-Abkommen) als den europäischen Anforderungen angemessen anerkannt. Datenempfänger mit Sitz in den USA, die sich verpflichtet hatten, die Grundsätze einzuhalten und entsprechend den vorgegebenen Leitlinien umzusetzen, galten von nun an als mit ausreichendem Datenschutzniveau ausgestattet.

Vor dem Hintergrund der NSA-Enthüllungen von Edward Snowden hatte die EU-Kommission im November 2013 begonnen, diese Safe Harbor-Regelungen zu überprüfen und ein neues Abkommen mit den USA zu verhandeln.[13] Im Oktober 2015 hatte der Europäische Gerichtshof (EuGH) mit einem Paukenschlag das Safe Harbor-Abkommen gekippt und die Entscheidung der EU-Kommission aus dem Jahr 2000, insbesondere mangels ausreichender inhaltlicher Prüfungen der tatsächlichen Angemessenheit des Schutzniveaus in den USA, für ungültig erklärt.[14]

Im Februar 2016 stellte die EU-Kommission einen ersten Entwurf eines neuen EU-US-Datenschutzschilds, das sog. Privacy Shield, vor[15] und erklärte, dies sei die

13 Pressemitteilung der EU-Kommission vom 27. November 2013, abrufbar unter http://europa.eu/rapid/press-release_MEMO-13-1059_de.htm

14 EuGH, Urteil vom 6. Oktober 2015, C-362/14 (Rs. Schrems); siehe JB 2015, 14.1 (S. 162)

15 Pressemitteilungen der EU-Kommission vom 2. und 29. Februar 2016, abrufbar unter http://europa.eu/rapid/press-release_IP-16-216_de.htm und http://europa.eu/rapid/press-release_IP-16-433_de.htm

„Antwort auf die Forderungen, die der EuGH" bei der Ungültigkeitsfeststellung des Safe Harbor-Abkommens aufgestellt hätte.

Die Art. 29-Datenschutzgruppe, die aus Vertreterinnen und Vertretern sämtlicher europäischer Datenschutzbehörden besteht und beratende Funktion hat, zeigte sich skeptisch: Mit den Arbeitspapieren WP 237 und 238 legte sie eine fundierte Analyse der europäischen Rechtsprechung und darauf basierend eine Einschätzung des Privacy Shields vor.[16] Zwar stellte die Art. 29-Gruppe einige Fortschritte im Gegensatz zur Vorgängerregelung fest, brachte allerdings auch eine Reihe von Bedenken zum Ausdruck.[17] Im sog. Art. 31-Ausschuss, der sich aus Vertreterinnen und Vertretern der EU-Mitgliedstaaten zusammensetzt und dessen Stellungnahme im Falle von Angemessenheitsentscheidungen einzuholen ist, konnten sich anschließend die Delegierten nicht darauf einigen, das vorliegende Ergebnis freizugeben. Auch das Europäische Parlament äußerte sich kritisch und drängte zu weiteren Verhandlungen.[18]

Die EU-Kommission führte daraufhin Nachverhandlungen und legte dem Art. 31-Ausschuss einen zweiten Entwurf mit einzelnen Änderungen und weiteren Erläuterungen vor. Dieser Entwurf wurde vom Ausschuss angenommen. Eine erneute Beteiligung der Art. 29-Gruppe erfolgte nicht. Die EU-Kommission stellte daraufhin am 12. Juli die Angemessenheit des Privacy Shields fest und veröffentlichte die Unterlagen.[19]

16 WP 237 vom 13. April 2016 (Essential Guarantees), nur englische Fassung abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf, WP 238 vom 13. April 2016 (Opinion on the EU-U.S.-Privacy Shield draft adequacy decision), nur englische Fassung abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

17 Pressemitteilung der Art. 29-Gruppe vom 13. April 2016, nur englische Fassung abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf

18 Pressemitteilung des Europäischen Parlaments vom 26. Mai 2016, abrufbar unter http://www.europarl.europa.eu/news/de/news-room/20160524IPR28820/geplanter-eu-us-datenschutzschild-verbesserungsw%C3%BCrdig

19 Durchführungsbeschluss (EU) 2016/1250 vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. EU vom 1. August 2016, L 207/1; siehe auch Pressemitteilung der EU-Kommission vom 12. Juli 2016, abrufbar unter http://europa.eu/rapid/press-release_IP-16-2461_de.htm

Privacy Shield – kurz zusammengefasst

Wie schon bei Safe Harbor sind auch beim Privacy Shield bestimmte Datenschutzgrundsätze[20] das Kernelement. Auch das System der Selbstzertifizierung ist erhalten geblieben. US-amerikanische Organisationen, die sich zertifizieren möchten, müssen entweder den Untersuchungsbefugnissen der Federal Trade Commission (FTC) oder denen des US-Verkehrsministeriums unterliegen. Die Organisationen müssen sich öffentlich bereit erklären, die Grundsätze einzuhalten und entsprechende Datenschutzbestimmungen zu veröffentlichen. Das Gesamtsystem wird vom US-Handelsministerium überwacht und verwaltet. Die zertifizierten US-Unternehmen werden ebenfalls online in einer Liste veröffentlicht. [21]

Daneben beinhaltet das Privacy Shield ein Geflecht aus weiteren Anlagen und Anhängen. Dazu gehören eine Reihe von ministeriellen Schreiben mit Erläuterungen zum Rechtssystem in den USA, Verpflichtungserklärungen zur Umsetzung und Durchsetzung des Privacy Shields, Erläuterungen zu den Zugriffen durch nationale Sicherheitsbehörden und Abfragen durch Strafverfolgungsbehörden sowie bestimmte Zusicherungen, die der Absicherung der Betroffenenrechte dienen sollen.

Eine wesentliche Neuerung stellt die Einrichtung einer Ombudsstelle im Bereich der nationalen Sicherheit dar.[22] Betroffene, deren Daten in die USA übermittelt wurden , können sich mit Anfragen zum Zugriff auf die Daten durch US-Geheimdienste über die nationalen Aufsichtsbehörden in Europa an die Ombudsstelle wenden. [23]

In der Angemessenheitsentscheidung selbst ist vorgesehen, dass das Privacy Shield jährlich evaluiert werden soll.[24] Hierzu ist zusammen mit der US-Seite eine gemeinsame Prüfung vorgesehen, die sich auf alle Aspekte der Funktionsweise

20 Anhang II der Privacy Shield-Angemessenheitsentscheidung (a. a. O.)

21 Abrufbar unter www.privacyshield.gov

22 Anlage A zum Anhang III der Privacy Shield-Angemessenheitsentscheidung (a. a. O.)

23 Dabei ist unerheblich, ob die Übermittlung auf dem Privacy Shield beruht oder auf anderen Instrumenten des Drittstaatentransfers wie Standardvertragsklauseln oder verbindlichen Unternehmensregelungen oder aber auf den Ausnahmetatbeständen in Art. 26 Abs. 1 der Europäischen Datenschutzrichtlinie.

24 Erwägungsgrund (146)

des Privacy Shields erstrecken soll, darunter auch die Handhabung der aus Gründen der nationalen Sicherheit und Strafverfolgung gewährten Ausnahmen von den Grundsätzen. Darüber hinaus hat sich die EU-Kommission in der Angemessenheitsentscheidung vorbehalten, das gebotene Schutzniveau nach dem Inkrafttreten der EU-Datenschutz-Grundverordnung (neu) zu bewerten.[25]

Nach dem Urteil ist vor dem Urteil

Nachdem die EU-Kommission ihre Entscheidung ohne weitere Beteiligung der Art. 29-Gruppe getroffen hatte, wies diese darauf hin, dass auch bei der nachgebesserten Fassung des Privacy Shields etliche Bedenken fortbestünden, die in ihrem Arbeitspapier WP 238 dargestellt worden waren.[26]

Das Privacy Shield enthält ebenso wie seinerzeit das Safe Harbor-Abkommen generelle Ausnahmen von der Verpflichtung, die Datenschutzgrundsätze einzuhalten, u. a. im Zusammenhang mit Erfordernissen der nationalen Sicherheit. Ein Schreiben des US-Geheimdienstdirektors,[27] das Bestandteil des Privacy Shields ist, soll erläutern, welche Beschränkungen und Garantien für solche Zugriffe durch nationale Sicherheitsbehörden gelten. Dreh- und Angelpunkt der Diskussion ist die Frage der sog. „bulk collection", d. h. der massenhaften, unterschiedslosen Datenerhebung, die nicht als verhältnismäßig angesehen werden kann. Aus Sicht der Art. 29-Gruppe fehlt es hier an konkreten Zusicherungen, dass derartige Datenerhebungen nicht stattfinden.

Bei der neu eingerichteten Ombudsstelle bestehen zudem Bedenken, ob dieser Mechanismus einen hinreichend effektiven Rechtsschutz bietet. Es ist fraglich, ob und ggf. inwieweit die Ombudsperson eigene Prüfbefugnisse gegenüber den US-Geheimdiensten erhält oder inwieweit sie auf die Prüfergebnisse von anderen Behörden vertrauen muss. Darüber hinaus ist nicht vorgesehen, dass die Betrof-

25 Erwägungsgrund (146)

26 Pressemitteilung der Art. 29-Gruppe vom 26. Juli 2016, nur in englischer Fassung abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

27 Schreiben des „Office of the Director of National Intelligence (ODNI)", Anhang V der Privacy Shield-Angemessenheitsentscheidung (a. a. O.)

fenen eine Rückmeldung darüber erhalten, ob auf ihre personenbezogenen Daten tatsächlich zugegriffen wurde und ob diese zwischenzeitlich gelöscht wurden.

Diese und andere Einwände sind durch die Angemessenheitsentscheidung der EU-Kommission und das Anlagenkonvolut nicht abschließend ausgeräumt worden. In der Safe Harbor-Entscheidung hatte der EuGH kritisiert, dass die EU-Kommission nicht ausreichend festgestellt habe, ob die USA aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen ein angemessenes Datenschutzniveau gewährleisten. Der EuGH hatte der EU-Kommission vorgehalten, dass sie bei den generellen Ausnahmen von den Datenschutzgrundsätzen (z. B. für Aktivitäten im Bereich der nationalen Sicherheit) hätte überprüfen müssen, ob sich nach der US-Rechtsordnung wiederum ausreichende Beschränkungen für solche Zugriffe ergeben, so dass die Ausnahmen als akzeptabel im Hinblick auf die Gleichwertigkeit des Schutzniveaus hätten angesehen werden können.[28]

Vor diesem Hintergrund ist ungewiss, ob sich die EU-Kommission nach den Maßstäben des EuGH ausreichend mit den Ausnahmen vom Schutz personenbezogener Daten in den USA auseinandergesetzt hat und ob das Privacy Shield einer zu erwartenden gerichtlichen Überprüfung vor dem EuGH standhalten wird.

Auch in Bezug auf die kommerziellen Aspekte des Privacy Shields sind einige Fragen offen geblieben: So enthält es keine Regelung zur automatisierten Einzelentscheidung, d. h. Entscheidungen, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zur Bewertung von Persönlichkeitsmerkmalen ergehen, und ebenso wenig eine Regelung zum allgemeinen Widerspruchsrecht. Nicht eindeutig ist zudem, wie die Datenschutzgrundsätze auf Auftragsdatenverarbeiter anzuwenden sind. Hier hatte die EU-Kommission zwar im Rahmen der Nachbesserungen Klarstellungen in die Angemessenheitsentscheidung aufgenommen. Diese spiegeln sich allerdings in den Anhängen bzw. Datenschutzgrundsätzen so nicht wider.

Insgesamt ist festzuhalten, dass die Form des Privacy Shields als „verschlungenes Geflecht“ aus Anlagen und Anhängen nicht zur Verständlichkeit der Regelung

28 Urteil des EuGH (Rs. Schrems), Rn. 88, 96, 97

beiträgt. Wohlweislich hat die EU-Kommission einen „Leitfaden zum EU-US-Datenschutzschild“ herausgegeben.[29]

In der Praxis

Im Rahmen einer koordinierten Prüfung starteten wir zusammen mit anderen Datenschutzaufsichtsbehörden[30] im November eine Fragebogenaktion bei ca. 500 Unternehmen zu Übermittlungen personenbezogener Daten in Nicht-EU-Staaten. Hintergrund sind neben dem zunehmenden Einsatz von Cloud-Services und anderen grenzüberschreitenden Diensten nicht zuletzt die Diskussionen des letzten Jahres zum transatlantischen Datenverkehr und die Entwicklungen hin zum Privacy Shield. Die Prüfung zielt auch darauf ab, die verantwortlichen Stellen für die Fragestellungen des Drittstaatentransfers zu sensibilisieren; daneben sollen Erkenntnisse über die aktuelle Unternehmenspraxis gewonnen werden. Die Prüfung ist noch nicht abgeschlossen.

Bisher gibt es kaum Erfahrungen mit dem Privacy Shield. In der Liste mit den Zertifizierungen[31] werden inzwischen 1337 Anmeldungen angezeigt.[32] Unternehmen und öffentliche Stellen, die an US-Organisationen auf der Grundlage des Privacy Shield personenbezogene Daten übermitteln wollen, sollten zuvor mindestens prüfen,

- ob die Zertifizierung der Empfängerorganisation gültig ist,
- ob die zu übermittelnden Daten von der Zertifizierung abgedeckt sind,
- ob nach der Datenschutzerklärung der Empfängerorganisation die Umsetzung der Datenschutzgrundsätze plausibel ist,
- ob – sofern Daten an Tochtergesellschaften übermittelt werden – diese von der Zertifizierung umfasst sind und
- wie die Informationspflichten erfüllt werden.

29 Abrufbar unter http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf

30 Bayern, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland und Sachsen-Anhalt

31 www.privacyshield.gov

32 Stand: 30. Dezember 2016

Nächste Schritte und Ausblick

Die Art. 29-Gruppe hatte vor dem Hintergrund der fortbestehenden Kritik deutlich gemacht, dass die erste Evaluation ein entscheidender Moment für die Bewertung der Stabilität und Effizienz des Privacy Shields sein wird.[33] Auf europäischer Ebene gilt es nun, die gemeinsame Prüfung intensiv vorzubereiten.

Derzeit werden sowohl auf europäischer als auch auf nationaler Ebene die Konsequenzen aus dem EuGH-Urteil für die anderen Möglichkeiten der Übermittlung von Daten in Drittstaaten wie Standardvertragsklauseln und verbindliche Unternehmensregelungen analysiert. Die EU-Kommission hat in einem ersten Schritt die Beschränkung der aufsichtsbehördlichen Befugnisse in den übrigen Angemessenheitsentscheidungen und -beschlüssen betreffend Drittländer und die Standardvertragsklauseln revidiert.[34] Denn solche Beschränkungen hatte der EuGH in Bezug auf Safe Harbor ebenfalls für unzulässig erklärt.

Dabei wird es allerdings nicht bleiben können.[35] Der EuGH hatte mit Verweis auf die EU-Grundrechte-Charta[36] und den Wesensgehalt der Grundrechte deutlich gemacht, dass Einschränkungen des Schutzes personenbezogener Daten verhältnismäßig und auf das absolut Notwendige beschränkt sein müssen und dass das Recht der Betroffenen auf einen wirksamen gerichtlichen Rechtsschutz gewahrt bleiben muss. Auch diese Feststellungen und deren Auswirkungen auf die Instrumente des Drittstaatentransfers bzw. auf andere Angemessenheitsentscheidungen werden zu überprüfen sein.

Die Diskussionen über die Instrumente zur Datenübermittlung in Drittstaaten bzw. über die Angemessenheitsentscheidungen der EU-Kommission sind auch nach mehr als einem Jahr seit dem EuGH-Urteil nicht zur Ruhe gekommen. Das Privacy Shield hat daran bisher nichts ändern können. Zwar ist die Ange-

33 Pressemitteilung der Art. 29-Gruppe vom 26. Juli 2016 (a. a. O.)

34 Durchführungsbeschluss (EU) 2016/2295 vom 16. Dezember 2016, ABl. EU vom 17. Dezember 2016, L 344/83; Durchführungsbeschluss (EU) 2016/2297 vom 16. Dezember 2016, ABl. EU vom 17. Dezember 2016, L 344/100

35 Siehe auch die Stellungnahme der Art. 29-Gruppe (WP 241) vom 31. Oktober 2016, abrufbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=40820

36 Art. 7 und Art. 47

messenheitsentscheidung auch für die Aufsichtsbehörden verbindlich. Gleichwohl sind seriöse Aussagen zur Stabilität des Privacy Shields derzeit nicht möglich. Viele Fragen sind unbeantwortet, die z. B. auch ein mögliches Klagerecht der Aufsichtsbehörden[37] und deren Aussetzungsbefugnisse betreffen. Es bleibt zu hoffen, dass die für Mitte 2017 angestrebte erste Evaluation die notwendigen Klärungen bringt.

1.2 Europäische Datenschutz-Grundverordnung

Lange haben die Gesetzgeber in Brüssel um die Datenschutz-Grundverordnung (DS-GVO) gerungen, die nun endlich in Kraft getreten ist und am 25. Mai 2018 unmittelbare Wirkung entfalten wird.[38] Die DS-GVO enthält einige Neuerungen, die unmittelbar den Bürgerinnen und Bürgern zugutekommen. Neben der Stärkung der Betroffenenrechte ist für Bürgerinnen und Bürger sicherlich die bedeutendste Verbesserung, dass sie sich auch bei Datenschutzverstößen durch ausländische Unternehmen bei ihrer Aufsichtsbehörde vor Ort beschweren können. Wir prüfen die jeweilige Fragestellung dann gemeinsam mit anderen europäischen Aufsichtsbehörden. Dies bedeutet für unsere Behörde zwar erheblich mehr Arbeit, aber auch einen enormen Zuwachs an Kompetenzen. Dies gilt vor allem für Bereiche, in denen wir befugt sind, Sanktionen auszusprechen.[39]

Aber auch für Unternehmen verspricht die DS-GVO viele Vorteile. Allerdings müssen sie ebenfalls neue Regeln beachten, auf die es sich schon jetzt einzustellen gilt.[40] Dies gilt nicht nur für klassische Datenverarbeiter, sondern für alle möglichen Bereiche. Beispielhaft behandeln wir die Auswirkungen der DS-GVO auf die

37 Siehe 1.2.1

38 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. EU vom 4. Mai 2016, L 119/1

39 Siehe 1.2.4

40 Siehe 1.2.2

Banken,[41] die Sanktionspraxis der Aufsichtsbehörden,[42] die Wissenschaft und Forschung[43] und die Informationsfreiheit.[44]

Leider ist auch nach Inkrafttreten der DS-GVO für Bürgerinnen und Bürger, Aufsichtsbehörden, Unternehmen und sonstige Stellen nicht in Gänze klar, auf welche datenschutzrechtlichen Rahmenbedingungen sie sich ab Mai 2018 konkret einstellen müssen. Dies liegt daran, dass die Verordnung an vielen Stellen Spielräume für nationales Recht enthält, die ausgefüllt werden können. Dabei ist darauf zu achten, dass die Verbesserungen, die die DS-GVO bereithält, nicht vom nationalen Gesetzgeber wieder abgeschafft werden.[45]

1.2.1 Gesetzgeberische Aktivitäten im Bereich der Öffnungsklauseln

Das Bundesministerium des Innern (BMI) hat einen Entwurf für ein Datenschutz-Anpassungs- und Umsetzungsgesetz EU vorgelegt. Mit diesem Gesetz sollen einerseits die gesetzgeberischen Spielräume aus der DS-GVO genutzt und zugleich die RL 2016/680[46] umgesetzt werden. Damit wird das derzeitige Bundesdatenschutzgesetz (BDSG) völlig neu gefasst. Der zeitliche Rahmen für das Gesetzgebungsverfahren ist denkbar knapp: Die DS-GVO enthält eine Reihe von zwingenden Regelungsaufträgen, die die nationalen Gesetzgeber bis zum Geltungsdatum am 25. Mai 2018 umsetzen müssen. Darüber hinaus existieren Handlungsoptionen, von denen die Bundesregierung offensichtlich Gebrauch machen möchte. Zeitlich erschwerend kommt hinzu, dass Deutschland im Herbst 2017

41 Siehe 1.2.3

42 Siehe 1.2.4

43 Siehe 1.2.5

44 Siehe 1.2.6

45 Siehe 1.2.1 und 1.2.2

46 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. EU vom 4. Mai 2016, L 119/89

wählt und die Legislaturperiode damit de facto vor der Sommerpause endet. Das bedeutet, dass der Gesetzesentwurf spätestens im Frühjahr 2017 in das Parlament eingebracht werden muss. Vor diesem Hintergrund zeigt sich, mit welchem Zeitdruck an dem Gesetzesentwurf gearbeitet wurde. Leider hat sich dies nicht positiv auf den Inhalt des BDSG-Neu ausgewirkt. Wir sind mit folgenden Forderungen an den Gesetzgeber herangetreten:

- **Keine Einschränkung der Betroffenenrechte!**

Noch in den Verhandlungen um die DS-GVO wurde vom BMI stets argumentiert, dass das hohe deutsche Datenschutzniveau bewahrt werden solle. Nun nutzt das BMI Öffnungsklauseln in der DS-GVO, um die Betroffenenrechte einzuschränken.[47] Dies führt dazu, dass Betroffene in vielen Fällen von vornherein nichts von dem Eingriff in Datenschutzrechte erfahren, sodass die Ausübung weiterer Rechte (z. B. Löschung, Widerspruchsrecht) erschwert wird. Das ist nicht nur nachteilig für den Datenschutz, sondern auch europarechtswidrig und nicht mit der DS-GVO zu vereinbaren.

So sieht das BDSG-Neu vor, dass Informations- und Auskunftspflichten eingeschränkt werden können, wenn die Information einen „unverhältnismäßigen Aufwand" erfordern würde[48] oder die „Geschäftszwecke" erheblich gefährdet.[49] Zwar ergibt sich aus der DS-GVO die Möglichkeit, in bestimmten Ausnahmefällen Betroffenenrechte einzuschränken, wenn z. B. die Landesverteidigung oder die nationale bzw. öffentliche Sicherheit betroffen ist. Bloße Geschäftszwecke oder ein hoher Aufwand für das Unternehmen sind demnach jedoch gerade keine Gründe, Betroffenenrechte einzuschränken. Schließlich geht es hier um Grundrechtsschutz.

- **Zweckändernde Weiterverarbeitung von personenbezogenen Daten**

Die DS-GVO sieht vor, dass zweckändernde Datenverarbeitungen zunächst daraufhin überprüft werden müssen, ob der Zweck, für den die Daten weiterverarbei-

47 §§ 30 bis 32 BDSG-Neu
48 § 30 Abs. 1 Nr. 2 BDSG-Neu
49 §§ 31 Abs. 1 Nr. 2 lit. a, 32 Abs. 1 Nr. 1 BDSG-Neu

tet werden sollen, mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbar ist. Dort wo eine Vereinbarkeit der Zwecke anhand von festgelegten Kriterien festgestellt wird, dürfen die Daten weiterverarbeitet werden. Sofern eine Zweckvereinbarkeit nicht gegeben ist, kommt im nicht-öffentlichen Bereich die Einwilligung als Rechtsgrundlage in Betracht. Als Ausnahme in diesem System sieht die DS-GVO vor, dass die Daten auf Basis einer gesetzlichen Regelung, die im nationalen Recht existiert, weiterverarbeitet werden dürfen. Diese Möglichkeit wird unter den Vorbehalt gestellt, dass es sich um eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme handelt, die zum Schutz von bestimmten in der DS-GVO abschließend festgelegten wichtigen Zielen erfolgt.

Diesem Ausnahmecharakter werden die Vorschriften zur Verarbeitung zu anderen Zwecken im BDSG-Neu nicht gerecht. Vielmehr schafft das BDSG-Neu weitreichende Weiterverarbeitungsbefugnisse, so etwa die Befugnis zur Verarbeitung zu einem anderen Zweck, wenn dies zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist. Eine Abwägung mit den schutzwürdigen Interessen der Betroffenen ist dafür nicht vorgesehen.

Es ist bereits fraglich, ob eine solch weitreichende Ausnahme eine notwendige und verhältnismäßige Maßnahme darstellen kann, wie dies in der DS-GVO zwingend vorgesehen ist. Darüber hinaus ist zu berücksichtigen, dass der Europäische Gesetzgeber mit der DS-GVO vor allem eine bessere Harmonisierung der Datenschutzvorschriften der europäischen Mitgliedstaaten erreichen wollte. Aus diesem Grund hat der europäische Gesetzgeber die Datenschutzvorschriften im Rahmen einer Verordnung geregelt, d. h. ein Regelungsinstrument gewählt, das in den Mitgliedstaaten unmittelbar Geltung erlangt und diesen kaum eigene Regelungsspielräume lässt. Mit der Regelung zur Verarbeitung zu anderen Zwecken im BDSG-Neu entsteht faktisch die paradoxe Situation, dass für die Erstverarbeitung personenbezogener Daten im nicht-öffentlichen Bereich (quasi) kein nationaler Gesetzgebungsspielraum besteht, für die zweckändernde Weiterverarbeitung hingegen weiterreichende Möglichkeiten vorgesehen werden, die sogar über die Grenzen der in der DS-GVO vorgesehenen Ersterhebung hinausgehen (etwa die fehlende Abwägung mit den schutzwürdigen Interessen). Dies kann der europäische Gesetzgeber vor dem Hintergrund der angestrebten Harmonisierung der Vorschriften nicht gewollt haben.

- **Datenschutzkontrolle auch bei Berufsgeheimnisträgern!**

Der Gesetzesentwurf sieht vor, dass Berufsgeheimnisträger weitgehend von der Datenschutzkontrolle durch Datenschutzbehörden ausgenommen werden.[50] Diese Regelung ist äußerst problematisch. Berufsgeheimnisse – wie die ärztliche oder anwaltliche Schweigepflicht – sind wichtige Instrumente zum Schutz der Privatsphäre, insbesondere wenn ein Geheimnisträger Daten an Dritte offenbaren möchte. Dies kann aber jedenfalls dann nicht gelten, wenn der Betroffene selbst bei der Durchsetzung seiner Datenschutzrechte gegenüber der eigenen Ärztin/Rechtsanwältin bzw. dem eigenen Arzt/Rechtsanwalt die Hilfe der Datenschutzaufsichtsbehörden in Anspruch nimmt. Zumindest in solchen Fällen sollten die Aufsichtsbehörden eine uneingeschränkte Kontrollbefugnis haben. Im Übrigen ist unklar, welche Berufsgruppen sich auf Berufsgeheimnisse berufen können sollen, sodass die Vorschrift auszuufern droht.

- **Direkte Länderbeteiligung in europäischen Abstimmungsprozessen!**

In Deutschland wird die Datenschutzaufsicht über die datenverarbeitende Wirtschaft ganz überwiegend von den jeweiligen Landesdatenschutzbehörden ausgeübt. Das BDSG-Neu sieht aber vor, dass im Europäischen Datenschutzausschuss die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als Vertreterin für Deutschland bestellt wird. Da die zukünftig im Europäischen Datenschutzausschuss zu verhandelnden Einzelfälle primär die Datenverarbeitung durch Wirtschaftsunternehmen betreffen, wird das Ergebnis dieser Regelung sein, dass nicht die zuständigen Landesbehörden, sondern in der Regel die Bundesbeauftragte mit den anderen europäischen Aufsichtsbehörden über diese konkreten Einzelfälle verhandelt. Aufgrund der Sachnähe wäre es jedoch besser, diese Aufgabe den fachlich zuständigen Landesbehörden zu übertragen und diese direkt auf europäischer Ebene beraten und abstimmen zu lassen, anstatt sie lediglich über ein möglicherweise kompliziertes Verfahren mittelbar zu beteiligen. Die deutsche Vertretung im Europäischen Datenschutzausschuss sollte aus dem Kreis der Landesdatenschutzbehörden bestimmt werden.

50 § 26 BDSG-Neu

- **Keine Ausweitung der Videoüberwachung!**

Die Vorschrift zur Videoüberwachung[51] ist ungeeignet, terroristische Anschläge oder Amokläufe zu verhindern (so aber das Ziel des Gesetzgebers). Sie zielt auf die Überwachung von Bereichen, in welchen Menschen ihre Freizeit verbringen und in denen ohne einen entsprechenden Anlass keine Überwachung stattfinden sollte. Außerdem überträgt sie die klassische hoheitliche Aufgabe, für Sicherheit zu sorgen, auf Private,[52] die nach dem Gesetzesentwurf die Überwachungsanlagen betreiben sollen.[53] Zu deren eigenem Schutz wäre die Vorschrift nicht erforderlich, weil die Videoüberwachung zum Schutz eigener berechtigter Interessen (z. B. Eigentumsschutz, Aufklärung von Diebstahl, Gewalt und Vandalismus) bereits in der DS-GVO selbst geregelt ist.[54]

- **Gerichtlicher Rechtsschutz und Sanktionen**

Der Referentenentwurf sieht vor, dass die Anordnung der sofortigen Vollziehung von Verwaltungsentscheidungen[55] der Aufsichtsbehörde gegenüber Behörden unzulässig sein soll,[56] und begründet dies mit dem fehlenden Subordinationsverhältnis[57] zwischen den beteiligten Verwaltungsbehörden. Hierbei wird nicht beachtet, dass aufgrund der Abhilfebefugnisse der Aufsichtsbehörde gegenüber Behörden nach der DS-GVO[58] ein faktisches Über-/Unterordnungsverhältnis besteht, ohne dass nach Beginn des Vollzugs der getroffenen Verwaltungsentscheidungen differenziert wird. Dabei besteht auch keine Rechtsschutzlücke für die betroffene Behörde, da sie wie alle Adressaten einer Verwaltungsentscheidung jederzeit die Möglichkeit hat, die Anordnung der sofortigen Vollziehung gerichtlich überprüfen

51 § 4 BDSG-Neu

52 Wie z.B. Betreiber von Einkaufspassagen, Vergnügungsstätten und Sportveranstaltungen

53 Siehe auch Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 9./10. November 2016: „Videoüberwachungsverbesserungsgesetz" zurückziehen!, Dokumentenband 2016, S. 36

54 Generalklausel des § 6 Abs. 1 lit. f DS-GVO

55 § 80 Abs. 2 Satz 1 Nr. 4 Verwaltungsgerichtsordnung (VwGO)

56 § 20 Abs. 7 BDSG-Neu

57 Über-/Unterordnungsverhältnis

58 Art. 58 Abs. 2 DS-GVO

zu lassen.[59] Durch die Regelung würde Gerichten zudem systemwidrig die Aufgabe der Exekutive als erste Prüfinstanz von Verwaltungsentscheidungen übertragen werden. Wir haben deshalb die Streichung dieser Sonderregelung gefordert.

Zukünftig kann die Höhe einer Geldbuße bei Datenschutzverstößen durch ein Unternehmen anhand seines gesamten weltweit erzielten Jahresumsatzes des vorausgegangenen Geschäftsjahres bemessen werden.[60] Hierfür sind konkrete Informationen über die Umsatzhöhe des Unternehmens erforderlich. Es ist verpflichtet, diese Informationen bereitzustellen.[61] Wir haben empfohlen, in der Begründung des Gesetzes zur Umsetzung der DS-GVO darauf hinzuweisen, dass Unternehmen gegenüber der Aufsichtsbehörde Auskunft über ihre wirtschaftlichen Verhältnisse erteilen und Unterlagen hierzu herausgeben müssen. Da sich die DS-GVO im Bereich der Sanktionsregelungen in vielen Teilen am Kartellrecht orientiert,[62] bietet es sich alternativ an, eine deklaratorische Vorschrift entsprechend den Regelungen zur Auskunftspflicht von Unternehmen gegenüber Kartellbehörden[63] in den Gesetzesentwurf aufzunehmen.

Legt ein Adressat eines Bußgeldbescheids Einspruch gegen die Verhängung des Bußgeldes ein, dem die Aufsichtsbehörde nicht abhilft, gehen deren Aufgaben im sog. Zwischenverfahren auf die Staatsanwaltschaft über.[64] Künftig soll diese das weitere Verfahren nur mit Zustimmung der betreffenden Aufsichtsbehörde einstellen können. Diese Verfahrensänderung berücksichtigt nicht in ausreichendem Maße die Bedeutung der in der DS-GVO bestimmten uneingeschränkten Eigenständigkeit der Aufsichtsbehörde auf exekutiver Ebene. Zudem wird die Regelung nicht den Vorgaben der DS-GVO gerecht, wonach die Mitgliedstaaten Rechtsvorschriften erlassen müssen, die es der jeweiligen Aufsichtsbehörde erlauben, Verstöße gegen die DS-GVO den Justizbehörden zur Kenntnis zu bringen und ggf. die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen der DS-GVO durchzusetzen.[65] Um eine solch

59 § 80 Abs. 5 VwGO
60 Art. 83 Abs. 4, 5 DS-GVO
61 Art. 58 Abs. 1 lit. a und Art. 83 Abs. 8 DS-GVO
62 Siehe 1.2.4
63 § 81a Gesetz gegen Wettbewerbsbeschränkungen (GWB)
64 § 69 Abs. 4 Satz 1 Gesetz über Ordnungswidrigkeiten (OWiG)
65 Art. 58 Abs. 5 DS-GVO

verpflichtende Beteiligung der Aufsichtsbehörde am Gerichtsverfahren zu gewährleisten, haben wir gefordert, die geplante Regelung so zu ändern, dass die Aufsichtsbehörde anstelle der Staatsanwaltschaft direkt Beteiligte in Gerichtsverfahren wird. Hierdurch wird auch der Expertise der Aufsichtsbehörden in Datenschutzangelegenheiten Rechnung getragen und somit die Qualität der gerichtlichen Auseinandersetzung bedeutend gestärkt.

1.2.2 Der Countdown für Unternehmen läuft!

Die DS-GVO, die ab dem 25. Mai 2018 unmittelbare Gültigkeit erlangt, bringt Unternehmen viele Vorteile. Erstmals verpflichtet das europäische Datenschutzrecht auch außereuropäische Unternehmen, die auf dem europäischen Markt agieren. Damit werden endlich einheitliche Wettbewerbsbedingungen für europäische und außereuropäische Unternehmen geschaffen. Neben dem einheitlichen Rechtsrahmen wird auch eine abgestimmte Struktur der Datenschutzaufsicht geschaffen. Daher wird es für Unternehmen nicht länger nötig sein, die Zulässigkeit von Datenverarbeitungsprozessen an die – möglicherweise divergierenden – Anforderungen verschiedener europäischer Datenschutzbehörden anzupassen. Künftig werden Unternehmen mit der Aufsichtsbehörde vor Ort eine kompetente Ansprechpartnerin vorfinden, die sie auch bei grenzüberschreitenden Datenverarbeitungsprozessen berät und ggf. strittige Fragen mit Datenschutzbehörden aus anderen EU-Staaten, in welchen das Unternehmen tätig wird, abschließend klärt.

Diesen Erleichterungen steht auch ein neues Regelwerk gegenüber, welches zwar nicht per se strenger als das bisherige Recht ist, aber neue Regelungen enthält, auf die sich die Unternehmen einstellen müssen. Schließlich gilt das neue Recht schon ab dem 25. Mai 2018 unmittelbar, ohne dass es eines Umsetzungsaktes bedarf. Ab diesem Zeitpunkt gilt auch der erhöhte Sanktionsrahmen.[66] Daher sollte es keine Option sein abzuwarten, wie sich der deutsche Gesetzgeber zu der DS-GVO verhält und wie er die in der DS-GVO enthaltenen Öffnungsklauseln nutzt. Unter Umständen kann es bis Anfang 2018 dauern, bis das Bundesdatenschutzgesetz angepasst wird.

66 Siehe 1.2.4

Deshalb sollten sich Unternehmen unabhängig von gesetzgeberischen Aktivitäten ohne Zeitverzögerung mit den neuen rechtlichen Rahmenbedingungen vertraut machen und sich – soweit dies jetzt schon möglich ist – darauf vorbereiten. Gerade weil die technische Umsetzung neuer Gesetzesvorgaben kompliziert sein kann und unter Umständen einen langen Zeitraum erfordert, wird jedem Unternehmen geraten, sich sobald wie möglich mit den neuen Anforderungen auseinanderzusetzen und mit der Implementierung zu beginnen. Die in der DS-GVO angeordnete Übergangsfrist ist nicht nur eine Frist für den nationalen Gesetzgeber, sondern auch eine Frist, die den Unternehmen dazu dienen soll, sich auf die neue Rechtslage einzustellen. Z. B. kann jetzt bereits begonnen werden, das Verfahren zur Einholung von Einwilligungserklärungen grundverordnungskonform auszugestalten. Die DS-GVO enthält etwa ein Koppelungsverbot, das besagt, dass eine Dienstleistung nicht von einer Einwilligung in die Verarbeitung personenbezogener Daten abhängig gemacht werden darf, die für die Erfüllung des Vertrags nicht erforderlich sind. Darüber hinaus muss die oder der Betroffene stets ausdrücklich über das Widerrufsrecht belehrt werden. Es gelten besondere Regelungen bei der Verarbeitung personenbezogener Daten eines Kindes. Die Liste der Vorgaben, die ohne weiteren Umsetzungsakt am 25. Mai 2018 Geltung erlangen, ließe sich fortsetzen. Sollten trotz sorgfältiger Prüfung Unsicherheiten bestehen, ob ein Verarbeitungsverfahren mit den neuen Datenschutzregeln zu vereinbaren ist, besteht auch schon jetzt die Möglichkeit, sich an die zuständige Aufsichtsbehörde zu wenden. Wir beraten bei strittigen Umsetzungsfragen gerne.

In Bereichen, in denen Konkretisierungen durch den deutschen Gesetzgeber zu erwarten sind, haben Unternehmen natürlich immer die Möglichkeit, bestimmte Rechte wie z. B. Transparenzvorgaben aus Gründen der Kundenfreundlichkeit freiwillig und unabhängig von einer möglichen Regelung im neuen Bundesgesetz zu gewähren. Ein vorbildlicher Datenschutz kann auch ein Wettbewerbsvorteil sein und das Vertrauen in ein Unternehmen stärken. Dies hat auch den Vorteil, nicht auf nationale Gesetze warten zu müssen, die ggf. erst kurz vor dem 25. Mai 2018 in Kraft treten.

1.2.3 Umsetzungsbedarf im Bankenbereich

Die Kreditwirtschaft hat sofort mit dem Inkrafttreten der DS-GVO begonnen, sich auf die neue Rechtslage ab dem 25. Mai 2018 einzustellen. Gerade bei Großbanken besteht ein erhöhter Umsetzungsbedarf. Zur Unterstützung des Implementierungsprozesses haben wir im September die Bankenverbände und die anderen Aufsichtsbehörden zu einer Ad-hoc-AG eingeladen, bei der insbesondere bankspezifische Probleme bei der Auslegung der DS-GVO erörtert wurden. Hier eine Auswahl erörterter Themen:

Die in der Bankenpraxis bestehenden Einwilligungserklärungen, wie etwa die Einwilligung in die Datenübermittlung an die Verbundunternehmen, bleiben auch nach dem Inkrafttreten der DS-GVO wirksam, auch wenn unter der Geltung des BDSG-Alt die neuen Transparenzvorgaben[67] nicht voll umgesetzt wurden und kein Hinweis auf das Widerrufsrecht gegeben wurde.[68] Wir haben den Banken allerdings empfohlen, die Kundinnen und Kunden nachträglich auf die Widerrufsmöglichkeit hinzuweisen, etwa als Textmitteilung auf den Kontoauszügen.

Kontrovers diskutiert wurde die Frage, ob die SCHUFA-Klausel, bei der die Kundinnen und Kunden in die Weiterleitung ihrer Daten an die SCHUFA einwilligen und das Kreditinstitut vom Bankgeheimnis befreien, aufgrund fehlender Freiwilligkeit und des Koppelungsverbots unwirksam wird.[69] Dies beträfe sowohl die Alt- als auch die Neufälle. Während die Freiwilligkeit von den Aufsichtsbehörden in Zweifel gezogen wird, vertreten die Banken die Auffassung, dass auch nach der DS-GVO Freiwilligkeit anzunehmen sei, da die Banken bei Abschluss eines Kreditvertrages die Kreditwürdigkeit prüfen und zu diesem Zweck bei einer Auskunftei anfragen müssten. Wir haben den Banken empfohlen, spätestens mit Geltung der DS-GVO auf eine Einwilligung zu verzichten. Stattdessen sollten die gesetzlichen Tatbestände bei Gewährung größtmöglicher Transparenz ausgeschöpft werden. Die DS-GVO gestattet Datenflüsse zur Wahrung berechtigter Interessen des

67 Art. 13 DS-GVO

68 Art. 7 Abs. 3 Satz 3 DS-GVO; siehe auch Beschluss des Düsseldorfer Kreises vom 13./14. September 2016: Fortgeltung bisher erteilter Einwilligungen unter der Datenschutzgrundverordnung, Dokumentenband 2016, S. 41

69 Art. 7 Abs. 4 DS-GVO

Kreditinstituts oder der SCHUFA, etwa um das Ausfallrisiko für einen Kredit zu ermitteln. Dabei werden die Kundinnen und Kunden über die Datenflüsse zwischen dem Kreditinstitut und der SCHUFA möglichst umfassend informiert.

Zu klären war auch allgemein die Frage nach der zeitlichen Geltung der DS-GVO, insbesondere die Frage der Rückwirkung. Unstreitig war, dass die Verpflichtung zur Datenschutz-Folgenabschätzung und zur Konsultation der Aufsichtsbehörde[70] erst für neue oder wesentlich geänderte Verarbeitungsprozesse mit Anwendung der Verordnung ab dem 25. Mai 2018 gilt. Demgegenüber gelten die neuen Betroffenenrechte (wie Auskunftsanspruch und das Recht auf Datenübertragbarkeit) auch bei Verarbeitungen, die vor dem 25. Mai 2018 erfolgt sind. Umstritten war, ob die neuen Betroffenenrechte auch auf Daten anwendbar sind, die vor dem 25. Mai 2018 archiviert wurden.

Besonderes Augenmerk müssen die Banken auf die verschärften Transparenzvorschriften bei der Datenerhebung legen. Die Informationspflichten sind eine Bringschuld des Verantwortlichen. Den Kundinnen und Kunden sind sämtliche Informationen medienbruchfrei zugänglich zu machen. In der Filiale darf die oder der Betroffene deshalb nicht auf Informationen im Internet verwiesen werden. Eine Ausnahme könnte nur dann gemacht werden, wenn über die Informationspflichten hinaus vertiefte Informationen z. B. zum Scoring[71] gegeben werden.

Mit der DS-GVO werden zahlreiche Regelungen des Bundesdatenschutzgesetzes, die die Datenverarbeitung bei Auskunfteien und insbesondere den Datenaustausch mit Auskunfteien betrafen, unwirksam.[72] Trotzdem ist unstreitig, dass auch unter der DS-GVO eine Zusammenarbeit mit Auskunfteien weiter möglich ist.[73] Die Rechtmäßigkeit der Datenflüsse ist nunmehr durch Auslegung der Generalklauseln der DS-GVO zu beurteilen. Dies wird zumindest anfangs zu Rechtsunsicherheit führen. Diese entsteht auch dadurch, dass in keinem anderen Land der EU

70 Art. 35, 36 DS-GVO

71 Siehe § 28b BDSG, nach dem bei der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses unter bestimmten Voraussetzungen ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden darf.

72 §§ 28a, b, 29 BDSG

73 Art. 6 Abs. 1 lit. b und f DS-GVO

eine ähnliche Auskunfteistruktur besteht wie in Deutschland, sodass noch offen ist, wie in einem etwaigen Kohärenzverfahren strittige Themen behandelt werden. Beispielsweise ist zweifelhaft, ob die DS-GVO[74] branchenübergreifende Informationssysteme, die sämtliche Lebensbereiche von Betroffenen abdecken, zulässt, oder ob bei derartigen Systemen nicht generell von überwiegenden schutzwürdigen Interessen Betroffener auszugehen ist.

1.2.4 Auswirkungen auf Sanktionsverfahren der Aufsichtsbehörden

Verstöße gegen datenschutzrechtliche Bestimmungen sollen künftig konsequenter durchgesetzt werden.[75] Hierfür stellt die DS-GVO den Aufsichtsbehörden ein breites Spektrum an sanktionsrechtlichen Abhilfebefugnissen zu Verfügung.[76]

So können sie Verantwortliche und Auftragsverarbeiter warnen, wenn diese eine Datenverarbeitung planen, die voraussichtlich gegen die Verordnung verstoßen wird, und verwarnen, wenn ein solcher Verstoß bereits geschehen ist.

Verantwortliche und Auftragsverarbeiter können von den Aufsichtsbehörden angewiesen werden, Betroffenenrechten zu entsprechen und Datenverarbeitungsvorgänge an die Verordnung anzupassen. Auch muss ein Verantwortlicher auf Weisung der Aufsichtsbehörde von einem Datenschutzverstoß betroffene Personen benachrichtigen.

Wie bisher können Aufsichtsbehörden überdies eine Datenverarbeitung beschränken oder auch verbieten sowie die Berichtigung und Löschung von Daten oder eine eingeschränkte Verarbeitung und die Unterrichtung von Datenempfängern über solche Maßnahmen anordnen.

Außerdem wird es künftig möglich sein anzuordnen, dass Datenübermittlungen an einen Empfänger in einem Drittland oder an eine internationale Organisation

74 Art. 6 Abs. 1 lit. f
75 Erwägungsgrund (148)
76 Art. 58 Abs. 2

ausgesetzt werden, und anzuweisen, dass Zertifizierungsstellen erteilte Zertifizierungen widerrufen müssen bzw. Zertifizierungen nicht erteilen dürfen.

Zusätzlich oder anstelle der vorgenannten Maßnahmen können die Aufsichtsbehörden auch Geldbußen verhängen. Die Bußgeldtatbestände wurden im Vergleich zur bisherigen Rechtslage deutlich ausgeweitet.[77] Bußgelder müssen nach den neuen Regelungen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein.[78]

Der Bußgeldrahmen wurde daher deutlich erhöht. So können bei schweren Verstößen oder Nichtbefolgung einer Anweisung der Aufsichtsbehörde Bußgelder in Höhe von bis zu 20 Millionen Euro bzw. im Fall eines Unternehmens auch von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden.

Für die konkrete Bestimmung der Höhe eines Bußgeldes muss eine Vielzahl von Aspekten einbezogen werden.[79] Neben Art, Schwere und Dauer des Verstoßes ist u. a. zu berücksichtigen, welche Art von Daten rechtswidrig verarbeitet wurde und ob finanzielle Vorteile durch die Datenverarbeitung erlangt wurden. Zu beachten ist ebenfalls, ob und wie die oder der Verantwortliche oder ein Auftragsdatenverarbeiter mit der Aufsichtsbehörde zusammengearbeitet hat, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern, und ob die Stellen die Verstöße eigenständig der Aufsichtsbehörde mitgeteilt haben.

Wenn Unternehmen Bußgelder auferlegt werden, ist zu beachten, dass der sog. funktionale Unternehmensbegriff anzuwenden ist.[80] Danach ist ein Unternehmen jede wirtschaftliche Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung.[81] Eine wirtschaftliche Einheit kann aus mehreren natürlichen oder juristischen Personen bestehen. Sie liegt insbesondere dann vor, wenn eine Mut-

77 Art. 83 Abs. 4 bis 6

78 Art. 83 Abs. 1

79 Art. 83 Abs. 2 Satz 2

80 Erwägungsgrund (150) mit Verweis auf Art. 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union – AEUV

81 Ständige Rechtsprechung des EuGH; z. B. EuGH, Slg. 1991, I-2010, Rn. 21, EuGH, Slg. 2006, I-6391, Rn. 25

tergesellschaft auf eine Tochtergesellschaft einen bestimmenden Einfluss ausübt. Davon ist regelmäßig bei einem Stimmenanteil an der Tochtergesellschaft von über 50 % auszugehen. Allerdings genügt auch die tatsächliche Möglichkeit der Kontrolle und Einflussnahme unabhängig von einer starren Beteiligungsschwelle.[82]

Die Anwendung dieses im Kartellrecht wurzelnden funktionalen Unternehmensbegriffs hat u. a. für die Höhe der zu verhängenden Bußgelder weitreichende Folgen, da die Basis der Bußgeldberechnung der weltweite Unternehmensumsatz ist. Begeht z. B. eine Unternehmenstochter einen durch Bußgeld zu ahndenden Verstoß und liegt eine wirtschaftliche Einheit mit der Muttergesellschaft vor, so bildet der gesamte weltweite Konzernumsatz (Mutter plus Tochter) die Berechnungsgrundlage für die Höhe des Bußgeldes.[83]

Die Anwendung des funktionalen Unternehmensbegriffs wirkt sich auch auf haftungsrechtliche Fragen aus. Denn nach der hierfür maßgeblichen kartellrechtlichen Rechtsprechung genügt für die Verantwortlichkeit eines Unternehmens bzw. einer Unternehmensvereinigung die Handlung einer Person, die berechtigt ist, für das Unternehmen bzw. die Unternehmensvereinigung tätig zu werden.[84] Erfasst sind daher nicht nur wie bisher die gesetzlichen Vertreter oder Leitungspersonen,[85] sondern sämtliche Bedienstete oder auch Beauftragte außerhalb des Unternehmens oder der Unternehmensvereinigung.[86] Eine Kenntnis der Inhaber oder Geschäftsführer des Unternehmens von der konkreten Handlung oder eine Verletzung der Aufsichtspflicht[87] ist für die Zuordnung der Verantwortlichkeit nicht erforderlich, wobei Exzesse ausgenommen sind.[88] Darüber hinaus können bei Vorliegen einer wirtschaftlichen Einheit für ein Fehlverhalten der Tochtergesellschaft Mutter und Tochter gesamtschuldnerisch herangezogen werden, ohne dass die

82 Siehe EuGH, Beschluss vom 10. Mai 2007, Rs. C-492/04 – Lasertec

83 Siehe auch § 81 Abs. 4 Satz 3 GWB

84 EuGH, Urteil vom 7. Juni 1983 Musique Diffusion française, 100-103/80, Slg. 1983,1825, Rn. 97; EuG, Urteil vom 29. April 2004 – Tokai Carbon,T-236/01, Slg. 2004, 1181, Rn. 278

85 § 30 Abs. 1 OWiG

86 Siehe EuGH, Urteil vom 7. Februar 2013 – Protimonopolný úrad Slovenskej republiky, C68/12, Rn. 25-28

87 Bisher gemäß § 130 OWiG notwendig

88 Siehe Karlsruher Kommentar zum OWiG, Rogall, Rn. 249 zu § 30

Beteiligung der Mutter nachgewiesen werden müsste.[89] Auch bei Umstrukturierungen verbleibt die Haftung im Konzern bzw. geht auf die Rechtsnachfolge über.

Unsere Bußgeldpraxis wird sich durch die neuen Bestimmungen deutlich ändern. Insbesondere müssen Unternehmen bei Verstößen gegen die DS-GVO mit erheblich höheren Bußgeldern rechnen.

1.2.5 Was Forscher und Wissenschaftler zu beachten haben

Forschung wird an verschiedenen Stellen der DS-GVO erwähnt. Eine konkrete inhaltliche Forschungsklausel enthält die DS-GVO aber nicht. Art. 89 DS-GVO regelt seinem Titel entsprechend nur Garantien und Ausnahmen in Bezug auf die Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken. Zu den dort genannten geeigneten Garantien gehören neben den in der DS-GVO geregelten Grundsätzen für die Verarbeitung personenbezogener Daten[90] und der Datenschutz-Folgenabschätzung auch die Rechtmäßigkeitsanforderungen.

Grundsätzlich kommt ein Forschungsanliegen in Betracht, sofern es zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse[91] liegt. Nach der DS-GVO[92] soll allerdings auch explizit privat finanzierte Forschung unter den Begriff der wissenschaftlichen Forschungszwecke fallen. Als Rechtsgrundlage kommt nach wie vor eine Einwilligung in Betracht, an die spezifische Anforderungen zu stellen sind.[93] Es wird keine Schriftform verlangt.[94] Allerdings muss der Verantwortliche nachweisen können, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten zugestimmt hat. Es steht dem Verantwortlichen frei, eine geeignete – auch elektronische – Form zu wählen.

89 Ständige Rechtsprechung, etwa EuGH, Urteil vom 20. Januar 2011 – General Quimka, C-90/09 P, Slg. 2011, I-0001, Rn. 85, 89

90 Art. 5 DS-GVO

91 Art. 6 Abs. 1 lit. e DS-GVO

92 Erwägungsgrund (159)

93 Art. 7 DS-GVO

94 Im Gegensatz zum bisherigen § 4a Abs. 1 S. 3 BDSG

Offenbar soll es häufig nicht möglich sein, den konkreten Zweck einer Datenverarbeitung für wissenschaftliche Forschungszwecke zum Zeitpunkt der Erhebung personenbezogener Daten vollständig anzugeben.[95] Dies bezieht sich scheinbar auf langfristig angelegte Forschungsvorhaben mit einem offenen Forschungsansatz sowie auf Biobanken, die Bioproben ohne konkrete Zweckbestimmung für zukünftig mögliche Analysen lagern. Vor diesem Hintergrund soll es betroffenen Personen erlaubt sein, ihre Einwilligung in bestimmte Bereiche wissenschaftlicher Forschung zu geben.

Dieser Ansatz wird als „Broad Consent" bezeichnet und war bisher wegen der mangelnden Bestimmtheit umstritten. Die DS-GVO versucht einen Kompromiss insofern herzustellen, als die Einhaltung anerkannter ethischer Standards der wissenschaftlichen Forschung gefordert wird. Konkret sollen Probanden die Gelegenheit erhalten, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten zu erteilen. Es muss also je nach Einzelfall eine Aufbereitung des Forschungsvorhabens erfolgen und die größtmögliche Transparenz und Dispositionsmöglichkeit für die Teilnehmerinnen und Teilnehmer an Forschungsprojekten hergestellt werden. Jedenfalls ist eine pauschale Forschungseinwilligung nicht möglich.

Werden – wie etwa in der Gesundheitsforschung – besondere Kategorien personenbezogener Daten verarbeitet, sind spezifische Anforderungen zu erfüllen. Grundsätzlich ist eine Einwilligung einzuholen, wenn nicht eine der genannten Ausnahmen greift.[96] Es bleibt abzuwarten, in welcher Form der deutsche Gesetzgeber von der Öffnungsklausel in diesem Bereich Gebrauch macht.[97] Auch sollen wohl die Betroffenenrechte durch nationales Recht wieder eingeschränkt werden.[98]

Zudem finden sich in der DS-GVO für bestimmte Forschungsbereiche relevante Definitionen, wie die für Gesundheitsdaten.[99] Auch die Pseudonymisierung, eine wesentliche technisch-organisatorische Maßnahme im Forschungsbereich, wird

95 Erwägungsgrund (33)
96 Art. 9 Abs. 2 DS-GVO
97 Art. 9 Abs. 2 lit. j DS-GVO
98 Art. 9 Abs. 4 bzw. Art. 89 Abs. 2 DS-GVO; siehe auch 1.2.1
99 Art. 4 Ziff. 15 DS-GVO

definiert.[100] Pseudonymisierte Daten sind als Informationen über eine identifizierbare Person zu betrachten.[101] Schließlich sollen Pseudonymisierungsmaßnahmen bei demselben Verantwortlichen möglich sein.[102] D. h. es soll ausreichen, dass neben den eigentlichen Forschungsdaten auch die die Zuordnung zu einer Person ermöglichenden Informationen bei dem Verantwortlichen intern gesondert gespeichert werden. Die genaue Ausgestaltung der „erforderlichen technischen und organisatorischen Maßnahmen" wird im Einzelfall zu prüfen sein.

Nicht definiert wird der für die Forschung relevante Begriff der Anonymisierung. Es wird allerdings – explizit auch in Bezug auf Forschung – die Geltung der Datenschutzgrundsätze für anonyme Informationen ausgeschlossen.[103] Da ein hoher und unverhältnismäßiger Aufwand für die Identifizierung einer Person nicht als ausreichend genannt wird, muss eine absolute Anonymisierung vorliegen.

1.2.6 Auswirkungen auf die Informationsfreiheit

Nach der DS-GVO haben die Mitglieder der Aufsichtsbehörde von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen abzusehen und während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit auszuüben.[104] Im Hinblick auf die Aufgaben als Informationsfreiheitsbeauftragte[105] besteht indes kein Interessenkonflikt, da diese nicht unvereinbar mit den Aufgaben als Datenschutzbeauftragte sind. Vielmehr ermöglicht die Personalunion beider Ämter einen konstruktiven Ausgleich zwischen den Belangen des Datenschutzes und der Informationsfreiheit: Dies hat sich auch in der bisherigen guten Praxis vieler Aufsichtsbehörden gezeigt. Weder nach der bisherigen Rechtslage noch nach der DS-GVO spricht etwas dagegen, dass die Datenschutzbeauftragten zugleich Aufgaben als Informationsfreiheitsbeauftragte wahrnehmen.

100 Art. 4 Ziff. 5 DS-GVO
101 Erwägungsgrund (26)
102 Erwägungsgrund (29)
103 Erwägungsgrund (26)
104 Art. 52 Abs. 3 DS-GVO
105 Siehe § 18 Berliner Informationsfreiheitsgesetz (IFG)

Eine Angleichung der Aufgaben und Befugnisse der Datenschutzbeauftragten auf die Informationsfreiheitsbeauftragten ist rechtspolitisch nicht geboten. Anders als die Datenschutzbeauftragten werden die Informationsfreiheitsbeauftragten primär als Schlichtungsstelle sowie beratend gegenüber den Antragstellerinnen und Antragstellern sowie den informationspflichtigen Stellen tätig. Dies verträgt sich nicht mit Anordnungs- bzw. Durchsetzungsbefugnissen.

Um die eigenständige Bedeutung der Informationsfreiheit zu verdeutlichen, wäre es jedoch wünschenswert, die Aufgaben und Befugnisse der Berliner Beauftragten für Informationsfreiheit unmittelbar in das IFG aufzunehmen.[106]

1.3 Starker Verbesserungsbedarf beim Gesundheitsdatenschutz in der öffentlichen Verwaltung

Der öffentlichen Verwaltung obliegt es in vielfacher Weise, durch die Erhebung und Verarbeitung von Gesundheitsdaten für den öffentlichen Gesundheitsschutz zu sorgen und Bürgerinnen und Bürger in ihren gesundheitlichen Anliegen zu beraten. Wir geben Hinweise im Zuge der Schaffung der erforderlichen landesrechtlichen Grundlagen für diese Tätigkeit und begleiten die Einführung von technischen Verfahren, soweit uns diese rechtzeitig vorgestellt werden.

Am öffentlichen Gesundheitsschutz sind in Berlin eine ganze Reihe von Institutionen beteiligt: Angefangen von der für Gesundheit zuständigen Senatsverwaltung und ihren nachgeordneten Behörden wie dem Landesamt für Gesundheit und Soziales und dem Landesinstitut für gerichtliche und soziale Medizin über die Gesundheitsämter der Bezirke, die mit verschiedenen Diensten wie z. B. dem Kinder- und Jugendgesundheitsdienst und dem Sozialpsychiatrischen Dienst sowie zahlreichen Beratungsstellen das Herzstück des öffentlichen Gesundheitsdienstes bilden, bis hin zu Einrichtungen wie der Zentralen Medizinischen Gutachtenstelle, der Gewaltschutzambulanz und den Kinderschutzambulanzen,

106 Bislang gibt es lediglich einen Verweis in § 18 Abs. 2 Satz 2 IFG auf die Befugnisse nach dem Berliner Datenschutzgesetz (BlnDSG).

den Zentralen Stellen für das Einladungswesen für Früherkennungsuntersuchungen und für das Mammographie-Screening, dem epidemiologischen und dem klinischen Krebsregister und nicht zuletzt dem Krankenhaus des Maßregelvollzugs.

Gesetzliche Grundlage für die Tätigkeit des Berliner Gesundheitsdienstes bildet das **Gesundheitsdienst-Gesetz (GDG)**. Hier werden die Aufgaben und die Struktur des Gesundheitsdienstes festgeschrieben sowie der Rahmen für die Zuständigkeiten vorgegeben. Bereits 2015 haben wir festgestellt, dass insbesondere für die Gesundheitsberichterstattung Rechtsgrundlagen für die vorgenommenen Datenflüsse fehlen.[107] Die grundlegende Verordnung über die Verarbeitung von personenbezogenen Daten und die Schweigepflicht im Gesundheitsdienst regelt lediglich die Schaffung und Auswertung anonymisierter Datenbestände. Dies reicht nicht aus, um die für die Tätigkeit des öffentlichen Gesundheitsdienstes zwingend erforderlichen Datenverarbeitungen auf eine rechtliche Grundlage zu stellen.

Abhilfe soll der Erlass einer **Verordnung zur Regelung der Datenverarbeitung in Einrichtungen des öffentlichen Gesundheitsdienstes (DatVO)** schaffen. 2015 konnten wir berichten, dass die zuständige Senatsverwaltung die Arbeit an der DatVO nach knapp zweijährigem Stillstand wieder aufgenommen hat.[108] Diese Arbeit wurde auch 2016 fortgeführt. Zuletzt hat uns die Senatsverwaltung für Gesundheit und Soziales im November 2016 einen weiteren – wenn auch unvollständigen – Verordnungsentwurf zukommen lassen. Wir werden den Prozess weiterhin eng begleiten und auf den baldigen Erlass der Rechtsverordnung hinwirken. Dieser ist überfällig.

Über die Regelung der Datenflüsse zwischen den Behörden hinaus bedarf auch der Umgang mit den anvertrauten und geheim zu haltenden Patientendaten innerhalb der Behörden der Regelung. Das Gesetz legt allgemein fest, dass im Gesundheitsdienst die Berufsgeheimnisse und insbesondere die ärztliche Schweigepflicht zu wahren sind. Genau mit dieser berechtigten Erwartung kommen die Bürgerinnen und Bürger in die Gesundheitsämter und andere Einrichtungen.

107 JB 2015, 8.1
108 JB 2015, 8.1

Doch kann ihr überhaupt entsprochen werden? Kommen tatsächlich nur Personen mit den Daten in Berührung, die selbst der strafbewehrten Schweigepflicht unterliegen? Liegt die Regelung der Zugriffsmöglichkeiten wirklich effektiv in der Hand der obersten selbst der Schweigepflicht unterliegenden Leitung? Wie weit geht z. B. das Weisungsrecht der Amtsärztinnen und Amtsärzte gegenüber den IT-Stellen der Bezirke? Was passiert, wenn ihre Dispositionsgewalt durch mangelhafte Technik und fehlende Ressourcen so eingeschränkt wird, dass es zu ungewollten Offenlegungen von Daten an unbeteiligte Beschäftigte kommen kann?

Schon die Frage, auf welcher Grundlage die Beschäftigten in den IT-Stellen der Bezirksämter und anderen Behörden sowie ggf. eingeschaltete Dienstleister mit den geheim zu haltenden Daten umgehen, ist ungeklärt. Es ist unvermeidbar, dass zumindest einige der dort Beschäftigten mit den Daten in Berührung kommen und sie ggf. auch zur Kenntnis nehmen können. Diesen Personen dürfen die Daten aber nur zur Kenntnis gegeben werden, wenn sie der unmittelbaren Kontrolle und Weisung der Schweigepflichtigen unterstehen. Dies ist bereits für Beschäftigte separater IT-Stellen fraglich, für Dienstleister, darunter auch das IT-Dienstleistungszentrum Berlin, jedoch offensichtlich nicht der Fall. Der Landesgesetzgeber ist daher dringend aufgerufen, eine Regelung zu schaffen, die eine Weitergabe dieser besonders geheimhaltungsbedürftigen Daten unter engen Voraussetzungen erlaubt und die zugleich eine etwaige Verletzung der Geheimhaltungspflicht durch dieses Personal und externe Dienstleister unter Strafe stellt.

Geregelt ist das Vorgehen bei der Einführung von Datenverarbeitungsverfahren: Zunächst müssen die Rechtsgrundlagen geprüft werden. Dazu muss bekannt sein, welche Daten von wem für welchen Zweck wie verarbeitet werden sollen. In der Regel handelt es sich dabei um einen komplexen Verarbeitungsprozess, der die Erledigung einer oder mehrerer Fachaufgaben unterstützt. Im Kontext von Aufgaben und Prozessen ist zu bewerten, ob der Umfang der zu verarbeitenden Daten und der Umgang mit ihnen im Rahmen des Erforderlichen bleiben.

Für die Planung der nötigen technischen und organisatorischen Maßnahmen muss es eine Risikoanalyse und ein Sicherheitskonzept geben. Eine Kontrolle der vorgesehenen Verarbeitung vor ihrer Aufnahme, eine sog. Vorabkontrolle, ist vorgeschrieben. Vielfach ist unsere Behörde daran zu beteiligen. Dafür haben wir

eine Aufstellung der benötigten Unterlagen veröffentlicht.[109] Die Unterlagen dienen dazu, die nötigen Vorarbeiten und ihre Ergebnisse zu dokumentieren. Doch oft erhalten wir diese nicht oder müssen sogar feststellen, dass die Vorarbeiten nicht erledigt wurden. Hierfür trägt die Leitung der datenverarbeitenden Behörden die Verantwortung, auch wenn die Vorabkontrolle zunächst Aufgabe der behördlichen Datenschutzbeauftragten ist.

Besonders gravierend wirkt es sich aus, wenn die Behörde oder Institution über kein Sicherheitskonzept für die eigene IT-Infrastruktur verfügt, das den Schutzbedarf von Gesundheitsdaten berücksichtigt. Diese Infrastruktur besteht in der Regel aus dem IT-Netzwerk, den wichtigsten Servern und den von ihnen angebotenen allgemeinen Diensten sowie den Rechnern, die sich auf den Arbeitsplätzen der Beschäftigten befinden. Viele Anforderungen an die Sicherheit eines Fachverfahrens lassen sich dadurch erfüllen, dass eine entsprechend vorgestaltete Infrastruktur in Anspruch genommen wird. Nur das Spezielle an einem Verfahren und seine Interaktion mit der bestehenden Infrastruktur bedürfen dann noch der Betrachtung.

Defizitäre und gänzlich fehlende behördliche Sicherheitskonzepte haben wir insbesondere bei einigen Bezirksämtern bemängelt.[110] Leider führte dies nicht durchgehend dazu, dass die Mängel abgestellt wurden. So hat das Bezirksamt Steglitz-Zehlendorf auch zwei Jahre nach unserer formellen Beanstandung[111] weder ein behördliches Sicherheitskonzept noch ein Sicherheitskonzept für das beanstandete Verfahren mit hoch sensitiven Daten und betreibt dieses mit unklaren Risiken weiter.

2014 haben wir auch ein völlig ungeregelt eingeführtes **Verfahren für den Kinder- und Jugendgesundheitsdienst (KJGD)** des Bezirks Friedrichshain-Kreuzberg bemängelt, das daraufhin pflichtgemäß eingestellt wurde. Der offenkundige Bedarf des KJGD in ganz Berlin an informationstechnischer Unterstützung sollte durch zentral beschaffte Software gedeckt werden. Wir unterstützen diesen Prozess und

109 https://datenschutz-berlin.de/attachments/1068/2014-Handreichung_beteiligung_vorabkontrolle.pdf

110 JB 2014, 1.5

111 JB 2014, 5.6

haben detaillierte Hinweise für die Verfahrenseinführung gegeben. Doch die benötigten Konzepte kamen bisher nicht zustande. Bezirke und das Landesamt für Gesundheit und Soziales weisen sich gegenseitig die Verantwortung zu. Die im E-Government-Gesetz[112] vorgesehene Koordination und Regelung durch die zentrale Steuerung der Informations- und Kommunikationstechnik wird das Ihre tun müssen, um Blockaden wie diese zu vermeiden. Doch bleibt es dabei: Die Verantwortung für die korrekte Einführung eines Verfahrens liegt bei den datenverarbeitenden Stellen, hier also bei den Bezirksämtern.

Auch wenn ein Bundesgesetz Berliner Behörden Aufgaben zuweist und bestimmte Datenübermittlungen anordnet, entbindet dies die Behörden nicht von der Pflicht, die dazu nötigen informationstechnischen Verfahren datenschutzgerecht zu planen und einzuführen. So weist das **Infektionsschutzgesetz** die Gesundheitsämter der Bezirke an, Meldungen über bestimmte übertragbare Krankheiten zu erfassen. Zur Meldung sind Ärztinnen und Ärzte sowie weitere Berufsgruppen verpflichtet. Die Meldungen enthalten die Namen der Erkrankten. Die Gesundheitsämter sind verpflichtet, die Daten ohne die Namen über das Landesamt für Gesundheit und Soziales an das Robert-Koch-Institut weiterzugeben.

Zur Erfüllung dieser Pflicht und Erledigung weiterer Aufgaben haben die Gesundheitsämter die Entwicklung einer umfangreichen Software in Auftrag gegeben. Auch hier gelang es nicht, über eine Zusammenarbeit zwischen Landesamt für Gesundheit und Soziales und Bezirksämtern die nötigen Konzepte zu entwickeln. Stattdessen entschieden sich die Gesundheitsämter, kurzfristig eine einfachere, frei verfügbare Software einzusetzen. Inwieweit sie eine Vorabkontrolle durchgeführt haben, ist uns (mit Ausnahme eines Amtes) nicht bekannt. Wir wurden lediglich von der Aufnahme der Verfahren informiert, jedoch nicht beteiligt. Rechtmäßig ist eine Erfassung der Meldungen daher derzeit nur, wenn die Namen der Erkrankten nicht in das System aufgenommen werden, sodass für die Betroffenen keine Risiken entstehen.

Intensiv einbezogen wurden wir in die **Errichtung des klinischen Krebsregisters der Länder Berlin und Brandenburg**. Diese erfolgte nach Verzögerungen bei der Schaffung der Rechtsgrundlagen über einen Staatsvertrag zwischen den beiden

112 § 21 E-Government-Gesetz Berlin; siehe auch 2.1

Ländern[113] unter erheblichem Zeitdruck. Das Register wurde feierlich eröffnet, ohne dass die vorgesehene Informationstechnik bereitstand. Stattdessen griff das Register auf die Technik der brandenburgischen Vorläuferinstitution zurück.

Leider wurden dabei auch einfache Anpassungen an die neuen Umstände nicht durchgeführt. So blieb die Technik einer von uns geprüften Registerstelle integriert in das Netzwerk eines Krankenhauses. Nur ein kleiner Teil der erfassten Krebskranken wurde jedoch dort behandelt. Die Daten der anderen Patientinnen und Patienten haben in der IT eines fremden Krankenhauses nichts zu suchen. Weitere festgestellte Mängel bezogen sich auf den mangelnden Einbruchsschutz und die freie Zugänglichkeit der Papiermeldungen in der Dienststelle, das Fehlen von vorgeschriebener Funktionalität der zentralen Registersoftware und wenig differenzierte Zugriffsberechtigungen. Einige dieser Mängel werden mit gewissem Aufwand zu beheben sein, ggf. durch einen Umzug der Registerstelle in geeignetere Räume. Unsere Zweifel an der grundsätzlichen Eignung der zentralen Registersoftware, die beibehalten werden soll, sind dagegen noch nicht ausgeräumt.

Erst mit der vollständigen Umsetzung der geplanten IT-Infrastruktur wird das Register über angemessene technische Maßnahmen zum Schutz von Netzwerk und Datenbanken verfügen. Wir begrüßen die Bereitschaft des klinischen Krebsregisters, Beratung durch unsere Behörde und die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg zu suchen und unsere Hinweise aufzunehmen. Die Länder tätigen die hierfür nötigen Investitionen. Die entstandene Schutzlücke ist jedoch problematisch und geht zu Lasten der Betroffenen.

Die Nagelprobe für das Register wird darin bestehen, seine internen Prozesse mit besonderem Augenmerk auf den notwendigen besonderen Schutz der hoch sensitiven Daten auszurichten. Diese Verpflichtung hat das Register gegenüber den Krebskranken, deren Daten ihm in der Hoffnung auf eine Verbesserung der Qualität der Behandlung ohne ihr Zutun anvertraut werden.

113 Siehe JB 2015, 8.2

Neue IT-Verfahren in der Gesundheitsverwaltung bedürfen der sorgfältigen Einführung. Notwendige Rechtsgrundlagen sind rechtzeitig zu schaffen. Technischer Schutz ist nach dem Stand der Technik zu gewährleisten. Die Verfahren sind vor der Aufnahme ihres Betriebs zu kontrollieren, verwaltungsübergreifende Verfahren unter unserer rechtzeitigen Beteiligung.

1.4 Rechtliche Grenzen des Outsourcings von Patientendaten im Krankenhausbereich am Beispiel der Digitalisierung und Archivierung von Patientenakten

Bedingt durch den steigenden wirtschaftlichen Kostendruck haben einige Kliniken Tochtergesellschaften gegründet, um bestimmte im Krankenhaus anfallende Dienstleistungen auszulagern. Auf unsere Initiative hin wurde 2011 bei der Novellierung des Landeskrankenhausgesetzes[114] eine Regelung geschaffen, die es ermöglicht, dass bei der Übertragung von Dienstleistungen an Dritte, wie z. B. Patiententransport und Speisenversorgung, die für die Erbringung dieser Leistungen notwendigen Patientendaten den Dritten bekannt gegeben werden dürfen. Von dieser Regelung werden jedoch nur Funktionsübertragungen erfasst, die nicht im unmittelbaren inneren Zusammenhang mit dem Behandlungsgeschehen stehen und bei denen es nicht zu einer Verarbeitung medizinischer Daten der Patientinnen und Patienten kommt.

Mittlerweile gibt es Bestrebungen, weitere Tätigkeiten, die den inneren Bereich des Krankenhauses betreffen und bei denen unmittelbar medizinische Daten verarbeitet werden, wie die Archivierung und Digitalisierung von Patientenakten, ebenfalls an Dritte auszulagern. Bei dieser Tätigkeit ist es unumgänglich, anvertraute Patientendaten zur Kenntnis zu nehmen. Es handelt sich dabei um eine Auftragsdatenverarbeitung, die für Krankenhäuser ebenfalls im Landeskrankenhausgesetz geregelt ist und für deren Zulässigkeit bestimmte Vorgaben bestehen.[115] So ist eine Auftragsdatenverarbeitung nur dann zulässig, wenn die

114 Siehe JB 2011, 2.2.2
115 § 24 Abs. 7 LKG

Patientendaten durch das Krankenhaus selbst oder im Auftrag durch ein anderes Krankenhaus verarbeitet werden. Durch andere Stellen dürfen Patientendaten im Auftrag des Krankenhauses nur dann verarbeitet werden, wenn durch technische Schutzmaßnahmen sichergestellt ist, dass der Auftragnehmer keine Möglichkeit hat, beim Zugriff auf die Patientendaten den Personenbezug herzustellen.

Soweit Archivdienstleistungen durch das Krankenhaus selbst geleistet werden, unterliegen die mit dieser Aufgabe betrauten Mitarbeiterinnen und Mitarbeiter als Gehilfen des ärztlichen Personals der beruflichen Schweigepflicht. Durch die Auslagerung dieser Aufgabe an einen Dienstleister, bei dem die Beschäftigten nicht der ärztlichen Schweigepflicht unterliegen, würden schweigepflichtige Daten unzulässig und strafbewehrt offenbart.

Eine Möglichkeit, dem zu begegnen, besteht darin, diese Aufgabe durch die Einbeziehung des Dienstleisters im Wege der Arbeitnehmerüberlassung ausführen zu lassen. Die Mitarbeiterinnen und Mitarbeiter sind in diesem Fall in den organisatorischen und weisungsgebundenen internen Bereich des Krankenhausbetriebes eingebunden und üben innerhalb des beruflichen Wirkungskreises eines Schweigepflichtigen eine auf dessen berufliche Tätigkeit bezogene unterstützende Tätigkeit aus, die die Kenntniserlangung von fremden Geheimnissen zwingend mit sich bringt. Sie sind damit als Gehilfen des ärztlichen Personals anzusehen und unterliegen insoweit ebenfalls der Schweigepflicht.

Aufgrund von Änderungen bei der rechtlichen Regelung zur Arbeitnehmerüberlassung wurde von den Kliniken vorgetragen, dass die Einbindung eines externen Dienstleisters über den Weg der Arbeitnehmerüberlassung zukünftig keine wirtschaftlich tragbare Lösung mehr sei.

Bei allen Erwägungen, den wirtschaftlichen Belastungen begegnen zu können, muss jedoch der Schutz der sensitiven Patientendaten, die im Rahmen der ärztlichen Schweigepflicht anvertraut wurden, immer höchste Priorität haben. Nach jetziger Rechtslage reicht allein die Zusammenarbeit mit einem Tochterunternehmen oder einem externen Dienstleister nicht aus, um den Beschäftigten des Dienstleisters einen Gehilfenstatus zu verschaffen. Es bestehen zwei rechtlich selbstständige Unternehmen, die gerade nicht über eine gesellschaftsrechtliche Konstruktion zu einer maßgeblichen Funktionseinheit werden. Eine vom Kranken-

haus ausgegründete Tochtergesellschaft ist nicht als funktionaler Teil der Einrichtung Krankenhaus anzusehen. Die im Landeskrankenhausgesetz vorgenommene Definition lässt keinen Raum für eine Erweiterung auf Tochterunternehmen, die geschaffen werden, um gerade nicht Teil des Krankenhauses zu sein, sondern um selbstständig handeln zu können.

Die im Landeskrankenhausgesetz vom Gesetzgeber getroffene Regelung zur Auftragsdatenverarbeitung im Krankenhausbereich verfolgt den Zweck, den Kreis der Personen, die mit medizinischen, also sensitiven Daten in Berührung kommen, möglichst klein und das Schutzniveau der Patientendaten möglichst hoch zu halten. Durch die Beteiligung externer Stellen wird der Kreis derer, die mit medizinischen Daten in Berührung kommen, größer. Um dem zu begegnen, hat der Gesetzgeber ganz bewusst enge Grenzen gesteckt. Überdies entspricht die für Berliner Krankenhäuser geltende Regelung den europarechtlichen Vorgaben der Datenschutz-Grundverordnung. Danach dürfen Gesundheitsdaten zum Zwecke der Gesundheitsvorsorge nur von Fachpersonal, das dem Berufsgeheimnis unterliegt, oder unter dessen Verantwortung verarbeitet werden oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls einer Geheimhaltungspflicht unterliegt. Damit sind im Bereich der Verarbeitung von Gesundheitsdaten Übermittlungen und Outsourcing an Dritte, die nicht selbst einer Schweigepflicht unterliegen, unzulässig.

Neben der Möglichkeit der Einbindung externer Kräfte im Wege der Arbeitnehmerüberlassung wäre eine Legitimierung von an Dritte übertragenen Archivdienstleistungen langfristig nur durch eine Anpassung der gesetzlichen Regelung zur beruflichen Schweigepflicht durch den Bundesgesetzgeber denkbar. Das grundsätzliche Problem der Einbindung externer Dienstleister bei der Schweigepflicht unterliegenden Berufsgruppen ist dem Bundesgesetzgeber bereits bekannt, da sich auch bei anderen der Schweigepflicht unterliegenden Berufsgruppen, wie beispielsweise Rechtsanwälten, vergleichbare Probleme ergeben.

Unter Berücksichtigung der Rechtslage ist eine Auslagerung von Dienstleistungen im Krankenhaus nur in sehr engen Grenzen zulässig, um dem Schutzbedarf der anvertrauten sensitiven Patientendaten Rechnung zu tragen. Eine neue gesetzliche Regelung muss gewährleisten, dass die Kenntnisnahme von

Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird und die Dienstleister ebenfalls der Schweigepflicht unterworfen werden. Auch muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt werden.

1.5 Einsatz von Stillen SMS in strafrechtlichen Ermittlungsverfahren

Wir haben den Einsatz von Stillen SMS in strafrechtlichen Ermittlungsverfahren geprüft und hierbei gravierende Mängel festgestellt.

Strafverfolgungsbehörden benutzen Stille SMS, um unbemerkt herauszufinden, wo sich das jeweils adressierte Telefon bzw. sein Besitzer befindet. Hierfür versenden sie einen Ortungsimpuls an ein Telefon, der nicht im Telefondisplay angezeigt wird und der auch kein akustisches Empfangssignal auslöst, jedoch bewirkt, dass von diesem Telefon eine technische Meldung an den Telekommunikationsanbieter übermittelt wird. Die Meldung enthält Angaben über das Telefon, insbesondere dessen Standort und Anschlusskennung. Die Daten werden sodann beim Telekommunikationsanbieter aus technischen Gründen bzw. zur Ermöglichung der Abrechnung von erbrachten Leistungen für einen gewissen Zeitraum gespeichert.[116] Die Notwendigkeit der Datenspeicherung durch den Telekommunikationsanbieter zu vorgenannten Zwecken nutzen nun die Ermittlungsbehörden, um die Daten, die sie selbst erzeugt haben, zu Strafverfolgungszwecken abzurufen.[117]

Zur Vorbereitung der Prüfung baten wir den Leitenden Oberstaatsanwalt und den Polizeipräsidenten um Übersendung einer Liste der zuletzt durchgeführten Ermittlungsverfahren, in denen Stille SMS versandt worden sind. Dies war den Straf-

116 Siehe zur Zulässigkeit der Erhebung und Verwendung der Daten § 96 Abs. 1 Satz 1 TKG; Telekommunikationsanbieter sind zudem gem. § 150 Abs. 13 Satz 1 i. V. m. §§ 113 b, c TKG verpflichtet, spätestens ab dem 1. Juli 2017 Verkehrsdaten auch zu Zwecken der Strafverfolgung und Gefahrenabwehr zu speichern (sog. Vorratsdatenspeicherung).

117 Siehe zur Zulässigkeit der Verwendung der Daten zu anderen Zwecken § 96 Abs. 1 Satz 2 TKG

verfolgungsbehörden mangels gesonderter Erfassung des Einsatzes von Stillen SMS in den jeweiligen Informationssystemen nach eigenen Angaben nicht möglich. Damit wir die Prüfung dennoch durchführen konnten, bot uns der Polizeipräsident an, für einen bestimmten zukünftigen Erhebungszeitraum technisch eine manuelle Abfrage im System der Telekommunikationsüberwachung einzurichten.

Wir haben diesem Vorschlag zugestimmt und die so dokumentierten, in der Zeit von Dezember 2014 bis August 2015 durchgeführten Strafermittlungsverfahren[118] stichprobenartig geprüft. Hierfür haben wir 38 Akten im Rahmen einer Vor-Ort-Prüfung im Juni dieses Jahres bei der Staatsanwaltschaft ausgewertet. Die geprüften Akten betrafen insbesondere Straftaten nach dem Betäubungsmittelgesetz, Straftaten des Raubes und der Erpressung, Bandendiebstähle und schwere Bandendiebstähle, Geld- und Wertzeichenfälschung sowie Mord und Totschlag.

Die rechtliche Würdigung der von uns geprüften Fälle gestaltete sich aufgrund der unklaren Rechtslage schwierig. Es gibt keine gesetzliche Norm, die nach ihrem Wortlaut den Einsatz von Stillen SMS in strafrechtlichen Ermittlungsverfahren erlaubt. Deshalb ist ihr Einsatz in Wissenschaft und Praxis äußerst umstritten. Die Rechtsprechung hat die Zulässigkeit der Maßnahme noch nicht überprüft. Der Leitende Oberstaatsanwalt erklärte, dass die Ermittlungsgeneralklausel § 163 Abs. 1 Strafprozessordnung (StPO) die Rechtsgrundlage für die Versendung von Stillen SMS darstelle. Die so anfallenden Daten könnten dann durch einen gerichtlichen Beschluss nach § 100g StPO erlangt werden. Der Polizeipräsident hingegen stützt die Maßnahme allein auf die Bestimmungen des § 100a StPO. Die Stille SMS sei eine Einzelmaßnahme, die im Rahmen angeordneter Maßnahmen der Telekommunikationsüberwachung durchgeführt werde und keiner Einzelanordnung bedürfe.

Neben der unklaren Rechtslage, den widersprüchlichen Angaben der Strafverfolgungsbehörden zur Rechtsgrundlage für den Einsatz von Stillen SMS sowie der bislang fehlenden gesonderten Dokumentation des Einsatzes von Stillen SMS in den staatsanwaltschaftlichen und polizeilichen Informationssystemen war die Erfüllung unseres gesetzlichen Prüfauftrags auch deshalb erheblich beeinträchtigt, weil aus den geprüften Ermittlungsakten größtenteils kaum ersichtlich war, zu welchem Zeitpunkt und aus welchen Gründen Stille SMS versandt worden sind,

118 Es betraf 257 Verfahren, in denen insgesamt 89.018 Stille SMS versandt wurden.

wer hiervon betroffen war und zu welchen Ergebnissen die Maßnahme jeweils führte.

Trotz dieser Schwierigkeiten bei der Durchführung der Prüfung konnten wir feststellen, dass es besonders in drei Punkten strukturelle Mängel bei dem Einsatz von Stillen SMS gibt:

- Oft setzten die Strafverfolgungsbehörden Stille SMS ein, ohne dass diese Maßnahmen für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der oder des Beschuldigten erkennbar erforderlich waren. Zudem wurde eine nicht geringe Anzahl dieser Maßnahmen durchgeführt, ohne weitere weniger eingreifende Ermittlungsansätze zu prüfen, Ergebnisse bereits durchgeführter Ermittlungen abzuwarten oder zu untersuchen, ob die Maßnahmen zum Zeitpunkt ihrer Durchführung aufgrund anderer Ermittlungsergebnisse noch notwendig waren.

- Die Staatsanwaltschaft beantragte regelmäßig gerichtliche Beschlüsse für die Durchführung von TKÜ-Maßnahmen oder die Abfrage von Verkehrsdaten, die sie sodann auch für die Versendung von Stillen SMS nutzte. Sie erklärte dabei nicht, weshalb ohne die konkrete Maßnahme die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der oder des Beschuldigten wesentlich erschwert oder aussichtslos gewesen wäre bzw. warum sie für die Erforschung des Sachverhalts erforderlich war und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache stand.

  Weiterhin benannte die Staatsanwaltschaft bei der Beantragung von TKÜ-Maßnahmen oder der Abfrage von Verkehrsdaten in keinem einzigen der geprüften Fälle den geplanten Einsatz von Stillen SMS und machte es somit dem Gericht unmöglich, die Rechtmäßigkeit genau dieser Maßnahmen zu prüfen.

- In der überwiegenden Anzahl der geprüften Fälle fand keine Benachrichtigung der Betroffenen statt bzw. wurden keine Gründe für nicht oder noch nicht erfolgte Benachrichtigungen aktenkundig gemacht, obwohl dies verpflichtend vorgeschrieben ist. Weiterhin war aus dem Großteil der Akten der Einsatz von Stillen SMS nicht ersichtlich. Selbst wenn also Betroffene Kenntnis von der Durchführung von TKÜ-Maßnahmen gegen sie oder von der Abfrage sie betref-

fender Verkehrsdaten erlangt haben, werden sie durch Akteneinsicht regelmäßig nicht erfahren, dass auch Stille SMS an ihre Telefone gesendet worden sind.

Wir haben den Strafverfolgungsbehörden geraten, in den zurückliegenden Verfahren die Betroffenen, die noch keine Kenntnis von den gegen sie gerichteten Maßnahmen haben, soweit erforderlich zu informieren und über ihre Rechtsschutzmöglichkeiten aufzuklären. Ferner sollte die Einhaltung von Dokumentations-, Kennzeichnungs- und Löschpflichten nochmals überprüft werden.

Im Hinblick auf die Durchführung zukünftiger Verfahren haben wir den Strafverfolgungsbehörden im Ergebnis unserer Prüfung insbesondere folgende Empfehlungen gegeben:

- Mit einer Dienstanweisung sollte bei der Staatsanwaltschaft verpflichtend eingeführt werden, dass der Einsatz von Stillen SMS in den Ermittlungsakten dokumentiert wird. Dabei sollte ersichtlich sein, zu welchem Zeitpunkt und aus welchen Gründen Stille SMS versandt worden sind, wer hiervon betroffen war und zu welchen Ergebnissen die Maßnahme jeweils führte. Mit der Polizei sollte eine entsprechende Zuarbeit zur Dokumentation vereinbart werden.

- In den elektronischen Verfahrensverwaltungen der Ermittlungsbehörden sollte erfasst werden, in welchen Verfahren Stille SMS versandt worden sind, um generelle Prüfungen ihres Einsatzes zu erleichtern und statistische Auswertungen zu ermöglichen.

- Bei der Staatsanwaltschaft sollte eine Kontrollliste für die Ermittlungsakte eingeführt werden, mit deren Hilfe regelmäßig während des laufenden Verfahrens überprüft werden kann, ob Daten aus den Maßnahmen, die zur Akte gelangt sind, entsprechend den gesetzlichen Vorgaben gekennzeichnet wurden, ob Betroffene benachrichtigt oder Gründe einer Nichtbenachrichtigung dokumentiert wurden und ob eine unverzügliche Datenlöschung erforderlich ist.

- Die betreffenden Ermittlungspersonen sollten in einem Rundschreiben nochmals ausführlich auf die rechtlichen Pflichten bei der Durchführung von TKÜ-Maßnahmen bzw. dem Abrufen von Verkehrsdaten bei Telekommunikationsanbietern hingewiesen werden.

Zudem wäre es zu begrüßen, wenn sich das Abgeordnetenhaus für die Schaffung einer normenklaren, bereichsspezifischen Rechtsgrundlage für die Verwendung von Stillen SMS in strafrechtlichen Ermittlungsverfahren einsetzen würde. Der Senat sollte darüber hinaus verpflichtet werden, dem Abgeordnetenhaus einmal jährlich einen Bericht über den Einsatz von Stillen SMS in strafrechtlichen Ermittlungsverfahren vorzulegen. Aus dem Bericht sollten sich die Anzahl der versandten Stillen SMS, die Anzahl der hiervon Betroffenen sowie die Deliktsbereiche und die Anzahl der Verfahren, in denen Stille SMS eingesetzt wurden, ergeben.

Der Einsatz Stiller SMS in strafrechtlichen Ermittlungsverfahren ist ein tiefer Eingriff in das Grundrecht auf informationelle Selbstbestimmung,[119] weil er für die Betroffenen unbemerkt erfolgt. Dies wiegt umso schwerer, als nicht nur Beschuldigte, sondern auch Dritte, wie Personen, die Kontakt zu der oder dem Beschuldigten haben, sowie Inhaber der Telefonanschlüsse, die Beschuldigte ebenfalls nutzen, hiervon betroffen sind.[120] Aufgrund der Eingriffstiefe sind daher hohe Anforderungen an die gesetzliche Zulässigkeit dieser Maßnahmen und deren praktische Umsetzung zu stellen sowie eine unabhängige Prüfung des Einsatzes von Stillen SMS zu gewährleisten.

119 Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG)

120 In den von uns geprüften Fällen richtete sich der Einsatz Stiller SMS in etwa einem Viertel der Fälle gegen Unbeteiligte.

2 Digitale Verwaltung

2.1 Das neue Berliner E-Government-Gesetz

Mit der Verkündung des Berliner E-Government-Gesetzes am 30. Mai 2016 ging ein über fünf Jahre dauernder Werdegang des Gesetzes zu Ende. Die datenschutz- und informationsfreiheitsrechtliche Begleitung wurde bereits in vorherigen Jahresberichten dokumentiert.[121] Richtig Fahrt nahm das Gesetz aber erst in diesem Jahr auf. Beim Berliner E-Government-Gesetz handelt es sich um ein Artikelgesetz. Artikel 1 enthält das eigentliche E-Government-Gesetz Berlin (EGovG Bln), Artikel 8 enthält eine Änderung des Berliner Datenschutzgesetzes (BlnDSG) und Artikel 7 eine Änderung des Berliner Informationsfreiheitsgesetzes (IFG).[122] Die anderen Artikel enthalten Änderungen verschiedener anderer Gesetze.[123]

Die Änderung des BlnDSG bezieht sich im Wesentlichen auf eine Neufassung des § 15 BlnDSG. Hier wird einerseits die Einrichtung gemeinsamer Verfahren ermöglicht, also automatisierter Verfahren, die mehreren datenverarbeitenden Stellen die Verarbeitung personenbezogener Daten in oder aus einem gemeinsamen Datenbestand ermöglichen, andererseits wird die Einrichtung automatisierter Abrufverfahren erleichtert, ohne dass das bestehende Datenschutzniveau abgesenkt wird. Die Neufassung gleicht dabei die Berliner Rechtslage an die des Bundes sowie des Landes Brandenburg an. Ein erster wichtiger Anwendungsfall wird das Service-Konto Berlin sein, das nach derzeitigem Planungsstand als gemeinsames Verfahren ausgestaltet werden soll.

Daneben wurde eine umfassende Verpflichtung für die Berliner Verwaltung geschaffen, Informationen, die sie in Erfüllung ihres öffentlichen Auftrags im Rah-

121 JB 2010, 1.2.1; JB 2011, 1.2.1; JB 2012, 1.1; JB 2013, 1.7

122 Zur Änderung des IFG siehe 13.2

123 Allgemeines Zuständigkeitsgesetz (AZG), Gesetz über die Anstalt des öffentlichen Rechts IT-Dienstleistungszentrum Berlin (ITDZG), Landesbeamtengesetz (LBG), Berliner Personalvertretungsgesetz (PersVG) und Landesgleichstellungsgesetz (LGG)

men ihrer jeweiligen Zuständigkeit erstellt hat und die in maschinenlesbaren Formaten darstellbar sind, im zentralen Datenportal als Bestandteil des elektronischen Stadtinformationssystems für das Land Berlin zu veröffentlichen.[124] Die Einzelheiten der Bereitstellung sowie die Art, der Umfang, die Form und die Formate der Daten sind jedoch nicht im Gesetz selbst geregelt, sondern sind vom Senat in einer Rechtsverordnung festzulegen. Zum jetzigen Zeitpunkt ist daher noch nicht absehbar, welche Informationen künftig in welcher Form zu veröffentlichen sein werden. Zwar wäre es vorzuziehen gewesen, die Veröffentlichungspflichten unmittelbar im IFG zu verankern, wie wir bereits 2013 vorgeschlagen hatten.[125] Auch hätten direkt im Gesetz angelegte Datenkategorien den Vorteil, dass diese nicht einfach durch die Änderung einer Rechtsverordnung abgeschafft werden können. Demgegenüber bietet die Verordnungsermächtigung aber den Vorteil, dass spiegelbildlich neue Datenkategorien mit erheblich weniger Aufwand aufgenommen werden können. Es bleibt daher erst einmal abzuwarten, inwieweit der Senat die Veröffentlichungspflichten nach dem E-Government-Gesetz Berlin im Rahmen der noch zu erlassenden Rechtsverordnung mit Leben füllen wird.

Im eigentlichen E-Government-Gesetz Berlin kommen datenschutzrechtliche und sicherheitstechnische Aspekte an verschiedenen Stellen zum Tragen.

Jede Berliner Behörde ist in Zukunft verpflichtet, einen Zugang für die Übermittlung elektronischer Dokumente, auch wenn sie mit einer qualifizierten elektronischen Signatur versehen sind, und eine De-Mail-Adresse sowie einen E-Mail-Zugang mit einer gängigen Ende-zu-Ende-Verschlüsselung (z. B. PGP) zu eröffnen.[126] Dies bedeutet, dass jede Bürgerin und jeder Bürger nun die Möglichkeit haben muss, mit Berliner Behörden verschlüsselt elektronisch zu kommunizieren.

In Abschnitt 3 wird eine zentrale Steuerung der Informations- und Kommunikationstechnik (IKT) installiert. Durch Festlegung von verbindlichen Grundsätzen, Standards und Regelungen soll u. a. die Sicherheit der Informations- und Kommunikationstechnik verbessert werden.[127] Wesentlich hierbei ist, dass verbind-

124 § 13 Abs. 1 EGovG Bln

125 JB 2013, 1.7

126 Siehe § 4 Abs. 1 und 2 EGovG Bln; diese Bestimmungen treten im Juni 2017 in Kraft.

127 § 20 Abs. 2 Nr. 1 EGovG Bln

liche Regelungen zur Sicherheit nicht nur festgelegt, sondern deren Einhaltung auch zentral überwacht werden soll.[128] Dies soll durch eine IKT-Staatssekretärin oder einen IKT-Staatssekretär mit dazugehöriger Organisationseinheit gewährleistet werden.

Durch Berücksichtigung der Belange der Informationssicherheit in den Planungsvorgängen der zentralen IKT-Steuerung besteht nun die Hoffnung, dass Probleme wie z. B. der jahrelange dezentrale Einsatz von Arbeitsplatzcomputern mit dem veralteten und nicht mehr gepflegten Betriebssystem Windows XP der Vergangenheit angehören.

2.2 Neues zum Ordnungsamt-Online

2015 haben wir über das Projekt „Einführung eines Anliegenmanagementsystems (AMS) für die Berliner Ordnungsämter" berichtet.[129] Seit einiger Zeit befindet sich das Verfahren nun unter dem Namen „Ordnungsamt-Online" in mehreren Bezirken im Einsatz. Mit diesem Verfahren erhalten Bürgerinnen und Bürger die Möglichkeit, Meldungen zu Störungen im öffentlichen Raum über verschiedene Meldewege dem zuständigen Ordnungsamt zu übermitteln. Bei der Durchsicht der im Internet durch das zuständige Ordnungsamt veröffentlichten Meldungen mussten wir jedoch feststellen, dass bei mehreren Meldungen personenbezogene bzw. personenbeziehbare Daten im Portal Ordnungsamt-Online abrufbar sind. Dies betrifft in erster Linie Bilder, auf denen die gemeldete Störung veranschaulicht werden soll, die aber z. B. deutlich lesbare Kfz-Kennzeichen enthalten. Bei anderen Meldungen wurden Kfz-Kennzeichen direkt im Meldungstext aufgeführt.

Die Meldungen, die durch Bürgerinnen und Bürger an das Portal Ordnungsamt-Online über verschiedene Wege herangetragen werden, werden durch Mitarbeiterinnen und Mitarbeiter des jeweiligen Ordnungsamtes überprüft und in das Portal übernommen. Wir mussten feststellen, dass hierbei offensichtlich nicht immer mit der gebotenen Sorgfalt gearbeitet wurde und personenbezogene bzw.

128 § 20 Abs. 2 Nr. 1 EGovG Bln
129 JB 2015, 1.1

personenbeziehbare Daten, die von den Meldenden eingegeben wurden, einfach in das Portal übernommen wurden. Mit einer Übernahme in das Portal werden personenbezogene Daten einem unbestimmten Personenkreis bekannt gegeben. Dabei handelt es sich um eine Datenübermittlung im Sinne des Berliner Datenschutzgesetzes.[130] Dies wäre nur dann zulässig, wenn es eine besondere Rechtsvorschrift erlauben würde oder die jeweils betroffene Person eingewilligt hätte. Eine entsprechende Rechtsvorschrift ist jedoch nicht vorhanden und entsprechende Einwilligungen dürften ebenfalls nicht vorliegen, sodass die Veröffentlichungen der Daten unzulässig sind. Kfz-Kennzeichen sind daher zu schwärzen oder unlesbar zu machen.

Wir haben die betroffenen Ordnungsämter gebeten, darauf hinzuwirken, dass bei der Übernahme der Meldungen durch die Mitarbeiterinnen und Mitarbeiter der Ordnungsämter sorgfältiger vorzugehen ist und Maßnahmen definiert werden, die eine unzulässige Veröffentlichung personenbezogener Daten im Portal Ordnungsamt-Online zukünftig verhindern.

2.3 Speicherautomaten für biometrische Daten in den Bürgerämtern

Wenn es um die Speicherung biometrischer Merkmale geht, wird bei vielen Menschen ein unangenehmes Gefühl erzeugt. Der Grund ist, dass diese Merkmale mit der eigenen Person untrennbar verbunden und vor allem in der Regel nicht abänderbar sind. Zu diesen Merkmalen zählen u. a. die Vermessung des Gesichts, Erkennung der Retina- und Irisstruktur des Auges und die Fingerabdrücke. Aber auch viel vertrautere Dinge, wie die Unterschrift oder das eigene Lichtbild, gehören zu diesen Merkmalen.

Die meisten Personen versuchen die Speicherung biometrischer Merkmale zu vermeiden, da es vielfach Zweifel an der Zuverlässigkeit biometrischer Verfahren gibt. In einigen Situationen ist die Preisgabe dieser Daten jedoch unausweichlich und sogar vorgeschrieben. So ist in Deutschland der Besitz eines gültigen Per-

130 § 4 Abs. 2 Satz 2 Nr. 4 BlnDSG

sonalausweises Pflicht. Um in seinen Besitz zu gelangen, müssen diverse persönliche Daten, zu denen auch biometrische Daten gehören, an die ausstellende Behörde übermittelt werden. In Berlin ist dies Aufgabe der Bürgerämter.

Zur Service-Verbesserung für den Bürger, aber auch zur Optimierung der eigenen Arbeitsprozesse hat der Bezirk Marzahn-Hellersdorf spezielle Automaten für die Erfassung biometrischer Merkmale bei Beantragung von Personalausweisen oder Reisepässen aufstellen lassen. Diese Automaten übermitteln die erfassten Daten auf die Arbeitsplätze der Mitarbeiterinnen und Mitarbeiter im Bürgeramt.

Die Sensitivität der dort verarbeiteten Daten war Anlass für eine Kontrollmaßnahme nach dem Berliner Datenschutzgesetz[131] – mit durchaus erfreulichem Ergebnis. Bei dem automatisierten Verfahren werden im Einzelnen Fotos des Kopfbereichs, Fingerabdrücke und die persönliche Unterschrift erfasst. Die Erfassung der Fingerabdrücke erfolgt dabei jedoch nur nach Einwilligung. Die Unterschrift wird nur in erforderlichen Fällen, wie beispielsweise bei der Beantragung eines Personalausweises, verwendet. Neben den biometrischen Daten wird auch das Geburtsdatum für eine zweifelsfreie Zuordnung erfasst. Während der Nutzung besteht immer wieder die Möglichkeit, den Vorgang abzubrechen. Alle bisher erfassten Daten der Person werden dann unwiederbringlich gelöscht. Erst wenn letztmalig der Datenübermittlung zugestimmt wurde, erzeugt das Gerät eine verschlüsselte Datei, die an einen Datenbankserver des Bürgeramtes übermittelt und dann aus dem Speicher des Automaten gelöscht wird. Alle Vorgänge im Erfassungsautomaten erfolgen ausschließlich im Arbeitsspeicher. Eine Speicherung von Daten auf dauerhaften Speichermedien im Erfassungsautomaten erfolgt zu keinem Zeitpunkt.

Die Sachbearbeitung im Bürgeramt ist jetzt in der Lage, die Daten vom Datenbankserver auf dem Arbeitsplatz abzurufen und für den folgenden Vorgang, z. B. die Beantragung eines Personalausweises, weiterzuverarbeiten. Nach Abschluss des Vorgangs werden die Daten aus dem Datenbankserver gelöscht. Nicht abgerufene Datensätze werden nach einem definierten Zeitraum gelöscht. Auf eine Datensicherung wird sowohl im Automaten als auch beim Datenbanksystem zu-

131 § 24 Abs. 1 BlnDSG

gunsten der Erhöhung der Vertraulichkeit der verarbeiteten biometrischen Daten komplett verzichtet.

Eine Besonderheit ist, dass die Automaten durch ein privates Unternehmen und nicht durch das Bürgeramt betrieben werden. Die Firma ist für Wartung und Reparaturen der Geräte verantwortlich. Diese erfolgen nur vor Ort nach Absprache und unter Aufsicht des Bürgeramtes bzw. der IT-Stelle. Eine Fernwartung findet nicht statt. Die Einziehung des Nutzungsentgelts erfolgt durch das Bürgeramt, welches direkt mit dem Betreiber abrechnet. Eine Übermittlung von Nutzerdaten an den Betreiber findet nicht statt.

Unsere Kontrolle hat gezeigt, dass es möglich ist, auch sensitive biometrische Daten datenschutzgerecht zu verarbeiten. Auch andere Berliner Bezirke beabsichtigen den Einsatz entsprechender Terminals. Dabei sollen auch andere Anbieter berücksichtigt werden. Wir werden die dort eingesetzten Lösungen weiter datenschutzrechtlich begleiten.

2.4 Schweigen im Kabelwald

Im Zusammenhang mit eingehenden Beschwerden und der Beurteilung von IT-Verfahren haben wir uns vielfach an das IT-Dienstleistungszentrum Berlin gewendet. Mehrmals erreichten uns aussagekräftige Antworten nicht in angemessener Zeit.

Das IT-Dienstleistungszentrum Berlin (ITDZ) ist der zentrale IT-Dienstleister für die Behörden Berlins und spielt eine wichtige Rolle bei der Etablierung des E-Governments in unserer Stadt. Das ITDZ betreibt das Berliner Landesnetz, die dazugehörige Infrastruktur und auf seinen Servern eine große Zahl von Verfahren der Behörden.

Zum Schutz der eigenen Technik und der Behörden, die über das Landesnetz an das Internet angeschlossen sind, plante das ITDZ, ein System zur Kontrolle der ein- und ausgehenden Datenströme zu installieren. Da sich unter den geprüften Daten auch personenbezogene Daten befinden, darunter solche, die dem Fern-

meldegeheimnis unterliegen, baten wir das ITDZ, uns aussagekräftige Unterlagen über das geplante Vorgehen zuzusenden. Trotz mehrfacher Nachfrage über mehrere Monate hinweg erhielten wir nur bruchstückhafte Informationen, jedoch keine aussagekräftigen Unterlagen.

Um Beschäftigten von Berliner Behörden mit ihren mobilen Geräten, darunter auch Smartphones, Zugriff auf dienstliche Daten zu ermöglichen, betreibt das ITDZ ein Sicherheitssystem. Es soll den Verbindungsweg schützen und nur den berechtigten Beschäftigten Zugang erlauben. Bereits im Vorjahr hatten wir das ITDZ auf Schwächen des Systems hingewiesen, das nicht dem Stand der Technik entsprach. Weder Sicherheitskonzept noch Risikoanalyse überzeugten. Dies wurde durch das ITDZ auch eingeräumt. Wir forderten daraufhin das ITDZ auf, seine Kunden über die Risiken zu informieren, und mahnten eine Überarbeitung an. Auch nach Ablauf eines Jahres ist weiterhin ungeklärt, ob die Kunden informiert wurden. Und nach wie vor liegt uns nicht einmal eine Stellungnahme des ITDZ zu den bestehenden Risiken vor.

Das ITDZ erarbeitet Sicherheitskonzepte nicht nur für eigene Verfahren, sondern auch für seine Kunden. Diese Sicherheitskonzepte müssen den besonderen Anforderungen des Datenschutzes genügen. Dazu gehört es u. a., nur so wenige Daten wie möglich zu verarbeiten und die Nachvollziehbarkeit der Verarbeitung zu ermöglichen. Wir haben das ITDZ gebeten, uns die internen Regelungen zur Berücksichtigung dieser seit 2001 bestehenden Anforderungen zu übersenden. Als Antwort haben wir eine Richtlinie zur Erstellung von Sicherheitskonzeptionen erhalten. Die besonderen Anforderungen des Datenschutzes sind dort mit keinem Wort erwähnt.

Ausgehend von einem ersten Gespräch auf Leitungsebene werden wir verstärkt darauf hinwirken, dass das ITDZ seinen Verpflichtungen zur Erteilung von Auskünften und Übergabe von aussagekräftigen Planungsunterlagen sowie zur Berücksichtigung des Datenschutzes bei den von ihm gestalteten Verfahren nachkommt.

Alle öffentlichen Stellen des Landes trifft die Verpflichtung, der Berliner Beauftragten für Datenschutz und Informationsfreiheit zeitgerecht die angeforderten Auskünfte zu erteilen.

3 Inneres

3.1 Berliner Ausführungsgesetz zum Bundesmeldegesetz

Am 1. November 2015 hat das Bundesmeldegesetz (BMG) die Landesmeldegesetze abgelöst.[132] Seit diesem Zeitpunkt dürfen die Länder eigene melderechtliche Vorschriften nur in den Fällen erlassen, in denen das BMG sie hierzu ermächtigt. Dies betrifft z. B. regelmäßige Datenübermittlungen. In diesem Jahr wurde nun das Berliner Ausführungsgesetz zum Bundesmeldegesetz (BlnAGBMG) erlassen.[133] Wir hatten die Gelegenheit, zu dem Entwurf dieses Gesetzes Stellung zu nehmen.

3.1.1 Regelmäßige Datenübermittlungen an öffentliche Stellen

Das BMG selbst enthält bereits Regelungen, die festlegen, welche Daten regelmäßig an öffentlich-rechtliche Religionsgemeinschaften übermittelt werden dürfen. Diese Regelungen und insbesondere den Umfang der übermittelten Daten hatten wir im Gesetzgebungsverfahren bereits kritisiert.[134] Mit dem neuen Berliner Ausführungsgesetz wurde der Katalog an Daten, die an öffentlich-rechtliche Religionsgemeinschaften übermittelt werden, dann sogar noch erweitert. Zusätzlich zu den bundesgesetzlich festgelegten Daten sollen in Berlin auch „frühere Namen“ und „derzeitige Staatsangehörigkeiten“ von Familienangehörigen an öffentlich-rechtliche Religionsgemeinschaften übermittelt werden. Diese Informationen sind weder für die Besteuerung noch für die Aufgabenerfüllung der Kirchen erforderlich. Daher haben wir in unserer Stel-

132 Siehe bereits JB 2014, 3.2
133 GVBl. 2016, S. 430
134 JB 2014, 3.2

lungnahme empfohlen, diese zusätzlichen Datenkategorien zu streichen. Dieser Empfehlung ist der Gesetzgeber nicht gefolgt.

3.1.2 Regelmäßige Datenübermittlungen an den Rundfunk Berlin-Brandenburg

Im Rahmen des Gesetzgebungsverfahrens zum BlnAGBMG haben wir außerdem darauf hingewiesen, dass eine Regelungslücke bezüglich der regelmäßigen Datenübermittlungen von den Meldeämtern an den Rundfunk Berlin-Brandenburg besteht. Mit Inkrafttreten des BlnAGBMG fehlt eine geeignete gesetzliche Grundlage für diese Art der Datenübermittlungen. Wir haben daher empfohlen, eine derartige Vorschrift in das BlnAGBMG aufzunehmen, so wie es andere Bundesländer in ihren Landesmeldegesetzen getan haben. Auch diese Empfehlung wurde nicht umgesetzt.

3.2 Ausweitung polizeilicher Videoüberwachung im öffentlichen Raum?

Kurz vor Ende der 17. Legislaturperiode wurde im Abgeordnetenhaus der Entwurf eines Gesetzes diskutiert, das der Polizei ermöglichen sollte, an ausgewählten, sog. gefährlichen Orten[135] präventiv Videoüberwachungsmaßnahmen durchzuführen. Wir haben zu diesem Entwurf Stellung genommen und unsere Bedenken gegen die geplanten Regelungen deutlich gemacht.

Es war zu befürchten, dass die Vorschriften zu einer Videoüberwachung großer Bereiche insbesondere der Innenstadt ohne konkrete einzelfallbezogene Anlässe geführt hätten. Für diese Befürchtung sprach auch die Begründung des geplanten Gesetzes, wonach eine polizeiliche Videoüberwachung von Straßen und Plätzen mit besonders hohem Passantenaufkommen sowie Verkehrsknotenpunkten ermöglicht werden sollte. Derartige Örtlichkeiten sind in einer Großstadt wie Berlin eher die Regel als die Ausnahme. Hinzu kam, dass die Polizei erstmals außerhalb

135 § 21 Abs. 2 Nr. 1a ASOG

restriktiver Spezialvorschriften[136] befugt werden sollte, nicht nur den öffentlichen Verkehrsraum präventiv mit Kameras zu erfassen, sondern alle öffentlich zugänglichen Räume, zu denen nach der Gesetzesbegründung auch Einkaufszentren, Kaufhäuser, Restaurants, Schwimmbäder und Museen gehören sollten.

Eine Videoüberwachung in dem beschriebenen Ausmaß, die die geplanten Regelungen ermöglicht hätte, wäre unverhältnismäßig.

Bereits ihre Geeignetheit ist fraglich. Das Beispiel London zeigt, dass die Kriminalität trotz beinahe flächendeckender Videoüberwachung kaum zurückgegangen ist, sondern sich nur verlagert hat. Gerade deshalb bietet sich in Berlin vor einer Ausweitung der Videoüberwachung an, dass eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung der Erfolge der bereits jetzt stattfindenden Videoüberwachungsmaßnahmen auf der Grundlage eines umfassenden Bewertungsansatzes durchgeführt wird.

Weiterhin stellt sich die Frage nach der Erforderlichkeit und Angemessenheit solcher Videoüberwachungsmaßnahmen: Mildere Mittel als eine dauerhafte Videoüberwachung wären z. B. die Steigerung der Polizeipräsenz oder die bessere Ausleuchtung oder Gestaltung kritischer Bereiche.

Zudem ist zu berücksichtigen, dass eine nicht anlassbezogene großflächige Videoüberwachung u. a. aufgrund ihrer Streubreite ein tiefer Eingriff in das informationelle Selbstbestimmungsrecht der davon Betroffenen ist. 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.

Ferner ist auch zu bedenken, dass eine solche Überwachung dazu führen kann, das Wegsehen beim Auftreten von Gewalttaten zu fördern, weil man dem Trugschluss erliegen kann, dass auch ohne eigenes Handeln rechtzeitig Hilfe kommen müsste, da die Polizei das Geschehen wahrscheinlich über die Videokameras live

136 § 25 ASOG

an Monitoren verfolgt. Je mehr Videokameras installiert werden und je mehr Monitore dadurch zu kontrollieren wären, desto unwahrscheinlicher ist dies jedoch.

Unsere Stellungnahme hat dazu beigetragen, dass der Gesetzesentwurf letztlich nicht zur parlamentarischen Abstimmung gelangte.

Eine nicht anlassbezogene weiträumige Videoüberwachung durch die Polizei greift in die Persönlichkeitsrechte zahlloser unbeteiligter Personen ein. Ihre Eignung zur Gefahrenabwehr ist zudem bislang wissenschaftlich nicht belegt.

3.3 Polizeiliche Falldatei Rauschgift

Wir haben parallel zur Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und mehreren Landesdatenschutzbeauftragten die Führung der polizeilichen Falldatei Rauschgift (FDR) stichprobenhaft überprüft.[137]

Die FDR ist eine sog. Verbunddatei, die beim Bundeskriminalamt für alle Polizeibehörden des Bundes und der Länder geführt wird. Sie dient der Polizei als Informationsquelle bei der Verhütung und Verfolgung von Straftaten im Bereich der Rauschgiftkriminalität und wird von ihr mit entsprechenden Daten gespeist.

Wir stellten erhebliche Mängel bei der Verarbeitung von Daten in der FDR durch die Polizei fest. Diese speicherte entgegen den gesetzlichen Bestimmungen sämtliche Verstöße gegen das Betäubungsmittelgesetz in der FDR. Eine Prüfung, ob die Daten zur Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung erforderlich sind,[138] fand ebenso wenig statt wie eine Dokumentation der entsprechenden Einzelfallentscheidung. Weiterhin führte die Polizei vor der Speicherung von Daten keine Negativprognose durch, d. h. sie prüfte nicht, ob die Speicherung bestimmter personenbezogener

137 Siehe Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 9./10. November 2016: Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf – Konsequenzen für polizeiliche Datenverarbeitung notwendig, Dokumentenband 2016, S. 37

138 Erheblichkeitsprüfung gem. § 2 Abs. 1 Bundeskriminalamtgesetz (BKAG)

Daten in der FDR erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind.[139]

Aufgrund unserer Prüfung wurden von der Polizei Erfassungsrichtlinien zur Datenverarbeitung in der FDR erstellt, mithilfe derer der bisherige Datenbestand auf die Rechtmäßigkeit der Speicherung geprüft sowie ggfs. in Teilen gelöscht wird. Die Richtlinien bilden auch die Grundlage für die Neuerfassungen von Daten in der FDR. Der Bestand der von der Berliner Polizei in der FDR gespeicherten Daten hat sich durch die bislang erfolgte Durchsicht im Vergleich zum Bestand zu Beginn unserer Prüfung bereits um ein Viertel auf etwa 180.000 Datensätze reduziert. Auch die Daten der von uns geprüften Stichproben wurden größtenteils gelöscht, weil die Voraussetzungen für ihre Speicherung nicht bzw. nicht mehr vorlagen.

Die neuen Richtlinien entsprechen jedoch noch nicht vollständig den gesetzlichen Bestimmungen, weshalb wir die Polizei um Nachbesserung gebeten haben. Insbesondere sollte in den Richtlinien klargestellt werden, dass die dortigen abstrakten Vorgaben nicht die Entscheidung über eine Speicherung von Daten anhand des konkreten Einzelfalls ersetzen können. Zudem muss verdeutlicht werden, dass eine Negativprognose in allen Fällen vorgenommen werden muss, soweit – wie bisher – eine Sachverhaltsbeschreibung im Freitextfeld von Datensätzen erfolgt und/oder Angaben zu den sichergestellten Betäubungsmitteln gespeichert werden.

Voraussichtlich im kommenden Jahr wird die FDR durch die Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV) abgelöst. Hier muss sichergestellt sein, dass keine fehlerhaften Datensätze aus der FDR in den PIAV überführt werden.

Wir werden die polizeiliche Überprüfung des Datenbestandes in der FDR, die Datenmigration von der FDR zum PIAV sowie die Überarbeitung der Erfassungsrichtlinien begleiten.

139 Negativprognose gem. § 8 Abs. 2 BKAG

Die Erfassung von Daten in bundesweiten polizeilichen Verbunddateien wie der FDR, auf die alle Polizeibehörden des Bundes und der Länder Zugriff haben, darf nur nach sorgfältiger Einzelfallprüfung auf Grundlage der gesetzlichen Vorgaben erfolgen. Die pauschale Speicherung von Datensätzen kann weitreichende Folgen für die Betroffenen haben.

3.4 Polizeiliche Datei „Szenekunde Sport“

Die Polizei führt die Datei „Szenekunde Sport“[140] zur Unterstützung der Strafverfolgung und Gefahrenabwehr im Zusammenhang mit Sportveranstaltungen. Wir haben die Datei im Rahmen einer Vor-Ort-Kontrolle stichprobenhaft überprüft.

In der Datei werden Tatverdächtige, Beschuldigte und Gefahrenverursacher[141] gespeichert. Sie dient nach Angaben der Polizei in erster Linie als Hintergrundquelle für ihre Arbeit. Zum Zeitpunkt unseres Prüfbesuchs enthielt die Datei ca. 1.500 Datensätze.

Derzeit wird die Datensammlung in ein neues Verfahren überführt, womit u. a. die darin durchgeführten Recherchen vereinfacht werden sollen. Entsprechend der Errichtungsanordnung für das neue Verfahren sollten auch DNA-Daten, IP-Adressen, Netzbetreiber und Objektnamen in der Datei gespeichert werden. Die Polizei konnte hierfür jedoch keine Erforderlichkeit begründen, weshalb wir eine Streichung dieser Datenkategorien empfohlen haben. Dieser Empfehlung wurde gefolgt.

Die Errichtungsanordnung sieht ebenfalls vor, dass sonstige Hinweise in einem Freitextfeld in der Datei gespeichert werden dürfen. Die Polizei erläuterte, dass die Kategorie erforderlich sei, um wichtige Informationen zu speichern, die sich nicht in sonstiger Weise kategorisieren lassen, z. B. ob die oder der Betroffene momentan eine Haftstrafe verbüßt. Wir forderten die Eingrenzung der Kategorie durch die Erstellung einer Interpretationshilfe. Dieser Forderung wurde bislang

140 Früher Datei „Sportgewalt“
141 Siehe § 13 ASOG

unter Verweis auf den kleinen szenekundigen Nutzerkreis der Datei nicht nachgekommen.

Bei der stichprobenartigen Prüfung der Datei konnte uns die Polizei in einigen Fällen nicht erklären, weshalb einzelne Daten oder ganze Datensätze noch für ihre Arbeit erforderlich sind. Zum Teil lagen Vorfälle, die hinsichtlich der Betroffenen für die Polizei bedeutsam sind, bereits Jahre zurück und/oder waren einmalig. Zwischenzeitlich wurden diese Daten größtenteils gelöscht. Wir vereinbarten mit der Polizei zudem, dass die gesamte Datei auf Daten überprüft werden soll, deren Speicherung unzulässig ist, insbesondere weil die Betroffenen nur kurz bzw. zuletzt vor langer Zeit in Erscheinung getreten sind.

Die Verarbeitung von Daten durch die Polizei muss sich unter Berücksichtigung der Betroffenenrechte in jedem Einzelfall am Erforderlichkeitsgrundsatz orientieren. Die Führung der polizeilichen Datei „Szenekunde Sport" bedarf insoweit einer Veränderung. Wir werden die Umsetzung der entsprechenden Vorgaben prüfen.

3.5 Urteilsdatenbank zu Flucht und Asyl künftig besser anonymisiert

Ein eingetragener Verein, der im Bereich der Geflüchteten- und Migrationsarbeit aktiv ist, macht auf seiner Internetseite öffentlich verfügbare Gerichtsentscheidungen mit migrationspolitischem Bezug zugänglich. Dabei wurde eine Entscheidung über einen Asylantrag veröffentlicht, die aufgrund fehlender Schwärzungen die Identifikation der betroffenen Person und ihrer Familie ermöglichte. Dies erfolgte ohne die Einwilligung der Betroffenen, die das zur Anzeige gebracht haben.

Eine betroffene Person hatte das Urteil über die Eingabe ihres Namens in die Internetsuchmaschine „Google" gefunden. Personenbezogene Daten im Rubrum des Urteils waren zwar geschwärzt, auf den folgenden Seiten waren jedoch Namen und ehemaliger Wohnort der Betroffenen im Fließtext offen genannt. Außerdem war der Status eines Betroffenen als Deserteur erkennbar. Die Veröffentlichung des Urteils inklusive der personenbezogenen Daten von Betroffenen im

Internet stellt eine Übermittlung der Daten an einen unbestimmten Empfängerkreis dar. Wegen der fehlenden Einwilligung der Betroffenen war dieses Vorgehen unzulässig.

Nachdem die Betroffenen den Verein bereits mit anwaltlichem Schreiben zur Entfernung des Urteils von der Internetseite angehalten hatten, forderten wir den Verein zu einer Stellungnahme hinsichtlich des generellen Umgangs mit der Anonymisierung von veröffentlichten Gerichtsurteilen auf. Der Verein bestätigte uns den vorgetragenen Fall und drückte sein Bedauern über die unzureichende Anonymisierung aus. Das infrage stehende Urteil sei als Bilddatei veröffentlicht worden, erst durch eine kürzlich erfolgte Umstellung der Internetsuchmaschine würde auch bei solchen Dateien eine Texterkennung durchgeführt. Erst dadurch sei es möglich geworden, das Urteil über die Suchmaschine abzurufen. Darüber hinaus erklärte der Verein, dass die Aufbereitung der Gerichtsentscheidungen durch juristisch qualifizierte Personen erfolge. Bei der Anonymisierung von Urteilen würden alle Textpassagen, die Rückschlüsse auf die Identität von Betroffenen zulassen, geschwärzt. Warum die Anonymisierung im vorliegenden Fall unzureichend war, konnte nicht mehr nachvollzogen werden. Als Konsequenz auf den Hinweis der Betroffenen wurde der Zugriff von Suchmaschinen auf alle vor dem Jahr 2004 aufgenommenen Entscheidungen in der Datenbank des Vereins verhindert, um diese auf ihre vollständige Anonymisierung zu überprüfen. Zudem wurde die Löschung der das Urteil enthaltenden Internetseite aus dem Index der Internetsuchmaschine veranlasst.

Wir haben gegenüber dem Verein einen Verstoß gegen Vorschriften über den Datenschutz festgestellt. Weitere aufsichtsbehördliche Mittel wurden wegen der von dem verantwortlichen Verein bereits durchgeführten Maßnahmen zur besseren Anonymisierung von Urteilen nicht ergriffen.

Bei der Veröffentlichung von Gerichtsurteilen sind personenbezogene Daten vollständig zu schwärzen. Auch eingescannte Dokumente unterliegen im Internet einer Texterkennung durch Suchmaschinen und sind sorgfältig vor einer Veröffentlichung zu anonymisieren.

3.6 Übermittlung von Gefährdungsbewertungen und Verlaufsberichten von der Polizei an den Verfassungsschutz

Die Polizei übermittelt unter bestimmten Voraussetzungen Gefährdungsbewertungen und Verlaufsberichte zu Versammlungen und sonstigen Veranstaltungen an den Verfassungsschutz. Im Rahmen einer Prüfung der Auskunftspraxis der Polizei gegenüber Betroffenen bei solchen Unterlagen haben wir festgestellt, dass in drei Fällen unrechtmäßige Datenübermittlungen stattfanden.

Die Übersendung von Gefährdungsbewertungen oder Verlaufsberichten mit den darin enthaltenen personenbezogenen Daten durch die Polizei an den Verfassungsschutz ist nur unter engen gesetzlichen Vorgaben zulässig.[142] Danach muss die Staatsanwaltschaft und – vorbehaltlich der staatsanwaltlichen Sachleitungsbefugnis – die Polizei im Rahmen ihrer Aufgabenerfüllung bekannt gewordene Informationen über verfassungsfeindliche Bestrebungen[143] der Verfassungsschutzbehörde übermitteln. Diese Voraussetzungen waren in den o. g. Fällen nicht erfüllt.

Infolge der festgestellten unrechtmäßigen Datenübermittlungen hat die Polizei das gesamte Übermittlungsverfahren auf den Prüfstand gestellt. Nunmehr ist verbindlich festgelegt, dass die Übermittlung personenbezogener Daten zu Versammlungen oder sonstigen Veranstaltungen an den Verfassungsschutz grundsätzlich durch eine Dienstkraft des höheren Dienstes autorisiert werden muss. Hierüber wurden alle betroffenen Beschäftigten eingehend in Arbeitsbesprechungen informiert. Daneben erfolgte eine Sensibilisierung der Beschäftigten der weiteren Dienstbereiche des Polizeilichen Staatsschutzes. Zugleich wurde bestimmt, dass sämtliche Übermittlungen von Gefährdungsbewertungen in geeigneter Form nachvollziehbar dokumentiert werden müssen. Darüber hinaus wurden vorhandene Arbeitshinweise präzisiert, um insbesondere neuen Dienstkräften Handlungssicherheit zu verschaffen.

142 § 27 Abs. 1 Satz 2 Verfassungsschutzgesetz Berlin (VSG Bln)
143 § 5 Abs. 2 VSG

Zur Wahrung der Auskunftsrechte von Versammlungsanmeldern hinsichtlich angefertigter Gefährdungsbewertungen zu einer angemeldeten Versammlung wurde zudem festgelegt, dass in der Veranstaltungsdatenbank die Dienststelle eingetragen werden muss, die im Einzelfall federführend eine Gefährdungsbewertung für die Versammlung erstellt hat. So soll bei Auskunftsanträgen das Auffinden entsprechender Bewertungen gewährleistet werden.

Die Prüfung der Zulässigkeit der Übermittlung von polizeilichen Gefährdungsbewertungen und Verlaufsberichten für nachrichtendienstliche Zwecke muss entsprechend den gesetzlichen Bestimmungen anhand des jeweiligen Einzelfalls erfolgen. Ebenso müssen die Betroffenenrechte gewahrt sein. Durch die nunmehr ergriffenen organisatorischen Maßnahmen der Polizei wird die praktische Umsetzung der rechtlichen Anforderungen unterstützt.

3.7 Zusammenarbeit eines Vereins mit öffentlichen Stellen im Bereich Deradikalisierung

Wir haben die Verarbeitung personenbezogener Daten eines eingetragenen Vereins im Kontext von Deradikalisierungsprogrammen überprüft. Der Verein betreibt mehrere Beratungsstellen, die Präventionsarbeit im Bereich des religiös begründeten Extremismus (z. B. Salafismus) und dessen Gefahren leisten. Diese Stellen bieten z. B. ein Ausstiegsangebot für radikalisierte Personen an. Der Verein berät aber auch Angehörige und andere Personen, die den Verdacht haben, dass sich ihre Verwandten oder Bekannten einer extremistischen Gruppe angeschlossen haben, und nimmt dann Kontakt mit den Betroffenen auf.

Der Verein ist mit einer Beratungsstelle Teil des Berliner Deradikalisierungsnetzwerks (DeRadNet). Im Zusammenhang mit dieser Tätigkeit erhält der Verein öffentliche Fördermittel. Im DeRadNet arbeiten der Berliner Verfassungsschutz und das Landeskriminalamt mit dem von uns geprüften Verein zusammen. Die Stellen bearbeiten gemeinsam Fälle von Personen, deren Verhalten auf eine Radikalisierung schließen lässt. Darüber hinaus arbeitet der Verein mit dem Bundesamt für Migration und Flüchtlinge zusammen.

Bei unserer Prüfung sind wir zu dem Ergebnis gekommen, dass für die Verarbeitung sensitiver Daten durch den Verein in der überwiegenden Zahl der Fälle keine Rechtsgrundlage besteht. Zu den sensitiven Daten zählen Angaben über die politische Meinung und die religiöse Einstellung von Personen.[144] Diese Informationen sind für die Arbeit des Vereins relevant und fallen notwendigerweise an, da dieser im Rahmen des DeRadNet nur im Bereich des religiös begründeten Extremismus tätig wird.

Bei der Deradikalisierungsarbeit handelt sich zwar um eine Aufgabenwahrnehmung, die im öffentlichen Interesse liegt. Der Verein agiert aber dennoch als private Stelle und kann sich nicht auf öffentliche Befugnisnormen stützen. Die Verarbeitung sensitiver Daten durch den Verein kann auch nicht dadurch gerechtfertigt werden, dass ihm öffentliche Gelder zur Verfügung gestellt wurden. Zulässig ist die Verarbeitung sensitiver Daten durch ihn daher nur in zwei Konstellationen: Entweder es liegt eine Einwilligung der Betroffenen vor, oder die Betroffenen haben ihre Ansichten bereits ausdrücklich selbst öffentlich gemacht.

Was den Informationsaustausch mit den öffentlichen Stellen angeht, so sind wir zu dem Ergebnis gekommen, dass sowohl das Landeskriminalamt als auch der Berliner Verfassungsschutz unter bestimmten Umständen personenbezogene Daten an den Verein übermitteln dürfen. Die weitere Verwendung unterliegt aber den o. g. Einschränkungen. Der Verein wiederum darf sensitive Daten an die öffentlichen Stellen nur übermitteln, wenn eine erhebliche Gefahr besteht oder die Daten im Einzelfall für die Verfolgung von bestimmten schwerwiegenden Straftaten erforderlich sind.

Die Verarbeitung sensitiver Daten durch private Stellen im Bereich der Deradikalisierung von Personen mit religiös-extremistischem Hintergrund kann nicht allein durch die Bereitstellung öffentlicher Gelder oder eine Tätigkeit im öffentlichen Interesse gerechtfertigt werden. Beim Austausch von personenbezogenen Daten im Rahmen des DeRadNet muss stets im Einzelfall geprüft werden, ob bereits die nach den jeweiligen Übermittlungsvorschriften erforderlichen konkreten Gefahren vorliegen.

144 § 3 Abs. 9 BDSG

3.8 Videoüberwachung bei der Deutschen Bahn AG

Mitte der 90er Jahre hat die Deutsche Bahn AG (DB) damit begonnen, ihr sog. 3-S-Konzept einzuführen, um Service, Sicherheit und Sauberkeit im Bahnhofsbereich zu verbessern. Über dieses Konzept haben wir in der Vergangenheit bereits ausführlich berichtet.[145] Zu diesem Zweck wurden zunächst die großen Personenbahnhöfe im Bundesgebiet mit Videoanlagen ausgerüstet. Der Einsatz der Überwachungskameras dient der Koordinierung und Steuerung der Betriebsprozesse sowie der Sicherheit der Reisenden. Die Nutzung der optisch-elektronischen Einrichtungen (Videoüberwachung) in den Verkehrsstationen der DB wurde in einem Vertrag zwischen der DB und der Bundespolizei geregelt: Die Beschäftigten der DB in den 3-S-Zentralen beobachten die Livebilder der Kameras, haben aber keinen Zugriff auf gespeichertes Videomaterial. Die Beschäftigten der Bundespolizei in den 3-S-Zentralen beobachten die Livebilder der Kameras und zeichnen die Videobilder nach den Vorgaben des Bundespolizeigesetzes[146] auf. Durch technische und organisatorische Maßnahmen und eine räumliche Trennung in den 3-S-Zentralen wird ausgeschlossen, dass Beschäftigte der DB auf gespeicherte Videobilder zugreifen. Dieses Verfahren war zunächst nicht zu beanstanden.

Die in jüngster Zeit europaweit zu verzeichnenden Terroranschläge auf sog. „weiche" Ziele[147] haben das Bundesministerium des Innern (BMI) dazu veranlasst, die Sicherheitsmaßnahmen an neuralgischen Punkten verstärken zu lassen.

Hierzu wurde bereits im Jahr 2013 eine „Absichtserklärung zur Videotechnik auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes (Personenbahnhöfe)" geschlossen. Zur Umsetzung der Erklärung hat die DB gemeinsam mit dem BMI und der Bundespolizei ein 6-Jahres-Programm aufgestellt, das mittlerweile in einem Ende 2015 verabschiedeten Rahmenvertrag auf ein 10-Jahres-Programm ausgeweitet wurde. Dieser Vertrag regelt die Ausweitung der Videoüberwachung auf bundesdeutschen Bahnhöfen.

145 JB 1999, 4.6.3; JB 2003, 3.1

146 § 27 BPOLG

147 Als solche werden Orte des öffentlichen Lebens, an denen sich viele Menschen aufhalten, oder weitreichende wichtige Infrastrukturen bezeichnet.

Darüber hinaus ist das BMI der Ansicht, dass Sicherheitsbelange in öffentlich zugänglichen Anlagen mit großem Publikumsverkehr im Allgemeinen künftig noch stärker als bislang zu berücksichtigen sind. Hierzu hat das BMI den Entwurf eines sog. Videoüberwachungsverbesserungsgesetzes vorgelegt, den die Bundesregierung in das Gesetzgebungsverfahren eingebracht hat.[148] Demzufolge soll privaten Stellen der Betrieb von Videokameras zur Verhinderung von Anschlägen erleichtert werden.

Die Datenschutzbehörden des Bundes und der Länder lehnen den Gesetzesentwurf ab.[149] Der Entwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Mit § 6b BDSG existiert bereits seit Jahren ein ausreichender Rechtsrahmen und mit der Orientierungshilfe der Datenschutzaufsichtsbehörden[150] eine praktikable Handlungsanweisung. Hiernach kann die Zulässigkeit einer Videoüberwachung sachgerecht überprüft und beurteilt werden.

3.8.1 Videoüberwachung im Berliner Hauptbahnhof

Der Berliner Hauptbahnhof war einer der ersten Bahnhöfe, in dem die Videoüberwachung durch Neuinstallation und teilweise Erneuerung bestehender Anlagen ausgebaut wurde. Als zuständige Aufsichtsbehörde für die DB beabsichtigten wir Anfang 2016, den Ausbau der Videoüberwachung am Hauptbahnhof datenschutzrechtlich zu überprüfen. Im Vorfeld der Terminvereinbarung wurde jedoch festgestellt, dass die DB es versäumt hatte, vor Beginn des Ausbaus die datenschutzrechtliche Zulässigkeit der Videoüberwachung auf der Grundlage einer Vorabkontrolle zu prüfen.[151]

148 BR-Drs. 791/16 vom 30. Dezember 2016

149 Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 9./10. November 2016: „Videoüberwachungsverbesserungsgesetz" zurückziehen!, Dokumentenband 2016, S.36

150 Orientierungshilfe des Düsseldorfer Kreises vom 19. Februar 2014: „Videoüberwachung durch nicht-öffentliche Stellen", abrufbar unter https://datenschutz-berlin.de/attachments/1034/OH-Videoueberwachung.pdf?1397477659

151 § 4d Abs. 5 BDSG

Dieses Versäumnis wurde – auch im Hinblick auf den künftigen Ausbau der Videoüberwachung an anderen Bahnhöfen – in kürzester Zeit nachgeholt. In der Folge hat die DB einen Maßnahmenplan aufgestellt, wie Bahnhöfe systematisch hinsichtlich der Erforderlichkeit, der Geeignetheit und der Verhältnismäßigkeit zu überprüfen sind. Hierzu wurde die Gesamtzahl der mit Videokameras auszustattenden Bahnhöfe nach Größe in drei Prioritäten eingeteilt, um sie anhand verschiedener Kriterien wie z. B. Reisendenzahlen, Unterführungen oder Knotenpunkten begutachten zu können. Mit der Priorisierung soll sichergestellt werden, dass insbesondere größere Bahnhöfe, die in der Regel auch einer intensiveren Videobeobachtung ausgesetzt sind, zeitnah datenschutzrechtlich geprüft werden.

Alle Personen, die sich auf dem Bahnhof in den öffentlich zugänglichen Bereichen aufhalten, sind von der Videobeobachtung betroffen. Sie können sich ihr nicht entziehen, da sie in sämtlichen Bereichen des Bahnhofs stattfindet. Das gilt insbesondere in gastronomischen Bereichen, die mit Tischen und Sitzgelegenheiten ausgestattet sind und zu einem längeren Verweilen, Entspannen und Kommunizieren einladen.[152] Die Videoüberwachung ist in diesen Bereichen unzulässig. Die DB hat darauf zu achten, dass gastronomische Bereiche innerhalb des Bahnhofs nicht videoüberwacht werden.

Ähnliches gilt für die Videoüberwachung in Anlieferungsbereichen, die regelmäßig von Beschäftigten betreten werden. Da durch eine permanente Beobachtung dieser Bereiche eine Verhaltens- und Leistungskontrolle der Beschäftigten möglich wäre, hatte die DB zu prüfen, in welchem Umfang die Beobachtung von Anlieferungsbereichen erforderlich ist.

Vor diesem Hintergrund stellte die DB bei ihrer (nachgeholten) Vorabkontrolle fest, dass von den ursprünglich 215 Videokameras im Hauptbahnhof 34 Kameras neu auszurichten waren, wobei u. a. fernsteuerbare Funktionalitäten wie die Zoom- und Schwenkbarkeit eingeschränkt wurden. Bei 48 Kameras war keine Anpassung notwendig. Demgegenüber standen 133 Kameras, die den Anforderungen des BDSG nicht entsprachen. Von diesen 133 Kameras wurden 85 für die DB deaktiviert und 48 demontiert, sodass schließlich die Gesamtzahl der zulässigen Kameras auf 82 reduziert werden konnte.

152 Siehe AG Hamburg, Urteil vom 22. April 2008 – 4 C 134/08

Bei der von uns gemeinsam mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit als der zuständigen Aufsichtsbehörde für die Bundespolizei durchgeführten Überprüfung wurde festgestellt, dass die Videoüberwachung mit den verbliebenen Kameras im Berliner Hauptbahnhof überwiegend zulässig ist. Die Beschäftigten in der 3-S-Zentrale nutzen die Livebilder der Kameras hauptsächlich, um das Sicherheitspersonal im Bahnhof über Notfallsituationen zu informieren und bei Einsätzen zu koordinieren. Die Videoüberwachung dient dabei der Unterstützung eines sicheren und ordnungsgemäßen Betriebsablaufs, z. B. der Verkehrssicherung bei Überfüllung von Bahnsteigen bei Großveranstaltungen oder der Koordinierung von Reinigungsmaßnahmen.

Im Hinblick auf die vorgenannten Zwecke bleibt die Wirksamkeit der Videoüberwachung in ihrem Umfang allerdings zweifelhaft, da es in der 3-S-Zentrale derzeit nur vier Arbeitsplätze gibt, von wo aus nicht nur der Hauptbahnhof, sondern alle mit Überwachungstechnik ausgestatteten Bahnhöfe in Berlin mit insgesamt weit über 1000 Kameras überwacht werden. Sie kann lediglich als unterstützende Maßnahme in Kombination mit dem Einsatz von Sicherheitspersonal im Bahnhof sinnvoll sein.

3.8.2 Einsatz von Bodycams bei der Deutschen Bahn AG

Seit Ende Juli 2016 testet die DB im Rahmen eines Pilotprojekts den Einsatz von Bodycams. Bei einer Bodycam[153] handelt es sich um eine sichtbar am Körper getragene Videokamera, die zur Dokumentation des Geschehens in der unmittelbaren Umgebung eingesetzt wird.

Für das Pilotprojekt[154] wurden speziell geschulte Beschäftigte der DB Sicherheit mit einer Bodycam ausgestattet. Das bedeutete konkret, dass bei den in der Regel durch zwei Beschäftigte durchgeführten Kontrollrundgängen nur eine Person eine Bodycam trägt, und zwar diejenige, die nicht primär in ein Handlungsgesche-

153 Engl. für „Körperkamera"

154 Projekt „ChaRiSma" = „Chancen und Risiken von Smartcams im öffentlichen Raum", www.charisma-projekt.de

hen eingreift. Die Bodycams sollten zunächst nur bis zum 31. Dezember 2016 auf den Bahnhöfen Zoologischer Garten, Ostbahnhof und Alexanderplatz eingesetzt werden.

Vor Projektstart legte uns der Konzerndatenschutz der DB ein Konzept für die Pilotphase, den Entwurf einer Arbeitsanweisung für das Sicherheitspersonal und seine vorläufige datenschutzrechtliche Einschätzung vor. Danach speichert das Sicherheitspersonal bei Bedarf die Bilddaten, z. B. im Falle einer eskalierenden Situation. Es werden drei unterschiedliche Kameratypen eingesetzt, wobei zwei Modelle über einen eingebauten Monitor verfügen, in dem sich die gefilmten Personen wie in einem Spiegel sehen. Sofern sich eine zunächst eskalierende Situation wieder „beruhigt", werden die Bilddaten unmittelbar nach Dienstende gelöscht. Kommt es gleichwohl zu Übergriffen, bleiben die Bilddaten gespeichert. In diesen Fällen dienen die Aufnahmen der Beweissicherung. Auslöser für den Einsatz der Bodycams war nach Angaben der DB die steigende Zahl von Übergriffen auf Beschäftigte der DB Sicherheit.

Die Bodycams sollen das Sicherheitspersonal bei der Wahrnehmung und Ausübung des Hausrechts unterstützen,[155] indem durch ihre bloße Existenz ein Abschreckungseffekt erzielt werden soll. Mit ihrem Einsatz sollen eskalierende Situationen vermieden bzw. Straftaten später besser nachgewiesen werden. Ein weiterer Aspekt ist die Eigensicherung des Sicherheitspersonals.

Die schwierige praktische Umsetzung der Hinweispflicht[156] auf die Bodycams konnte durch die Aufschrift „Videoüberwachung" auf der Rückseite und eines Videopiktogramms auf der Vorderseite der Uniformen nur bedingt realisiert werden. Zudem kündigte die DB an, sowohl Betroffene als auch unbeteiligte Reisende mit Visitenkarten und direkten Ansprachen über das Verfahren zu informieren.

Ende November 2016 teilte uns die DB mit, den Test auf die Züge zwischen den drei Bahnhöfen auszuweiten. Bis dahin wurden die Bodycams stets abgelegt, wenn das eingesetzte DB-Sicherheitspersonal z. B. einsatzbedingt zwischen den Bahnhöfen wechselte. Zudem kündigte die DB an, die Testphase über 2016 hinaus

155 Siehe § 6b Abs. 1 Nr. 2 BDSG
156 Siehe § 6b Abs. 2 BDSG

zu verlängern, um z. B. die Auswirkungen von winterbedingten Witterungen (Kälte und Nässe) bezogen auf Akkulaufzeit und Aufnahmequalität besser erproben zu können.

Die Auswertung des Pilotprojekts wird zeigen, ob der Einsatz von Bodycams ein geeignetes Mittel ist, um Straftaten zu verhindern.

4 Verkehr und Wohnen

4.1 Datenerhebung und -verarbeitung bei der BVG auf neuer Rechtsgrundlage

Am 30. August 2016 hat der Senat die Verordnung über die Verarbeitung personenbezogener Daten bei den Berliner Stadtreinigungsbetrieben (BSR), den Berliner Verkehrsbetrieben (BVG) und den Berliner Wasserbetrieben (BWB) neu erlassen.[157] Die ursprüngliche Regelung bildete die Rechtslage aus den Neunzigerjahren ab und war an die aktuellen Entwicklungen anzupassen.

Für die BVG wurde eine Rechtsgrundlage zur Datenerhebung und Datenverarbeitung für die Fälle geschaffen, in denen Fahrgäste bei Kontrollen ohne gültigen Fahrausweis angetroffen werden. Die Senatsverwaltung für Wirtschaft, Technologie und Forschung folgte unserer Auffassung, dass die im Entwurf ursprünglich vorgesehene Erhebung und Verarbeitung der Personalausweisnummer für die Aufklärung derartiger Fälle nicht erforderlich und damit unzulässig war. Die Verordnung regelt neuerdings insbesondere die Bonitätsprüfung von Kundinnen und Kunden, die die BVG bis dahin ohne Rechtsgrundlage vorgenommen hatte. Dies hatte zu zahlreichen datenschutzrechtlichen Beschwerden geführt. Mit den Vorgaben der Verordnung steht diese Datenverarbeitung nun auf einer sicheren und hinreichend bestimmten Rechtsgrundlage einschließlich verbindlicher Löschfristen.

Bonitätsprüfungen durch die BVG sind aufgrund der neuen Verordnung nunmehr zulässig.

157 GVBl. 2016, S. 544

4.2 Datensicherheitsprobleme bei der VBB-fahrCard

Aus der Praxis

Ende 2015 erhielten wir Kenntnis von Datensicherheitsproblemen bei der Nutzung der elektronischen VBB-fahrCard. Durch eine technische Einstellung war es möglich, die personenbezogenen Fahrtdaten der Inhaberinnen und Inhaber der VBB-fahrCard derart zu erheben und zu verarbeiten, dass Bewegungsprofile erstellt und ausgelesen werden konnten. Die Betroffenen hatten darin weder eingewilligt noch gab es dafür eine Rechtsgrundlage.

Die Sicherheitslücke war durch eine fehlerhafte technische Voreinstellung bei den Lesegeräten der BVG-Busse für die VBB-fahrCard entstanden. Durch diese konnten personenbezogene Bewegungsdaten der Betroffenen, wie beispielsweise Uhrzeiten und Standorte, erhoben und gespeichert werden. Die auf der VBB-fahrCard gespeicherten personenbezogenen Daten konnten sowohl durch die Kontrollgeräte der BVG als auch mithilfe der öffentlich nutzbaren App „mytraQ“ von Dritten ausgelesen werden. Die Sicherheitslücke wurde inzwischen von der BVG geschlossen. Wir haben die BVG aufgefordert, die Betroffenen über das Problem zu informieren. Dabei war darauf zu achten, dass die Informationen der Betroffenen individuell erfolgen und auch die Nennung der Löschungsmöglichkeiten umfassen musste. Der BVG wurde darüber hinaus empfohlen, diese Informationen auch transparent auf ihrer Homepage bereitzustellen.

Wir haben diesen Datenvorfall zum Anlass genommen, bei der BVG eine derzeit noch andauernde Prüfung einzuleiten, die Fragen des Datenschutzes und der Datensicherheit umfasst.

Das Problem der Erstellung von Bewegungsprofilen bei der Nutzung der VBB-fahrCard wurde gelöst. Die Prüfung dauert an.

4.3 Neue Entwicklungen im Automobilverkehr – wird der Fahrer immer gläserner?

Im letzten Jahr[158] berichteten wir darüber, wie die Digitalisierung auch im Verkehrsbereich stetig voranschreitet und welche möglichen Risiken dabei aus Sicht des Datenschutzes erwachsen. Aktuell sind hierbei insbesondere das vernetzte und autonome Fahren wichtige Zukunftsfelder.

Im selben Maße, wie die Vernetzung der Stadt- und Verkehrsinfrastruktur vorangetrieben wird, geschieht dies auch bei den Fahrzeugen selbst. Dieser Trend betrifft sowohl Personen- als auch Lastkraftwagen. Durch die Vernetzung von Fahrzeugen untereinander mit Hilfe sog. C2C- (Car-to-Car-) und C2X- (Car-to-Infrastructure-) Dienste sind moderne Autos zunehmend in der Lage, miteinander zu kommunizieren und Daten auszutauschen. Ziel dieser Techniken ist es, dass entsprechend konfigurierte Fahrzeuge anhand der erhaltenen Informationen den Fahrer frühzeitig auf Gefahrensituationen und Verkehrsbehinderungen hinweisen können, um somit die Sicherheit im Straßenverkehr zu erhöhen und gleichzeitig den Verkehrsfluss zu verbessern. So kann z. B. ein vorausfahrendes Auto nachfolgende Fahrzeuge vor einem Stau oder Glatteis warnen. Ebenso ist es möglich, dass Fahrzeuge Hinweise zu Unfällen und Baustellen austauschen.

Die Funktechniken für die Kommunikation der Fahrzeuge untereinander reichen meist nur einige hundert Meter weit. Diese Reichweite kann jedoch durch Einbeziehung von Teilen der Verkehrsinfrastruktur als C2X-Dienste, wie z. B. Ampelanlagen, Brücken oder Verkehrsleitzentralen, deutlich erweitert werden. Geeignete Teile der bestehenden Infrastruktur werden hierfür umgerüstet. In Bayern wurde zur Förderung des autonomen Fahrens vor kurzem auch ein erster geeigneter Testabschnitt auf der Autobahn zwischen München und Ingolstadt eingerichtet. Dort wurden schwarz-weiße, rund 70 Zentimeter breite Schilder als Orientierungspunkte für computergesteuerte Autos aufgestellt, mit denen diese ihre eigene Position zentimetergenau bestimmen können. Das Bundesverkehrsminis-

158 JB 2015, 2.3

terium hat Teile der A9 und A93 zum „digitalen Testfeld Autobahn“ erklärt. Seit Mai 2015 erproben dort verschiedene Automobilfirmen autonom fahrende Pkw.[159]

Ungeklärt war bisher in weiten Teilen noch die Frage, wer wann und in welchem Umfang Zugriff auf die Daten der Fahrzeugnutzer und -insassen erhält. Ebenso war bisher nicht eindeutig geregelt, welche der beteiligten Institutionen die verantwortliche Stelle gegenüber dem Fahrzeughalter ist, sofern dieser eine Auskunft über die erhobenen und gespeicherten Daten verlangt. Um diesen Missstand zu beheben und mehr Transparenz herzustellen, finden seit dem Jahr 2014 verstärkt regelmäßige Gespräche zwischen den deutschen Aufsichtsbehörden für den Datenschutz und der Automobilwirtschaft statt. Im Zuge dessen haben sich die Mitglieder des Verbands der Automobilindustrie in einer gemeinsamen Erklärung mit den unabhängigen Datenschutzbehörden des Bundes und der Länder im Januar 2016 auf einheitliche Prinzipien verständigt.[160] Dadurch soll u. a. sichergestellt werden, dass die Fahrzeugnutzer durch verschiedene Optionen über die Verarbeitung und Nutzung ihrer personenbezogenen Daten selbst bestimmen können. Die Automobilhersteller streben an, durch standardisierte Symbole im Cockpit den aktuellen Vernetzungsstatus des Fahrzeugs erkennbar anzuzeigen und Möglichkeiten der jederzeitigen Aktivierung und Deaktivierung dieses Status vorzusehen. Darüber hinaus besteht gegenüber dem Hersteller ein unentgeltliches Auskunftsrecht des Halters über seine durch den Hersteller erhobenen und gespeicherten personenbezogenen Daten.[161]

Die neuen Möglichkeiten der Digitalisierung der Fahrzeugwelt haben zusätzlich auch in anderen Wirtschaftszweigen zu neuen Geschäftsmodellen geführt. So nimmt in den letzten Jahren das Angebot an Kfz-Versicherungstarifen zu, welche die Prämie für den Versicherungsnehmenden sehr präzise anhand erhobener Fahrzeugdaten berechnen. Diese Tarife für die Kfz-Haftpflicht werden oftmals als „Pay-as-you-drive“ (PAYD)-Tarife[162] bezeichnet. Hierbei wird im Fahrzeug zusätzlich zur bereits vorhandenen Technik eine kleine Box eingebaut, welche permanent

159 siehe http://www.spiegel.de/auto/aktuell/verkehrsschilder-auf-der-a9-und-a93-was-bedeutet-dieses-schild-a-1126092.html

160 Dokumentenband 2016, S. 9

161 § 34 Bundesdatenschutzgesetz (BDSG)

162 „Bezahle dafür, wie du fährst.“

alle Fahrtzeiten, -strecken und -häufigkeiten aufzeichnet und zusätzlich auch das Fahrverhalten analysiert. So wird u. a. gemessen, mit welcher Geschwindigkeit und in welchem Neigungswinkel der Fahrer in Kurven fährt, in welchen Gebieten er unterwegs ist und ob er das Auto bevorzugt nachts oder tagsüber nutzt. Zusätzlich fließt auch die Fahrweise des Fahrers in die Bewertung ein (etwa ruhiger oder aggressiver Fahrstil, sportliches oder gemächliches Beschleunigungsverhalten). Aus all diesen Rohdaten wird anhand von Algorithmen eine Bewertung erstellt, die die Grundlage für die Kalkulation des Versicherungstarifs bildet. Die Bewertung auf Basis der ermittelten Daten kann sowohl direkt im Fahrzeug oder mit einem Dienstleister vorgenommen werden. Im zweiten Fall erhält der Dienstleister die Rohdaten, erstellt daraus die Statistik und gibt diese an die Versicherung weiter. Nach eigener Auskunft haben die Versicherungen in beiden Fällen keinen Zugriff auf die Rohdaten.

Die Versicherungen werben damit, dass mit derartigen Angeboten ein rücksichtsvoller und defensiver Fahrstil gefördert wird und somit auch die Versicherungsbeiträge für entsprechend umsichtige Fahrer sinken. Zugleich soll damit die allgemeine Verkehrssicherheit erhöht werden. Ob sich diese positiven Prognosen bewahrheiten, kann erst in einigen Jahren beurteilt werden. Aktuell gibt es in Deutschland nur wenige Versicherungsgesellschaften, die entsprechende Tarife anbieten. Unbestritten bleibt für die Nutzenden derartiger Versicherungstarife das Risiko bestehen, dass anhand der umfangreichen Datenerhebung genaue Bewegungs- und Nutzungsprofile erstellt werden können, die auch eine Missbrauchsgefahr beinhalten.

Hier sind alle Beteiligten aus Forschung, Industrie und Politik gefordert, vernünftige und verbindliche Rahmenbedingungen zu schaffen, die einerseits technischen Fortschritt ermöglichen und gleichzeitig sicherstellen, dass der Kunde weiterhin sein Recht auf informationelle Selbstbestimmung ausüben kann und das Fahrzeug als technisches Gesamtsystem gegen unbefugte Eingriffe von außen geschützt bleibt. In Zukunft müssen an technische Systeme im Automobilbereich ähnlich hohe Anforderungen wie in anderen Branchen gestellt werden. Nur eine sichere, effiziente und gleichzeitig datensparsame Fahrzeugtechnik kann hier der Weg für das Fahrzeug des 21. Jahrhunderts sein.

Im Sinne der Erhöhung der Verkehrssicherheit sowie zur Steigerung des persönlichen Komforts beim Autofahren ist die stetige Fortentwicklung im Automobilbereich durchaus zu begrüßen. Gleichzeitig sollte dabei jedoch nicht außer Acht gelassen werden, dass durch die zunehmenden technischen Möglichkeiten auch neue Risiken entstehen.

4.4 Smart Meter und das vernetzte Zuhause – neue Entwicklungen und mögliche Risiken

Die in den letzten Jahren umfassend voranschreitende Digitalisierung des Alltags setzt sich weiter fort und erfasst auch zunehmend mehr Anwendungsgebiete innerhalb des eigenen Heims. Viele neue Produkte sind bereits ab Werk dafür konfiguriert, auch über das Internet Daten zu empfangen und zu senden. Und dies betrifft bei Weitem nicht mehr nur Alltagsprodukte wie Computer, Smartphones oder Fernseher (Smart TVs). Selbst eher unverdächtige Haushaltsgegenstände wie Kühlschränke, Waschmaschinen, Einbauherde oder Rollläden für die Fenster können heute oftmals auch „online" angebunden werden, um dann vom Nutzer jederzeit per Internetverbindung mit der passenden App ferngesteuert zu werden. So können Waschmaschine und Herd bereits eingeschaltet werden, wenn man selbst noch auf dem Weg nach Hause ist, und der Kühlschrank könnte auf Wunsch selbstständig neue Lebensmittel online beim Supermarkt bestellen.

Besonders deutlich wird die zunehmende Vernetzung der eigenen vier Wände für viele Menschen im Bereich intelligenter Messgeräte, sog. Smart Meter. Hierbei handelt es sich um digitale Zähler, welche typische Verbrauchsgrößen wie Wasser, Gas und Strom ermitteln, speichern und automatisiert per Funk übermitteln. Seitdem der Gesetzgeber festgelegt hat, dass diese Geräte von Vermietern und Immobilienbesitzern schrittweise in vielen Gebäuden verpflichtend eingebaut werden müssen, rüsten insbesondere Wohnungsbaugesellschaften und private Vermieter immer mehr Objekte damit aus.

Gegen den technischen Fortschritt ist nichts einzuwenden, sofern hierbei auch dem Datenschutz und der Datensicherheit ausreichend Rechnung getragen wird. Gerade dies ist jedoch leider oftmals nicht der Fall. Viele Geräte übertragen die

ermittelten Verbrauchswerte automatisch mehrfach am Tag (oftmals sogar im Sekundentakt) per Funk, ohne dass ein derart häufiger Datenversand notwendig erscheint, da nach wie vor die Ablesung bzw. Erfassung der Verbrauchswerte durch den Vermieter oder den entsprechenden Lieferanten häufig nur ein bis zwei Mal pro Jahr erfolgt. Darüber hinaus mussten wir feststellen, dass viele Geräte die Daten unverschlüsselt übertragen, sodass nicht ausgeschlossen werden kann, dass Unbefugte die Daten unbemerkt mitlesen oder sogar dauerhaft speichern. Mit passender technischer Ausstattung und entsprechendem Know-how wäre es durchaus möglich, anhand der ermittelten Daten detaillierte Verbrauchs- und Nutzungsprofile zu erstellen, die wiederum Rückschlüsse auf die Lebensumstände der Betroffenen (z. B. auch auf ihre Abwesenheiten) ermöglichen. Sowohl Gerätehersteller als auch Vermieter, Energiewirtschaft und Gesetzgeber schenken diesem Risiko bisher zu wenig Beachtung.

Bei allen Vorteilen, die das vernetzte Zuhause haben mag, darf nicht außer Acht gelassen werden, dass durch die zunehmenden technischen Möglichkeiten auch neue Risiken entstehen, denen entgegengewirkt werden muss.

4.5 Ausschluss unbequemer Personen bei der Mieterratswahl?

In diesem Jahr wurden bei allen landeseigenen Wohnungsbaugesellschaften zum ersten Mal Mieterräte gewählt. Diese sollen den Mieterinnen und Mietern mehr Mitbestimmungsrechte verschaffen. Bei der Prüfung, welche Kandidatinnen und Kandidaten für die Wahl zugelassen werden, kam es zu datenschutzrechtlichen Unregelmäßigkeiten.

Zur Durchführung der Wahl hat jede Wohnungsbaugesellschaft jeweils eine Wahlkommission eingesetzt, die aus Mieterinnen und Mietern sowie Beschäftigten des Wohnungsunternehmens gebildet wird. Die Wahlkommission kann Kandidierende, die sich für den Mieterrat bewerben, unter bestimmten Voraussetzungen ablehnen. Die Ablehnungsgründe werden in der Wahlordnung genannt und sind zum Teil sehr unbestimmt. So können Bewerberinnen und Bewerber nicht nur bei schweren Verletzungen der Pflichten aus dem Mietvertrag oder der Hausord-

nung abgelehnt werden, sondern auch bei „schwerwiegenden Verstößen gegen das friedliche Zusammenleben“. Was genau darunter zu verstehen ist, ist auslegungsbedürftig.

Die Wahlkommissionen der meisten Wohnungsbaugesellschaften haben von dieser Klausel Gebrauch gemacht und mehrere Bewerberinnen und Bewerber ausgeschlossen. Einige davon haben sich gegen den Ausschluss gewehrt und sich nach einem erfolglosen Widerspruchsverfahren an uns gewandt. Insbesondere wurde moniert, dass die betreffende Wohnungsbaugesellschaft im Rahmen dieses Widerspruchsverfahrens Dossiers zu den Kandidierenden angelegt hatte, auf deren Grundlage die Wahlkommission über die Ablehnung oder die Zulassung zur Wahl entscheiden sollte. Die Daten aus diesen Dossiers stammten zum Teil aus einer Internetrecherche und zum Teil aus der Mieterakte. Dort wurde z. B. festgehalten, ob sich die Betroffenen in der Vergangenheit öffentlich kritisch über die Wohnungsbaugesellschaft geäußert, ob sie sich an Mieterprotesten beteiligt oder bestimmten Modernisierungsmaßnahmen widersprochen hatten.

Diese Datensammlung war unzulässig. Grundsätzlich dürfen Daten aus der Mieterakte nur zur Durchführung des Mietverhältnisses verwendet werden. Sollen die Daten für andere Zwecke verwendet werden, muss eine Einwilligung eingeholt oder zumindest den Betroffenen transparent gemacht werden, dass sie damit rechnen müssen, dass ihre Mieterakte ausgewertet wird, wenn sie sich für den Mieterrat bewerben. Selbst dann dürfen nicht alle Informationen aus der Mieterakte verwendet werden, sondern nur solche, die schwere Verletzungen der Pflichten aus dem Mietvertrag oder der Hausordnung bzw. schwerwiegende Verstöße gegen das friedliche Zusammenleben im Sinne der Wahlordnung beinhalten. Ob die Betroffenen bestimmten Modernisierungsmaßnahmen widersprochen, sich an Mieterprotesten beteiligt oder sich kritisch geäußert haben, gehört jedenfalls nicht dazu. Schließlich soll der Mieterrat auch die Mieterinteressen in die Arbeit der Wohnungsbaugesellschaften einbringen, sodass es nicht im Sinne der Wahlordnung sein kann, kritische Bewerberinnen und Bewerber von vorneherein von einer Kandidatur auszuschließen.

Zu der durchgeführten Internetrecherche mit der Suchmaschine Google ist festzustellen, dass diese alle möglichen Daten über eine Person zu Tage fördert. Diese betreffen regelmäßig auch das Privatleben der Betroffenen. Sie ist an sich

schon ungeeignet, Ausschlussgründe im Sinne der Wahlordnung zu recherchieren. Vielmehr kommt es unweigerlich zu einer Erhebung von Daten, die für die Wahl nicht relevant sind. Sie ist daher ebenfalls unzulässig.

Wir haben diese Bewertung der betroffenen Wohnungsbaugesellschaft mitgeteilt. Zusätzlich haben wir eine Reihe von Empfehlungen erteilt, die insbesondere die Transparenz des Verfahrens betreffen. Ebenso haben wir empfohlen, dass Leitlinien erarbeitet werden, wie die relativ unbestimmten Ausschlussgründe aus der Wahlordnung zu interpretieren sind, damit zukünftig die zuständigen Mitarbeiterinnen und Mitarbeiter der Wohnungsbaugesellschaft wissen, welche Daten an die Wahlkommission herausgegeben werden dürfen.

5 Jugend und Bildung

5.1 Gemeinsame Ausführungsvorschriften für Maßnahmen zum Kinderschutz – eine unendliche Geschichte?

Aus der Praxis

Wir haben uns erneut mit dem Entwurf der „Gemeinsamen Ausführungsvorschriften über die Durchführung von Maßnahmen zum Kinderschutz in den Jugend-, Gesundheits- und Sozialämtern des Landes Berlin (AV Kinder- und Jugendschutz JugGesSoz)“ befasst. Obwohl bereits Ende 2015 ein zwischen der federführenden Senatsverwaltung für Bildung, Jugend und Wissenschaft und uns abgestimmter Entwurf vorlag, in dem die von uns vorgetragenen Kritikpunkte berücksichtigt waren,[163] sind die in der Praxis dringend benötigten Ausführungsvorschriften auch ein Jahr danach noch nicht in Kraft getreten. Grund hierfür ist die noch immer fehlende Zustimmung der Senatsverwaltung für Gesundheit.

Wir haben an den Entwürfen wiederholt kritisiert, dass die vom Gesetzgeber den einzelnen Akteuren im Bereich des Kinderschutzes zugewiesenen Aufgaben nicht ausreichend differenziert berücksichtigt wurden. Wir haben darauf hingewiesen, dass sich der gesetzliche Schutzauftrag bei Kindeswohlgefährdung[164] allein an die Jugendämter richtet, während den Gesundheitsämtern in erster Linie präventive Aufgaben im Bereich des Kinderschutzes zugewiesen sind. Aus diesen gesetzlichen Aufgabenzuweisungen ergeben sich unterschiedliche datenschutzrechtliche Befugnisse der Beteiligten, so dass wir immer wieder deutlich gemacht haben, dass der von der Senatsverwaltung für Gesundheit in den Entwürfen formulierte gemeinsame Schutzauftrag der Jugend- und Gesundheitsämter rechtlich nicht begründbar ist, eine erhebliche Gefahr unzulässiger Datenerhebungen und -übermittlungen birgt und von uns nicht mitgetragen werden kann. In einer konstruktiven Zusammenarbeit mit der Senatsverwaltung für Bildung, Jugend und

163 JB 2015, 6.2

164 § 8a Sozialgesetzbuch – Achtes Buch (SGB VIII)

Wissenschaft konnte ein Entwurf der Ausführungsvorschriften abgestimmt werden, in dem die von uns beschriebenen rechtlichen Einwände ausgeräumt und die Aufgaben und Befugnisse der Jugend- und Gesundheitsämter praxisgerecht beschrieben wurden. Leider hat sich die Senatsverwaltung für Gesundheit an diesem gemeinsamen inhaltlichen Abstimmungsprozess nicht beteiligt und den Entwurf als nicht konsensfähig angesehen.

Offenbar besteht zwischen der Senatsverwaltung für Gesundheit und uns ein unterschiedliches Verständnis zum Zweck der Ausführungsvorschriften. Wir gehen davon aus, dass mit den Ausführungsvorschriften die gesetzlich geregelten Aufgaben und Befugnisse in praxisgerechter Weise ausgestaltet werden sollen, um den in den Jugend- und Gesundheitsämtern Tätigen praktische Anweisungen für ihr tägliches Handeln zu geben. Dies ist gerade im Bereich des Umgangs mit Kindeswohlgefährdungen im Interesse der Rechtssicherheit unerlässlich, gerade auch im Hinblick auf die datenschutzrechtlichen Regelungen zum Umgang mit personenbezogenen Daten der betroffenen Familien.

Die Ausführungen der Senatsverwaltung für Gesundheit in der Stellungnahme des Senats[165] zu unserem letzten Jahresbericht lassen dagegen eher die Annahme zu, mit den Ausführungsvorschriften sollten Aufgaben zugewiesen werden, die politisch gewünscht, jedoch nicht im Gesetz verankert sind. So heißt es in der Stellungnahme u. a. , Anliegen der Neufassung sei die Weiterentwicklung des „Netzwerk Kinderschutz". Dazu gehöre, dass dem Kinderschutz grundsätzlich Vorrang vor dem Datenschutz eingeräumt werde. Auch sei es nicht zutreffend, dass der Gesetzgeber den Schutzauftrag bei Kindeswohlgefährdung (ausschließlich) den Jugendämtern zuweist bzw. zugewiesen hat.[166]

Die Ausführungen der Senatsverwaltung für Gesundheit stehen im Gegensatz zur geltenden Gesetzeslage. Kinderschutz und Datenschutz stehen nicht im Gegensatz zueinander. Vielmehr kann ein effektiver Kinderschutz nur gelingen, wenn auch die datenschutzrechtlichen Rahmenbedingungen eingehalten werden. Der Gesetzgeber hat insoweit Befugnisse geschaffen, die Datenverarbeitungen zum

165 Drs. 18/0028 vom 24. November 2016

166 Drs. 18/0028, S. 84 ff.

Zwecke der Abwehr von Kindeswohlgefährdung gerade zulassen. Es besteht weder Bedarf, Befugnisse zu erweitern, noch wären Ausführungsvorschriften hierfür geeignet.

Im Herbst haben wir auf Arbeitsebene ein konstruktives Gespräch mit den beiden beteiligten Senatsverwaltungen geführt. Es konnte auf dieser fachlichen Ebene eine Einigung auf der Grundlage des zwischen der Senatsverwaltung für Bildung, Jugend und Wissenschaft und uns bereits Ende 2015 abgestimmten Entwurfs erzielt werden. Leider wurde dieses Ergebnis auf politischer Ebene von der Senatsverwaltung für Gesundheit nicht mitgetragen, so dass die Praxis auch weiterhin auf die Ausführungsvorschriften warten muss.

Da die seit 2008 geltenden Ausführungsvorschriften zum Kinderschutz veraltet sind und ein großes Bedürfnis nach praktischer Ausgestaltung der gesetzlichen Regelungen besteht, sollten die Ausführungsvorschriften nunmehr endlich in Kraft gesetzt werden.

5.2 Kinderschutzambulanzen für Berlin

Der Senat hat im Jahr 2007 sein Konzept für ein Netzwerk Kinderschutz[167] beschlossen[168]. In den Folgejahren wurden nachhaltige ressortübergreifende Kooperationsstrukturen und Netzwerke weiterentwickelt bzw. neu geschaffen, um so eine Verbesserung des Kinderschutzes im Land Berlin zu erreichen. Tragisch verlaufene Kinderschutzfälle mit Todesfolge haben jedoch gezeigt, dass weitere Verbesserungen notwendig sind. Da sich Kindeswohlgefährdungen ohne besonders geschulten medizinischen Sachverstand nicht immer ohne Weiteres erkennen lassen, zeigte sich die Notwendigkeit, spezialisierte Kinderschutzambulanzen zu schaffen, in denen medizinisch besonders qualifizierte Fachkräfte, ggf. unter Hinzuziehung weiterer Fachdisziplinen, das jeweilige Kind begutachten und eine medizinische Diagnose vornehmen können.

167 Drs. 16/0285 vom 20. Februar 2007
168 JB 2006, 2.1

Im April 2016 haben fünf Kinderschutzambulanzen an verschiedenen Standorten mit ihrer Arbeit begonnen. Sie stehen so mit ihrer kinderärztlichen Expertise als kompetente Anlaufstellen für die Klärung von Verdachtsfällen von Kindeswohlgefährdung zur Verfügung. Die Untersuchungen in den Kinderschutzambulanzen setzen voraus, dass die sorgeberechtigten Eltern ihr Einverständnis in die Untersuchung sowie eine Schweigepflichtentbindungserklärung erteilen, damit die Kinderschutzambulanzen die Untersuchungsergebnisse an die die Untersuchung veranlassende Stelle (in der Regel das Jugendamt bzw. der Kinder- und Jugendgesundheitsdienst) weitergeben dürfen. Lediglich in denjenigen Fällen, in denen das Jugendamt das Kind aufgrund bestehender Indizien zunächst aufgrund eigener Entscheidung oder durch einen bereits vorliegenden familiengerichtlichen Beschluss in seine Obhut nehmen muss, kann die Untersuchung ohne diese Einwilligung veranlasst werden.

Angesichts der weitreichenden Folgen, die für die Eltern mit der Inanspruchnahme der Kinderschutzambulanzen verbunden sein können, und vor dem Hintergrund, dass eine vertrauensvolle Zusammenarbeit mit den Eltern von entscheidender Bedeutung für die Einleitung wirksamer Hilfen ist, ist es wichtig, den Eltern die Arbeitsweise der Kinderschutzambulanzen möglichst transparent zu machen. Auf diese Weise kann bei allen Beteiligten die in diesem sensiblen Bereich notwendige Rechtssicherheit erreicht werden.

Wir haben frühzeitig darauf hingewiesen, dass bereits in dem Konzept für die Etablierung der Kinderschutzambulanzen die datenschutzrechtlichen Rahmenbedingungen berücksichtigt werden sollten. In der praktischen Umsetzung haben wir die federführende Senatsverwaltung für Bildung, Jugend und Wissenschaft bei der Entwicklung einer informierten und transparenten Einwilligungs- und Schweigepflichtentbindungserklärung nebst Informationsblatt für die Eltern umfassend beraten. Den Kinderschutzambulanzen konnte diese Erklärung bereits bei Aufnahme ihrer Arbeit zur Verfügung gestellt werden. Sie wird unter Berücksichtigung der praktischen Erfahrungen weiterentwickelt werden.

Um die Zusammenarbeit zwischen den bezirklichen Jugend- und Gesundheitsämtern und den Kinderschutzambulanzen transparent zu machen, wurden die Verfahren und Abläufe durch die Senatsverwaltung für Bildung, Jugend und Wissenschaft in einem Leitfaden beschrieben, an dem wir ebenfalls beteiligt wurden.

Mit der Einführung der Kinderschutzambulanzen ergaben sich auch praktische datenschutzrechtliche Fragen hinsichtlich der Art und Weise der Verarbeitung und Speicherung der Daten der Kinder in den jeweiligen Krankenhausinformationssystemen sowie der Zugriffsrechte innerhalb der jeweiligen Klinik. Wir haben die Datenschutzkonzepte der einzelnen Kinderschutzambulanzen in Bezug auf die Einbindung der Kinderschutzambulanzen geprüft und im Wesentlichen für umsetzbar gehalten.

Wir werden die Arbeit der Kinderschutzambulanzen auch weiterhin datenschutzrechtlich begleiten und uns dafür einsetzen, dass die Verfahren und Abläufe im Interesse eines effektiven Kinderschutzes für alle Beteiligten rechtssicher ausgestaltet werden.

5.3 Einführung des Jugendportals „jup! Berlin“

Wir haben die Jugend- und Familienstiftung des Landes Berlin bei der Umsetzung des von der Senatsverwaltung für Bildung, Jugend und Wissenschaft in Auftrag gegebenen Internetportals „jup! Berlin“ beraten und werden das Projekt auch weiterhin begleiten.

Das Jugendportal „jup! Berlin“ soll zu einer zentralen Anlaufstelle für Jugendliche aus Berlin werden. Derzeit umfasst das Angebot an die Jugendlichen altersgerecht und zeitgemäß aufbereitete Informationen über aktuelle und allgemeine Themen, die die Probleme, Sorgen und Fragen der Jugendlichen betreffen. Über den Web-Browser und per Smartphone-App ist das Portal leicht erreichbar. Perspektivisch soll zudem ein Online-Beratungsangebot ausgebaut werden.

Ein weiterer wesentlicher Teil des Angebotes ist eine Übersicht der lokalen Angebote für Jugendliche in den Bezirken. Die jeweiligen Einrichtungen können sich auf dem Portal darstellen, auf eigene Webangebote verlinken und Termine von Veranstaltungen eintragen. Die Einrichtungen und Veranstaltungen werden den Jugendlichen übersichtlich, u. a. auf einer Karte, angezeigt.

Unsere Beratung bezog sich einerseits auf die technische Sicherheit der Plattform sowie auf die hohen datenschutzrechtlichen Anforderungen, die an ein Online-Beratungsangebot zu stellen sind. Hierfür müsste eine Nachrichtenaustauschplattform genutzt werden, da das Medium E-Mail weder die von den Jugendlichen gewünschte Anonymität noch technisch die erforderliche Sicherheit zur Übertragung von oft sensitiven personenbezogenen Daten sicherstellen kann, wenn diese nicht verschlüsselt werden. Auch werden E-Mails oder SMS- oder Messenger-Nachrichten u. U. an mehreren Stellen gespeichert, die weder unter der Kontrolle der Nutzer noch des Jugendportals stehen. Zudem besteht eine erhöhte Gefahr, dass Metadaten (d. h. wer kommuniziert mit wem) ausgewertet werden. Dadurch bestünde die Gefahr, dass die Informationen darüber, dass sich eine jugendliche Person an ein konkretes Beratungsangebot gewendet hat, an Dritte übermittelt würden. Bei dem bekannten Messenger-Dienst „WhatsApp“ besteht diese Gefahr in erhöhtem Maße durch die Weitergabe von Daten unklaren Umfangs an Facebook.[169]

Datenschutzrechtlich problematisiert haben wir auch die vom Jugendportal geplante Einbindung von sozialen Netzwerken und vor allem die Nutzung von YouTube für die Bereitstellung von Videoinhalten. Dies ist für ein mit öffentlichen Mitteln finanziertes Angebot problematisch, weil es sich um kommerzielle Anbieter handelt, die Daten der Nutzung ihrer Plattformen personenbezogen oder zumindest pseudonymisiert auswerten und u. a. für Werbezwecke nutzen.

Da Jugendliche mehrheitlich aktive Nutzer dieser Plattformen sind, ist es für uns nachvollziehbar, dass die Präsenz auf Facebook und YouTube für ein Jugendportal wichtig ist. Solange Alternativen wie ein eigenes Webangebot verfügbar sind, auf dem die wesentlichen Informationen ebenfalls verfügbar sind, ist es für uns akzeptabel, dass diese Angebote für die Bereitstellung von Informationen genutzt werden. Wir konnten erreichen, dass bei „jup! Berlin“ eine anonym bzw. pseudonym nutzbare Kommentarfunktion zur Verfügung steht.

Wir haben problematisiert, dass der Besuch des Webangebotes „jup.berlin“ nicht automatisch zu einer Datenweitergabe an Dritte führen darf. Dies ist jedoch im Internet leider oft der Fall: Bindet eine Webseite ein Social-Plugin wie

169 Siehe 12.4

z. B. einen Like-Button so ein, wie die Plattformbetreiber dies vorsehen, so werden die Daten über den Besuch der Webseite an die jeweilige Plattform weitergegeben und von dieser oft zu Werbe- und sonstigen Zwecken ausgewertet. Daher ist die Einbindung von Social-Plugins nur zulässig, wenn sie erst auf Aufforderung der Nutzenden aktiviert werden. Dies ist bei „jup! Berlin“ entsprechend umgesetzt worden.

Ein vergleichbares Problem zeigt sich auch bei der Einbindung von eingebetteten YouTube-Videos. Auch diese externen Videos müssen so eingebunden werden, dass die Datenübermittlung erst auf Aufforderung durch die Nutzerinnen und Nutzer erfolgt. Hierzu wird derzeit eine Lösung erarbeitet, die die Nutzung der Videos auf datenschutzgerechte Weise ermöglicht.

In konstruktiven Gesprächen mit den Beteiligten konnte erreicht werden, dass den Datenschutzbelangen bei der Implementierung des Portals Rechnung getragen wird. Wir werden das Jugendportal auch weiterhin begleiten und planen, mit den Betreibern in Bezug auf die Präsentation von Datenschutzinhalten für die Zielgruppe der Jugendlichen zu kooperieren.

5.4 Ein neues Fachverfahren für die Jugendhilfe – Fortsetzung

Die schrittweise Einführung von neuen Teilen des Fachverfahrens ISBJ[170] in den bezirklichen Jugendämtern schreitet voran. Mit ISBJ-WJH, der Komponente zur Bearbeitung der Aufgaben der wirtschaftlichen Jugendhilfe, wurde in drei Pilotbezirken der Anfang gemacht, mittlerweile läuft die Komponente in allen Bezirken. Die Teilkomponente zur Unterstützung der regionalen sozialen Dienste – ISBJ-RSD – steht kurz bevor.

Die Einführung eines verwaltungsübergreifenden Großprojekts erfordert viele koordinierende Arbeiten, die durch die Senatsverwaltung für Bildung, Jugend und Wissenschaft mit großem Engagement durchgeführt wurden. Die wesentli-

170 Integriertes System Berliner Jugendhilfe

chen Dokumente wurden in einem konstruktiven Abstimmungsprozess den datenschutzrechtlichen Anforderungen angepasst. Uneinigkeit besteht noch in der Frage, ob im Rahmen des Fach- und Finanzcontrollings lesender Zugriff auf Klientendaten eingeräumt werden muss. Entscheidend hierfür ist die Klärung der Frage, ob diese Aufgabe auch mit bereits anonymisierten bzw. pseudonymisierten Daten erfüllt werden kann. Hierzu befinden wir uns noch in Gesprächen mit der Senatsverwaltung. Das notwendige verfahrensspezifische Sicherheitskonzept lag uns vor. Es wurde auf Basis des BSI-Standards 100-2 erarbeitet. Allerdings wurde er nicht konsequent angewendet. So werden die Maßnahmen der Bausteine zwar aufgeführt, die vorgeschriebene Anpassung an die lokalen Bedingungen fehlt jedoch. Die Wirkung der vorgesehenen Maßnahmen muss durch ihre Darstellung einschätzbar sein. Klare Handlungsanweisungen führen zu vorhersehbaren Ergebnissen bei der Umsetzung und ermöglichen anschließend auch die Kontrolle der Durchführung der Maßnahmen.

Auch für die Einführung der weiteren Teilkomponenten gehen wir von einem konstruktiven Abstimmungsprozess mit der fachlich zuständigen Senatsverwaltung aus und erwarten, dass die datenschutzrechtlichen Anforderungen weiterhin berücksichtigt werden.

5.5 Unverschlüsselte Datenübermittlung per E-Mail zwischen Schulämtern und Schulen

Zwischen den Schulämtern in den Bezirken und den Schulen findet ein regelmäßiger Austausch personenbezogener Daten über Schülerinnen und Schüler statt, der für Planungszwecke durchaus notwendig und zulässig ist. Hierbei werden auch sensitive Daten übermittelt, wie Förderprognose und sonderpädagogischer Förderungsbedarf, die Rückschlüsse auf geistige oder körperliche Behinderungen der Betroffenen erlauben.

Während die Schulen bereits vielfach die Möglichkeit haben, den Datenaustausch per E-Mail verschlüsselt vorzunehmen, ist dies bei den Schulämtern nicht der Fall. Die Schulen werden daher aufgefordert, die Schülerdaten in Tabellenform unverschlüsselt an die Schulämter zu übermitteln.

Wir haben seit 2012 in mehreren Schreiben an die Senatsverwaltung für Bildung, Jugend und Wissenschaft auf die notwendigen technisch-organisatorischen Maßnahmen hingewiesen und Mindestanforderungen definiert, die bei dem Datenaustausch eingehalten werden müssen. Die regionalen Schuldatenschutzbeauftragten haben zusätzlich regelmäßig auf das Problem hingewiesen. 2015 haben wir darüber hinaus alle Bezirke in Form eines Fragebogens direkt zur Stellungnahme bezüglich des Umfangs der übermittelten Daten sowie der eingesetzten technischen Übermittlungswege aufgefordert. Auf diese Schreiben haben wir eine abgestimmte Antwort aller bezirklichen Schulämter erhalten, die aber die Frage nach der sicheren Übermittlung der Daten im Unklaren ließ. Ein Bezirk teilte mit, dass die Übermittlung von Daten sogar dann mittels unverschlüsselter E-Mail erfolge, wenn andere Wege empfohlen würden. Ein weiterer Bezirk hatte bereits zu einem früheren Zeitpunkt die Einführung verschlüsselter E-Mail-Kommunikation angekündigt, die Umsetzung jedoch bisher nicht bestätigt. Insgesamt ist davon auszugehen, dass die Kommunikation zwischen den Schulämtern und den Schulen weiterhin grundsätzlich unverschlüsselt und damit ohne einen entsprechenden Schutz erfolgt.

Wir haben gegenüber den Schulämtern der Bezirke die Anforderungen an die Übermittlung personenbezogener und insbesondere sensitiver Daten nochmals konkretisiert und um einen Zeitplan für die Umsetzung gebeten. Auf dieses Schreiben haben wir auch zwei Monate nach Fristablauf noch keine Antwort erhalten.

Seit Jahren erfolgt die Übermittlung von sensitiven Daten von Schülerinnen und Schülern zwischen den Schulen und den Schulämtern ohne ausreichende technische Schutzmaßnahmen. Unsere Hinweise, Nachfragen und Aufforderungen haben zu keiner wesentlichen Verbesserung der Situation geführt.

5.6 Erhebung von Angaben zur Staatsbürgerschaft bei der Einschulung

Bei der Anmeldung eines schulpflichtigen Kindes wurden die Eltern vom zuständigen Schul- und Sportamt auf die weiteren Staatsbürgerschaften, die das Kind neben der deutschen Staatsbürgerschaft habe, angesprochen. Die Eltern waren

der Auffassung, dass die Erhebung von Angaben über weitere mit der Geburt erworbene Staatsbürgerschaften für die Einschulung und den dafür notwendigen Verwaltungsablauf nicht erforderlich ist.

Vom Schulamt erhielten wir den Hinweis, dass die Daten der zukünftigen Schulanfänger dem Schulamt ca. vier bis fünf Wochen vor der Schulanmeldung auf dem Web-Server des Landesamtes für Bürger- und Ordnungsangelegenheiten (LABO) zur Verfügung gestellt würden. Neben dem Familiennamen, den Adress- und Geburtsdaten seien dort auch alle vorhandenen Staatsangehörigkeiten aufgelistet. Die Daten würden dann vom Schulamt an die Schulen weitergeleitet.

Bei der vom Schulamt mitgeteilten Bereitstellung von Daten handelt es sich um eine regelmäßige Datenübermittlung des LABO an die bezirklichen Schulbehörden. Dabei werden den Schulämtern die Angaben u. a. zum Vor- und Familiennamen, Tag und Ort der Geburt, Geschlecht, gesetzlichen Vertreter, zur Staatsangehörigkeit, zu gegenwärtigen und früheren Anschriften aller Einwohner vom vollendeten 4. Lebensjahr bis zum vollendeten 18. Lebensjahr übermittelt. Zweck der regelmäßigen Datenübermittlung durch das LABO an die Schulbehörde ist die Umsetzung des Schulgesetzes (Schulpflicht und vorschulische Sprachförderung).

Nach dem Schulgesetz[171] dürfen die Schulbehörden personenbezogene Daten von Schülerinnen und Schülern verarbeiten, soweit dies zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen schulbezogenen Aufgaben erforderlich ist. Nach der Schuldaten-Verordnung[172] darf auch die Staatsangehörigkeit einer Schülerin oder eines Schülers erfasst werden. Werden vom LABO im Rahmen der regelmäßigen Datenübermittlungen zu einer Person mehrere Staatsangehörigkeiten übermittelt, so hat die Schulbehörde zu entscheiden, welche dieser Staatsangehörigkeiten für die Erfüllung der Aufgaben nach dem Schulgesetz erforderlich ist. Das LABO selbst kann diese Entscheidung im Vorfeld der Datenübermittlung nicht treffen. Die Schulbehörde darf sodann nur die zur Aufgabenerfüllung nach dem Schulgesetz erforderlichen Daten zur Staatsangehörigkeit nutzen, im Rahmen des Einschulungsverfahrens speichern und an die aufnehmende Schule übermitteln. Hat die betroffene Person neben der deutschen Staatsangehörigkeit weitere

171 § 64 Abs. 1 SchulG
172 § 2 Abs. 2 Nr. 6

Staatsangehörigkeiten, ist davon auszugehen, dass für die Erfüllung schulbezogener Aufgaben nur die Erfassung der deutschen Staatsangehörigkeit erforderlich ist.

Vom Schulamt wurde uns bestätigt, dass die vom LABO übermittelten Daten zukünftig genauer hinsichtlich der angegebenen Staatsangehörigkeiten überprüft würden. Sollten für zukünftige Schulanfängerinnen und Schulanfänger mehrere Staatsangehörigkeiten angegeben sein, werde vom Schulamt nur noch die jeweils relevante Staatsangehörigkeit an die jeweils zuständige Schule übermittelt.

Auch in Routineverfahren ist die Erforderlichkeit der Datenverarbeitung im Einzelfall zu prüfen.

5.7 Klassenlehrer eröffnet „WhatsApp"-Gruppe für Eltern

Ein besorgter Vater teilte mit, dass der Klassenlehrer seines Kindes auf Anregung anderer Eltern für die Klasse eine gemeinsame „WhatsApp"-Gruppe eingerichtet habe, für die dieser die ihm bekannten privaten Mobilfunknummern nutzte. Dadurch sollte der Informationsfluss vom Klassenlehrer in die Gruppe (z. B. bei Hausaufgaben, Übungen oder Änderungen im Ablauf schulischer Veranstaltungen), aber auch der zwischen den Eltern untereinander sowie mit dem Klassenlehrer (für Nachfragen bei unklaren Aufgabenstellungen oder Unstimmigkeiten etc.) erleichtert werden.

Davon ausgehend, dass die Mitteilungen des Klassenlehrers an die Gruppenmitglieder auch Angaben über Schülerinnen, Schüler, Eltern und Lehrkräfte enthalten, handelt es sich um eine Übermittlung von personenbezogenen Daten der Betroffenen durch die Schule an private Dritte (die Gruppenmitglieder). Eine derartige Übermittlung ist für die Schule nur unter den Voraussetzungen des Schulgesetzes Berlin zulässig.[173] Keine der dort genannten Voraussetzungen ist hier erfüllt. Insbesondere kann die Datenübermittlung durch den Klassenlehrer auch nicht auf die Einwilligung der Betroffenen gestützt werden.

173 § 64 Abs. 5 SchulG

Eine datenschutzrechtlich wirksame Einwilligung setzt voraus, dass die Betroffenen von der datenverarbeitenden Stelle (Schule) umfassend über die Datenverarbeitungsvorgänge unterrichtet wird, um die Bedeutung und Tragweite ihrer Erklärung überblicken zu können (informierte Einwilligung). Bei dem Anbieter des Instant-Messaging-Dienstes „WhatsApp" handelt es sich um ein US-amerikanisches Unternehmen, bei den USA um ein Drittland ohne angemessenes Datenschutzniveau. Da nicht auszuschließen ist, dass US-amerikanische Einrichtungen und Behörden auf den Datenbestand des Unternehmens zugreifen können,[174] kann der Anbieter von „WhatsApp" die Einhaltung eines angemessenen Schutzniveaus im Sinne der europäischen Datenschutzregelungen nicht garantieren. Für die Teilnehmenden einer „WhatsApp"-Gruppe (Betroffene) ist es somit nicht möglich, die Bedeutung und Tragweite ihrer Erklärung zur Datenverarbeitung zu überblicken. Eine „informierte" Einwilligung in die Datenverarbeitung durch die Schule im Rahmen der Mitgliedschaft in einer „WhatsApp"-Gruppe ist somit nicht möglich. Die Einwilligung in die Datenverarbeitung ist zudem schriftlich zu erteilen und hat freiwillig zu erfolgen. Auch wenn die Eltern der Mitgliedschaft in der „WhatsApp"-Gruppe zugestimmt haben, kann die Freiwilligkeit dieser Erklärung bezweifelt werden, da nicht auszuschließen ist, dass das Akzeptieren der Teilnahme an der „WhatsApp"-Gruppe bei einigen Eltern mit der Befürchtung einherging, dass ihre Kinder ansonsten schulische Nachteile zu erleiden hätten.

Auch aus technisch-organisatorischen Aspekten ist die Einrichtung einer „WhatsApp"-Gruppe durch die Schule unzulässig. Die IT-Sicherheit des Messenger-Dienstes „WhatsApp", insbesondere die Vertraulichkeit der übertragenen Nachrichten, ist nicht gewährleistet. Zwar behauptet der Betreiber, dass die Daten verschlüsselt (im Ende-zu-Ende-Verfahren) übertragen würden, dies ist aber nicht in allen Fällen garantiert. Zudem erfährt der Anbieter des Dienstes dennoch die Umstände der Kommunikation (wer kommuniziert mit wem und zu welchen Zeitpunkten).[175]

Nachdem wir die Schulleitung in der Angelegenheit entsprechend beraten hatten, teilte diese uns unverzüglich mit, dass die „WhatsApp"-Gruppe aufgelöst und eine Datenschutzschulung für alle Lehrkräfte angesetzt worden sei.

174 Siehe 1.1
175 Siehe 12.4

Davon ausgehend, dass an anderen Schulen vergleichbare „WhatsApp"-Gruppen zur Kommunikation zwischen Lehrkräften und Eltern eingerichtet werden, haben wir es ausdrücklich begrüßt, dass die Senatsverwaltung für Bildung, Jugend und Wissenschaft Anfang 2016 den Entwurf einer „Ausführungsvorschrift zur Nutzung sozialer Medien durch Dienstkräfte an Schulen" vorgelegt hat, mit der den Lehrkräften in Berlin untersagt werden sollte, „für die dienstliche Kommunikation untereinander oder mit Schülerinnen und Schülern offene soziale Medien (z. B. Facebook, Google+, Twitter, WhatsApp) zu nutzen." Die Bedenken von Schulleitungen, das Verbot schränke die pädagogischen Freiräume der Lehrkräfte im Umgang mit sozialen Medien zu sehr ein, hat leider dazu geführt, dass der Entwurf der Ausführungsvorschrift zurückgezogen wurde. Damit wurde eine Chance vertan, vor Ort in der Schulpraxis für rechtsklare Verhältnisse zu sorgen.

Der Einsatz von sozialen Medien wie „WhatsApp" zur dienstlichen Kommunikation von Lehrkräften mit Dritten (z. B. Schülerinnen und Schülern, Eltern) ist rechtswidrig.

5.8 Wie geht's bei euch zu Hause zu? – Befragung von Schülerinnen und Schülern zum Sozialverhalten der Eltern

Datenerhebungen sollten grundsätzlich bei der betroffenen Person selbst vorgenommen werden. Dieses sog. Direkterhebungsprinzip im Datenschutzrecht soll insbesondere für Transparenz und Kontrolle der Datenerhebungen sorgen. Wenn im Ausnahmefall die Erhebung nicht bei der betroffenen Person stattfindet, müssen diese Ziele dennoch so gut wie möglich erfüllt werden. Wir hatten eine Schulstudie zu bewerten, die dieser Vorgabe nicht von vornherein gerecht wurde.

Schulen sind ein beliebtes Forschungsfeld. Schülerinnen und Schüler werden im Rahmen einer steigenden Zahl von Untersuchungen befragt. Dabei werden beispielsweise die Leseleistungen, das mathematische und naturwissenschaftliche Grundverständnis, computer- und informationsbezogene Kompetenzen, aber auch die Angebotsqualität und individuelle Wirkungen von Ganztagsschulen sowie der Übergang ins Ausbildungs- und Beschäftigungssystem untersucht. Die

Fragen betreffen allerdings teilweise nicht ausschließlich die Schülerinnen und Schüler selbst.

Teilweise fragen Forscher auch nach Sachverhalten, die die Eltern betreffen. Normalerweise werden diese unmittelbar im Rahmen einer freiwilligen Elternbefragung angesprochen. Die Schülerinnen und Schüler bringen hierfür einen Fragebogen sowie ein Informationsblatt zur Studie mit nach Hause. So können die Eltern ohne Zwang entscheiden, ob sie und ggf. welche Fragen sie beantworten wollen.

Wir hatten über eine Studie zu entscheiden, bei der den Schülerinnen und Schülern zahlreiche die Eltern betreffende Fragen gestellt wurden. Diese bezogen sich etwa auf die Beziehungen zu und Aktivitäten mit den Eltern, die finanzielle Situation, Berufstätigkeit und Ausbildung der Eltern, aber auch auf Probleme wegen Scheidung oder Trennung sowie die Form des Zusammenlebens. Begründet wurden entsprechende Fragen in der Regel damit, dass zahlreiche – auch außerschulische – Faktoren Einfluss auf die Leistung von Schülerinnen und Schülern haben können.

Im Rahmen der Studie sollten die Eltern durch ein Anschreiben nur allgemein darüber informiert werden, dass Fragen zum familiären und sozialen Hintergrund der Schülerinnen und Schüler gestellt würden. Nur beispielhaft wurden die Inhalte der Fragen erwähnt (zu Hause gesprochene Sprache, Staatsangehörigkeit, familiäre Beziehungen, Anzahl der Geschwister, berufliche Situation und Herkunftsland der Eltern). Auf dieser unvollständigen Informationsgrundlage sollten die Eltern eine Einwilligung erteilen.

Wir haben dieser Gestaltung der Studie widersprochen. Entsprechende Angaben zum familiären und sozialen Hintergrund sollten grundsätzlich in einer Elternbefragung direkt erhoben werden. An die Einwilligung bzw. die Begleitinformationen für die Eltern sind daher entsprechende Anforderungen zu stellen. Ohnehin hat eine Einwilligung informiert zu erfolgen, um wirksam zu sein. Das bedeutet, dass die konkreten elternbezogenen Fragen in übersichtlicher Weise unmittelbar einsehbar sein oder den Eltern vollständig zur Verfügung gestellt werden müssen. Nur unter dieser Voraussetzung kann von einer informierten Einwilligung als Rechtsgrundlage für die Datenerhebung ausgegangen werden. Wir konnten erreichen, dass die Unterlagen der Studie entsprechend angepasst wurden.

Vom Direkterhebungsgrundsatz darf nur in Ausnahmefällen abgewichen werden. In diesem Fall müssen geeignete Maßnahmen getroffen werden, um die Interessen der betroffenen Personen an Transparenz und Kontrolle zu gewährleisten. Die konkreten Daten, die bei Dritten erhoben werden sollen, müssen für die betroffene Person unmittelbar erkennbar sein.

5.9 Bibliotheken im Zeitalter der Digitalisierung

Wir haben den Verbund der Öffentlichen Bibliotheken Berlins (VÖBB) und die Zentral- und Landesbibliothek (ZLB) zu verschiedenen Digitalisierungsprojekten beraten. Ziel des Projektes „Digitale Welten" ist es, der Bibliothekskundschaft eine Fülle von Medien wie z. B. E-Books, Hörbücher, Musik und Filme online zugänglich zu machen. Wir begrüßen und unterstützen dieses Projekt, da hier als Zusatzangebot ein breiterer und zeitgemäßer Zugang zu den Angeboten der Bibliotheken geschaffen wird. Ein weiteres Projekt ermöglicht die Ausleihe von Lesegeräten für elektronische Bücher, sog. E-Book-Reader.

Es stellte sich die Frage, welche personenbezogenen Daten über die Nutzenden bei den Bibliotheken und externen Angeboten anfallen. Für die Ausleihe physischer Medien in den öffentlichen Bibliotheken ist seit langem die Maxime der Datensparsamkeit umgesetzt. Gespeichert werden Ausleihvorgänge nur solange wie nötig, d. h. bis das jeweilige Medium zurückgegeben wurde und etwaige Gebühren bezahlt worden sind.

Bei digitalen Medien (z. B. E-Books) wird die „Rückgabe" durch ein digitales Rechtemanagement (DRM) sichergestellt, welches fast ohne personenbezogene Daten auskommt. Das Rechtemanagement sorgt auf technischem Wege dafür, dass die Medien nicht über den vorgesehenen Zeitraum hinaus genutzt werden können. Gespeichert werden Ausleihvorgänge daher nur bis zum Ende der Leihfrist oder bis zur vorzeitigen Rückgabe.

Auf andere Angebote (z. B. Audiodateien) kann nur für einen begrenzten Zeitraum zugegriffen werden.

Während bei digitalen Angeboten häufig die Autorisierung der Nutzenden problematisch ist, da Nutzernamen und Passwörter an externe Anbieter entsprechender Angebote weitergegeben werden, erfolgt in Berlin die Autorisierung der Nutzenden direkt auf den Webseiten des VÖBB. Die jeweiligen externen Anbieter erhalten nur einen zeitlich befristeten Nachweis ohne Personenbezug über die Legitimation der Nutzenden. Diese Lösung begrüßen wir, da dadurch bei dem jeweiligen Dritten kein oder nur ein zeitlich beschränktes und zudem pseudonymes Nutzungsprofil entsteht.

Lediglich bei wenigen Einzelangeboten werden die Log-in-Daten auf den Webseiten der Dritten erhoben und zur Prüfung unmittelbar an den VÖBB übermittelt. Dieser plant, mittelfristig auch hier datenschutzgerechte technische Lösungen zu finden. Für die Übergangszeit ist die Nutzung der Daten durch die Dritten vertraglich ausgeschlossen.

Bezüglich der Entleihe von Lesegeräten stellte sich die Frage, welche Daten auf den Geräten bei Rückgabe verbleiben. Nach unserer Beratung wird den Nutzenden nun bei erstmaliger Ausleihe ein Merkblatt übergeben, das auch auf Datenschutzfragen eingeht. So wird z. B. empfohlen, die WLAN-Funktion unterwegs zu deaktivieren, um das Erheben von Bewegungsprofilen durch Hotspot-Betreiber zu vermeiden. Zudem wird empfohlen, das Gerät vor Rückgabe auf die Werkseinstellungen zurückzusetzen, wodurch unserer Kenntnis nach alle Daten gelöscht werden.

Die Bibliotheken bieten neben E-Books eine Reihe von weiteren digitalen Medien online über das Internet an und erweitern damit ihr Angebot für einen breiten Nutzungskreis. Hierbei legen die Bibliotheken großen Wert auf eine datenschutzgerechte Umsetzung, die wir auch weiterhin gern begleiten.

6 Gesundheit und Soziales

6.1 Ein Tanker versucht umzusteuern: Erste Schritte auf dem Weg zu Transparenz und systematischer Datensicherheit bei der Charité

Aus der Praxis

2015 haben wir gravierende Defizite bei der Einhaltung der gesetzlichen Vorgaben zur Einführung von neuen IT-Verfahren und der Führung eines Verzeichnisses dieser Verfahren bei der Charité festgestellt.[176] Wir verfolgten weiter, ob und wie diese Defizite behoben wurden.

Das größte Universitätsklinikum Deutschlands betreibt eine Vielzahl von informationstechnischen Verfahren für Krankenbehandlung und Forschung. 2015 mussten wir feststellen, dass die Charité den Überblick über die bei ihr betriebene Datenverarbeitung verloren hatte. Neue Verfahren wurden ungeregelt eingeführt. Die Sicherheit der verarbeiteten sensitiven Daten stand infrage.

Auf unsere formelle Beanstandung hin bekannte sich die Charité zu einer zügigen Beseitigung der Mängel. Eine Projektgruppe zur Aufarbeitung wurde beauftragt. Neue organisatorische Regelungen wurden erlassen. Der sog. CISO[177] wurde ausgetauscht. Der Vorstand der Charité ließ sich regelmäßig von den Fortschritten berichten.

Doch diese lassen auf sich warten. Auch ein Jahr nach der Beanstandung ist das gesetzlich vorgeschriebene Verzeichnis der Verarbeitungstätigkeiten nicht vollständig erstellt. Die Arbeit daran liegt mehrere Monate hinter dem Plan. Für die größere Aufgabe der Herstellung der durchgehenden und systematischen Informationssicherheit nach gesetzlicher Vorgabe liegt noch nicht einmal ein Zeitplan vor.

176 JB 2015, 8.4.1

177 „Chief Information Security Officer", also die für die Koordination aller Maßnahmen für die Gewährleistung der Sicherheit der Daten der Institution verantwortliche Person

So bleiben Teilergebnisse: Ende 2016 lag eine Übersicht über die zentral von den Geschäftsbereichen der Charité betriebenen Verfahren vor. Ziele und Zwecke der Verarbeitungstätigkeiten wurden benannt, ebenso wessen Daten erfasst werden und welche Daten das sind. Das Woher und Wohin der Daten wurde beschrieben.

Die Erfassung der Angaben über die ungewisse Zahl von dezentralen Prozessen in den vielen Kliniken, Instituten und anderen Einrichtungen der Charité hat jedoch gerade erst begonnen, vernünftigerweise verknüpft mit dem Bestreben, diese Prozesse zu vereinheitlichen und, soweit möglich, unter zentrale Steuerung zu stellen. Die Zusammenstellung der Informationen dagegen, wie die Verarbeitung erfolgt, blieb selbst bei zentralen Verfahren nur skizzenhaft, obwohl Transparenz Voraussetzung dafür ist, dass sich Kranke, Probandinnen und Probanden, Beschäftigte und Studierende sicher sein können, dass mit ihren Daten rechtmäßig umgegangen wird. Die Verarbeitung von Daten durch die moderne Medizintechnik, die die Charité betreibt, blieb gleich völlig außen vor, womit eine gähnende Lücke bestehen blieb, sowohl in der Gewährleistung des Datenschutzes als auch der Informationssicherheit.

In Bezug auf die Sicherheit der Daten musste die Charité bekennen, dass sie für keines der betriebenen Verfahren über ein dem Stand der Technik entsprechendes Sicherheitskonzept verfügt. Mehrere Anläufe zu einer Erarbeitung auch mit externer Unterstützung waren in den vergangenen Jahren im Sande verlaufen.

Die Arbeiten im Berichtszeitraum erbrachten eine grobe Klassifizierung der eingesetzten Technik und eine erste Einschätzung, welche der vom Bundesamt für Sicherheit in der Informationstechnik empfohlenen Maßnahmen bereits umgesetzt worden sind. Die Charité unternimmt Einiges, um die Datensicherheit zu gewährleisten. Doch sind auch die Defizite vielzählig. Selbst grundlegende Konzepte sind bisher nicht sämtlich ausgearbeitet. In Ermangelung einer Analyse lassen sich die Risiken nicht abschätzen oder einordnen. Ein Umsetzungsplan, der Defizite benennt, priorisiert und aufführt, in welchem Ablauf Lücken geschlossen werden sollen, steht noch in weiter Ferne.

Die Trägheit der Fortschritte auf beiden Gebieten hat ihre Ursache nicht in dem mangelnden Engagement der beteiligten Fachkräfte, sondern in dem Missverhältnis zwischen der Komplexität der Aufgabe angesichts der Struktur und Größe

der Charité einerseits und den zur Verfügung gestellten Ressourcen auf der anderen Seite. Das Datenschutzteam der Charité hatte jahrelange Defizite parallel zum Tagesgeschäft aufzuarbeiten, und das bei personellen Ressourcen, die unter denen vergangener Jahre lagen. Im Geschäftsbereich Informationstechnik wurde die Pflege des Informationssicherheitsmanagementsystems verantwortlichen Beschäftigten als zusätzliche Aufgabe neben ihrer bisherigen Tätigkeit übertragen. Der neue CISO ist zwar in der Lage, dringend benötigte Kompetenz einzubringen, wurde jedoch bisher nur stundenweise beschäftigt.

Krankenhäuser, die eine zentrale Rolle bei der Krankenversorgung einer Region übernehmen, gehören zur kritischen Infrastruktur. Patientinnen und Patienten haben nicht die Wahl, auf andere Häuser auszuweichen, in denen möglicherweise dem Datenschutz und der Datensicherheit größere Aufmerksamkeit geschenkt wird. Der daraus resultierenden unabweisbaren Verantwortung kann die Charité nur mit substanziellen neuen Mitteln und dem entschlossenen Willen gerecht werden, die über lange Jahre aufgehäuften Defizite schnellstmöglich abzubauen.

Der Wille zur Aufarbeitung datenschutzrechtlicher Mängel muss sich in der Bereitstellung adäquater Mittel ausdrücken, sowohl zum Aufbau benötigter eigener Kompetenz und zur Gewährleistung der nötigen personellen Ausstattung für Datenschutz und Informationssicherheit als auch zur Hinzuziehung externer Unterstützung zur Bewältigung der nötigen Nacharbeit der Versäumnisse. Die Charité hat hier noch einen weiten Weg vor sich.

6.2 Fernwartung in Krankenhäusern: Löcher in der Brandmauer

Aus der Praxis

Wir haben zwei große Krankenhausunternehmen in Berlin daraufhin geprüft, ob sie dem Schutz der Patientendaten auch bei der Wartung ihrer Informations- und Medizintechnik ausreichend Gewicht beimessen und die gesetzlichen Anforderungen einhalten.

Krankenhäuser betreiben komplexe Informationstechnik (IT). Damit diese zuverlässig ihren Dienst tun kann, Weiterentwicklungen übernommen und Sicherheits-

defizite beseitigt werden, ist eine regelmäßige Wartung von Software und Geräten erforderlich. In aller Regel besitzen selbst große Krankenhäuser mit substanziellen IT-Abteilungen nicht die Kompetenz, diese Wartungsaufgaben selbst zu übernehmen. Für eine Wartung vor Ort durch externe Spezialisten stehen vielfach die finanziellen Ressourcen nicht zur Verfügung. Daher wird der größte Teil der Informations- und der Medizintechnik durch Dritte aus der Ferne gewartet.

Der Gesetzgeber hat daher Krankenhäusern die Wartung von Datenverarbeitungssystemen durch Dritte ausdrücklich gestattet, auch wenn den Dienstleistern dabei Patientendaten offenbart werden.[178] Doch hat er hierfür klare Anforderungen gestellt, die den Schutz der Patientendaten im Auge haben:[179] Das Krankenhaus muss die volle Kontrolle über die eigene IT behalten. Wartungsvorgänge dürfen nur mit Wissen und Wollen der verantwortlichen Beschäftigten erfolgen und müssen während der Durchführung und im Nachhinein kontrolliert werden können. Weder Namen der Patienten noch Angaben über ihren Gesundheitszustand dürfen von den Dienstleistern eingesehen werden, wenn dies nicht unabweislich notwendig ist.

Für den Fall einer Offenlegung der Daten an einen Dienstleister ist dieser zur Geheimhaltung zu verpflichten.[180] Auch bei ihm dürfen Daten, die in seine Verfügung gelangen und im Krankenhaus der Schweigepflicht unterlegen haben, nicht beschlagnahmt werden. Dennoch bleibt es bei dem Widerspruch, dass eine Offenbarung von Patientengeheimnissen durch eigenes Personal der Kliniken strafbar ist, fremdes Personal dieser Strafandrohung trotz Geheimhaltungsverpflichtung jedoch nicht unterliegt. Die Datenschutzaufsichtsbehörden verlangen daher schon seit langem die Ausdehnung der Strafbarkeit auf externe IT-Dienstleister von Berufsgeheimnisträgern.

Schließlich darf die externe Wartung die Sicherheit der im Krankenhaus gespeicherten Daten nicht gefährden. Der Zugriff darf nur über einen verschlüsselten Kanal erfolgen. Dieser Kanal muss im Bedarfsfall durch das Krankenhaus selbst

178 Im Gegensatz zur allgemeinen Verarbeitung von Patientendaten durch Dritte; siehe 1.3

179 § 24 Abs. 6 Landeskrankenhausgesetz (LKG) i. V. m. § 3a Berliner Datenschutzgesetz (BlnDSG)

180 § 3a Abs. 2 Satz 3 BlnDSG

oder auf dessen Initiative hin aufgebaut werden. Jeder autorisierte Beschäftigte des Dienstleisters muss seine Identität beim Zugriff auf die Krankenhaus-IT nachweisen. Die Zugriffswege müssen so gestaltet werden, dass sie nicht von Dritten missbraucht werden können. Und auch die Wartungsdienstleister selbst sind in ihrer Zugangsberechtigung auf die Systeme zu beschränken, für die sie zuständig sind.

In den kontrollierten Krankenhäusern fanden wir eine lückenhafte Umsetzung dieser Vorgaben. Vorgaben sowohl der mit den Dienstleistern eingegangenen Verträge als auch interner Handlungsanweisungen wurden nicht umgesetzt. Der Schutz der Übertragungskanäle gegen das Mitlesen Dritter entsprach häufig nicht dem Stand der Technik. Verfahren wurden eingesetzt, die mittlerweile als kompromittierbar eingeschätzt werden. Oft hängt die Sicherheit des Krankenhausnetzwerks von einer einzigen Schutztechnik ab, obwohl bei hoch schutzwürdigen Systemen empfohlen wird, eine zweite Schutzlinie aufzubauen. Man spricht hier von einer „Verteidigung in der Tiefe" und setzt u. a. auf mehrfache Verschlüsselung und die Aufteilung des Netzes der Institution in mehrere Teilbereiche, die voneinander getrennt werden.

Am deutlichsten trat jedoch hervor, dass die Krankenhäuser bewusst in Kauf nehmen, die Hoheit über ihre Informationstechnik in Teilen zu verlieren, und sie vollständig in die Hände der Dienstleister geben. Es wird kein Sinn mehr darin gesehen, Kontrolle über die Dienstleister auszuüben, da ein Nachvollzug des Handelns dieser Dritten außerhalb der eigenen Kompetenz liegt. Die Tore zur Krankenhaus-IT stehen ständig offen, eine Protokollierung der Wartungsvorgänge erfolgt nur bruchstückhaft. Die Grenzen zu einem vollständigen Outsourcing von Teilen der Krankenhaus-IT verschwimmen.

Diesem hat der Berliner Gesetzgeber jedoch eine klare Absage erteilt:[181] Die Souveränität über die Patientendaten soll bei den Krankenhäusern selbst bleiben, die sich hierbei durchaus untereinander unterstützen können. So betreiben bereits jetzt in einzelnen Fällen Berliner Krankenhäuser IT-Verfahren für andere kooperierende Häuser.

181 § 24 Abs. 6 Satz 2 LKG i. V. m. § 3a Abs. 1 und 2 BlnDSG

In der Ausweitung dieser Kooperation könnte der Schlüssel für eine Krankenhaus-IT liegen, die Kompetenz zum Wohl der Patienten bündelt, effiziente und verlässliche IT-Dienste für die Prozesse im Krankenhaus gewährleistet und die Schweigepflicht unter ärztlicher Kontrolle wahrt. Die Gesundheitspolitik des Landes Berlin wird gut daran tun, diesen Prozess zu fördern, wenn sie Kompetenz im Land halten und Abhängigkeiten von Anbietern im In- und Ausland in diesem sensiblen Bereich nicht ausufern lassen möchte.

Krankenhäuser sind bei der Inanspruchnahme von Wartungsdienstleistungen verpflichtet, die Kontrolle über deren Ausführung zu wahren und die technischen Vorkehrungen nach dem Stand der Technik zu treffen, die notwendig sind, um unbefugte Eingriffe von Dritten und durch die Dienstleister selbst abzuwehren.

6.3 Patientenportale: Wer greift zu?

Wir haben ein Krankenhausunternehmen beraten, das beabsichtigt, seinen Patientinnen und Patienten Daten über ihre Behandlung über das Internet zur Verfügung zu stellen.

Wer sich im Krankenhaus behandeln lässt, möchte zumeist, so gut es ihm möglich ist, verstehen, was mit ihm geschieht, wie der Gesundheitszustand einzuschätzen ist und welche Hinweise es für die weitere Entwicklung gibt. Dies zu erläutern ist die Aufgabe der Ärztinnen und Ärzte. Doch diese stehen unter hohem zeitlichen Druck. Nicht immer gehen ihre Erklärungen weit genug oder in jedes die Betroffenen interessierende Detail. Vielleicht möchte die erkrankte Person auch nicht nur selbst in Patientenakte und Befunde hineinschauen, sondern außerhalb des Krankenhauses stehenden medizinischen Fachkräften Einblick geben, um unabhängige Einschätzungen oder Ratschläge zu erhalten. Das Zivilrecht gibt den Behandelten das Recht, nach dem Ende des Krankenhausaufenthalts elektronische Kopien ihrer Patientenakte zu erhalten. Aus Sicht des Krankenhauses lag es daher nahe, das weit verbreitete Instrument des modernen Menschen, sein Smartphone, zu nutzen, um diesen Einblick zu geben. Dies würde es nicht nur ermöglichen, die gewünschten Informationen noch während der stationären Behandlung

zu geben, es würde auch ein späteres langes Warten auf das Zusammentragen und Versenden der Daten vermeiden.

So naheliegend die Idee sein mag, so befrachtet ist ihre Umsetzung mit Hindernissen. Denn wie nützlich eine Dienstleistung auch ist, sie darf die Patientendaten keinen unangemessenen Risiken aussetzen, weder diejenigen Daten, die abgerufen werden, noch diejenigen all der Patientinnen und Patienten, die ein derartiges elektronisches Verfahren nicht wünschen. Die Daten müssen in die richtigen Hände gelangen. Auf dem Weg soll sie niemand mitlesen können. Und schließlich darf die Abrufmöglichkeit nicht die Sicherheit des Computernetzwerks des Krankenhauses schwächen. All diese Gefahren bestehen aber bei einem Abruf von Gesundheitsdaten über das Smartphone oder über ein anderes persönliches Gerät der Betroffenen.

Bei der Beratung des Krankenhausunternehmens war es unser Ziel, auf die höchstmögliche praktikabel erreichbare Sicherheit des Verfahrens hinzuwirken.

Leider konnte dabei noch nicht auf eine eigentlich seit 2003 gesetzlich vorgesehene Lösung zurückgegriffen werden, die zugleich hohe Sicherheit und Komfort bieten könnte: die elektronische Gesundheitskarte. Mit ihr soll sowohl eine elektronische Patientenakte als auch ein Patientenfach verknüpft werden, in welches das Krankenhaus die interessierenden Daten kopieren und aus dem die Versicherten sie mit ihrer Karte abrufen könnten. Doch liegt das Vorhaben weit hinter dem Plan. Insbesondere die Ärzteschaft hat immer wieder den Datenschutz in der Infrastruktur, die hinter der Gesundheitskarte steht, in einem Grad in Zweifel gestellt, der von den Datenschutzaufsichtsbehörden nicht geteilt wird.

Das von uns beratene Projekt ist in der Folge bei Weitem nicht das einzige, bei dem eine Funktion, die mit der Gesundheitskarte auf hohem Sicherheitsniveau abbildbar wäre, auf niedrigerem Schutzniveau in einer Insellösung einzelner Leistungserbringer bereits erbracht wird bzw. erbracht werden soll.

Der größte Schwachpunkt im Projekt des von uns beratenen Krankenhauses ist die Tatsache, dass die Patientinnen und Patienten dabei ihre eigenen Computer benutzen sollen. Viele Betroffene verfügen jedoch nicht über die Kenntnisse, um ihren Computer so zu schützen, wie es für ihre sensitiven Gesundheitsdaten ei-

gentlich erforderlich wäre. Damit vertrauen sie u. U. sehr sensible Informationen über sich selbst einem Gerät an, dessen Sicherheitsschwächen womöglich – wie bei Smartphones älterer Bauart mit dem Betriebssystem Android typisch – allgemein bekannt und ausnutzbar sind. Über diese Risiken müssten die Betroffenen zumindest deutlich aufgeklärt werden, damit sie eine bewusste Entscheidung treffen können, ob sie dieses Risiko in Kauf nehmen wollen.

Das Krankenhaus ist in jedem Falle verpflichtet, sicher festzustellen, ob tatsächlich die richtige Person Daten aus dem Patientenportal abruft. Hier helfen moderne technische Verfahren, die nicht nur auf das Wissen der sich Identifizierenden zurückgreifen wie z. B. typischerweise ein Passwort. Zusätzlich verlangen sie auch den Nachweis des Besitzes eines Objekts, das der Person eindeutig zugeordnet ist. Solche Objekte können die Form von Schlüsselanhängern haben, die auf jeden Knopfdruck eine neue Ziffernfolge anzeigen, welche nur diejenigen kennen können, die diesen Anhänger in der Hand halten. Auch ein Smartphone kann die Rolle eines solchen Objekts spielen – genau das war der Plan im vorgelegten Projekt. Doch wer dieses Smartphone gleichzeitig auch zum Surfen und für den Zugriff auf das Patientenportal nutzt, der öffnet potenziellen Angreifern Tür und Tor. Das haben erfolgreiche Angriffe auf das Online-Banking in den letzten Jahren mehrmals eindrucksvoll gezeigt.

Wir haben das Unternehmen in Bezug auf angemessene technische Schutzmaßnahmen beraten. Im kommenden Jahr werden wir überprüfen, wie die Umsetzung erfolgt, und einen besonders gründlichen Blick auf die Computersysteme des Krankenhauses werfen, auf denen die Daten bereitgestellt werden. Ein Angriff auf diese frei im Internet zugänglichen Systeme darf nicht dazu führen, dass Gesundheitsdaten von Patientinnen und Patienten offengelegt werden.

Es ist begrüßenswert, wenn Patientinnen und Patienten Zugriff auf Daten über ihre Gesundheit und Behandlung erhalten. Die Technik, die dabei zum Einsatz kommt, muss hohen Sicherheitsansprüchen gerecht werden und dafür sorgen, dass die Informationen ausschließlich in die Hände der Betroffenen gelangen.

6.4 Unabhängige Patientenberatung Deutschland: Der schwierige Weg zur anonymen Beratung

Durch eine Beschwerde wurde uns bekannt, dass die Unabhängige Patientenberatung Deutschland es entgegen ihren Zielen und geltendem Recht den Ratsuchenden erschwert, eine anonyme Beratung zu erhalten.

Die Unabhängige Patientenberatung Deutschland (UPD) soll Verbraucherinnen und Verbraucher sowie Patientinnen und Patienten in gesundheitlichen und gesundheitsrechtlichen Fragen qualitätsgesichert und kostenfrei informieren und beraten. Wir hatten uns im Jahr 2011 bei dem damaligen Anbieter über die Vorgehensweisen informiert und festgestellt, dass eine anonyme Beratung gewährleistet war. Zu Beginn des Jahres wechselte der Anbieter. Kurz darauf erhielten wir Beschwerden über mangelhafte Datensicherheit und die Aufforderung an eine Ratsuchende, ihre Kontaktdaten (Telefonnummer und Namen) preiszugeben. Dem gingen wir nach und führten eine Prüfung vor Ort durch.

Der Anbieter legte uns ein Datenschutzkonzept vor. Aus diesem geht eindeutig hervor, dass grundsätzlich eine anonyme Beratung angeboten werden soll. Die zum Prüfzeitpunkt angewandten Verfahren telefonischer Beratung gewährleisteten dies jedoch nur bei einfachen Beratungsvorgängen, die im Rahmen eines einmaligen Anrufs erledigt werden konnten. Für komplexere Vorgänge wurde ein Rückruf vereinbart und hierfür Name und Telefonnummer der Ratsuchenden aufgenommen.

Wir haben darauf hingewiesen, dass die Aufnahme dieser Daten nur auf ausdrücklichen Wunsch der Ratsuchenden erfolgen darf. Die UPD muss es ihnen überlassen, ob sie nach einer vereinbarten Bearbeitungszeit selbst erneut anrufen wollen – wofür sie ein Kennwort erhalten und weder Namen noch Telefonnummer angeben müssen – oder es vorziehen, zurückgerufen zu werden. Auch für diesen Weg sollte die Rückrufnummer genügen: Dass die Anrufenden die richtige Person erreicht haben, lässt sich mit dem vereinbarten Kennwort eher als durch Ansprache mit dem Namen sicherstellen. Natürlich ist auch der Wunsch, persönlich angesprochen zu werden, legitim und berechtigt, und wer als ratsuchende Person

dazu den Namen offenlegen möchte, kann dies selbstverständlich tun. Die UPD jedoch muss sich zurückhalten und darf diese Information nicht abfordern.

Wir haben die UPD aufgefordert, ihre Vorgehensweise zu ändern und deutschsprachige Personen und solche, die in einer der anderen Beratungssprachen angesprochen werden möchten, gleich zu behandeln. Die gleichen Vorkehrungen sind zu treffen, wenn die Anliegen nicht per Telefon, sondern per App übermittelt werden: Ein Rückruf zur Beratung kann als Option angeboten werden. Doch sollte stets auch der Weg eröffnet werden, dass die Ratsuchenden von sich aus anrufen, wenn sie über die App die Information erhalten, dass eine Antwort vorliegt.

Neben der persönlichen Beratung in Beratungsstellen und der Beratung per Telefon bietet die UPD auch mehrere elektronische Wege für die Kommunikation an. Hier gilt das Gleiche: Anonyme Zugangswege müssen Vorrang haben. Darüber hinaus darf die Übermittlung sensitiver gesundheitsbezogener Inhalte nur geschützt erfolgen. Die UPD bietet eine gut geeignete Online-Plattform für die Beratung an. Auf einer geschützten Webseite können Ratsuchende ihre Anliegen ohne Angabe ihres Namens einstellen und zu einem späteren Zeitpunkt die Antworten passwortgeschützt abholen. Leider konterkarierte die UPD das gute Konzept, indem sie die E-Mail-Adressen der Anfragenden abforderte, obwohl diese für die Nutzung des Angebots gar nicht erforderlich sind.

Statt der Online-Plattform stellt die UPD zudem ihre E-Mail-Beratung in den Vordergrund. Da gewöhnliche E-Mail-Nachrichten jedoch auf dem Transportweg mitgelesen und sogar verändert werden können, haben sensible medizinische Informationen in ihnen nichts verloren. Auch wenn der Gesundheitszustand einer Person nicht unmittelbar erörtert wird, so können die Beratungsinhalte dennoch Schlüsse darauf zulassen. Lediglich allgemeine Informationen zu unserem Gesundheitssystem und gesundheitsrechtlichen Fragestellungen können ohne Weiteres per E-Mail übermittelt werden.

Wir mussten feststellen, dass die UPD in ihrer E-Mail-Kommunikation über diesen Rahmen deutlich hinausgeht und haben das Unternehmen aufgefordert, ein alternatives Konzept zu erarbeiten, bei dem die Kommunikation auf ein sicheres Medium – wie die Online-Plattform – gelenkt wird, sobald sensible medizinische Fragestellungen thematisiert werden.

Bei gesundheitlicher und gesundheitsrechtlicher Beratung ist anonymen Beratungswegen der Vorrang einzuräumen, soweit das möglich ist. Ob und inwieweit die Betroffenen ihren Namen und Kontaktdaten preisgeben, muss ihnen überlassen werden.

6.5 Abfrage medizinischer Daten durch Polizei in Vermisstenfällen

Von der Kassenzahnärztlichen Vereinigung Berlin erfuhren wir, dass das Landeskriminalamt (LKA) in Vermisstenfällen mit der Aufforderung an einzelne Zahnarztpraxen herangetreten sei, Auskunft über den Zahnstatus der Betroffenen zu erteilen, um einen Abgleich des Zahnstatus der oder des Vermissten mit denen unbekannter Toter durchführen zu können. Das LKA habe sich bei diesen Auskunftsersuchen auf Ermittlungen nach dem Allgemeinen Sicherheits- und Ordnungsgesetz[182] berufen und bei verweigerten Auskünften durch die Zahnärzte darauf verwiesen, dass die Herausgabe von Daten mit Zwangsgeld nach dem Verwaltungsvollstreckungsgesetz durchgesetzt werden könne. Dadurch sei suggeriert worden, dass eine Offenbarungsverpflichtung bestünde.

Bei der zugrunde liegenden Regelung des Allgemeinen Sicherheits- und Ordnungsgesetzes handelt es sich um eine generalklauselartig ausgestaltete Befugnis der Polizei, Ermittlungen durchzuführen. Sie verweist auf die nach der Strafprozessordnung[183] geltenden Auskunftsverweigerungsrechte, die auch in den vorliegenden Fallkonstellationen bestehen.

Die in der Berufsordnung der Zahnärztekammer Berlin[184] und im Strafgesetzbuch[185] normierte zahnärztliche Pflicht zur Verschwiegenheit verpflichtet Zahnärzte, über alles, was ihnen in ihrer Eigenschaft als Zahnärztin oder Zahnarzt anvertraut und bekannt geworden ist, gegenüber Dritten Verschwiegenheit zu

182 Ermittlungen gemäß § 18 ASOG
183 § 53 Abs.1 Nr. 3 StPO
184 § 5 BO
185 § 203 StGB

wahren. Diese Pflicht zur Verschwiegenheit gilt auch gegenüber Strafverfolgungsbehörden und auch über den Tod der Patientin oder des Patienten hinaus. Eine Übermittlung an Dritte kann nur auf der Grundlage der Einwilligung der Betroffenen oder bei Vorliegen einer gesetzlichen Offenbarungsbefugnis erfolgen. Beim sog. gesetzlichen Notstand[186] kann die Schweigepflicht gebrochen werden, wenn dies zur Abwendung einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut erforderlich ist und unter Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dabei ist jedoch zu berücksichtigen, dass das Strafverfolgungs- bzw. Aufklärungsinteresse des Staates in der Regel kein höherrangiges Rechtsgut darstellt.

Wir konnten erreichen, dass die vom LKA verwendeten Schreiben nicht mehr verwendet werden und die verantwortlichen Fachdienststellen auf die Rechtslage hingewiesen wurden. Danach sind Zahnärztinnen und Zahnärzte über ihr Auskunftsverweigerungsrecht nach der Strafprozessordnung zu belehren.

6.6 Abfrage der Sozialdaten von Menschen mit Behinderung und Weiterleitung an private Dienstleister

Durch mehrere Eingaben erfuhren wir, dass ein Bezirksamt eine schriftliche Umfrage bei allen im Bezirk lebenden Menschen mit Behinderung hinsichtlich ihrer Lebenssituation durchgeführt hat. Das Landesamt für Gesundheit und Soziales (LAGeSo) übermittelte hierfür auf Anfrage 8.000 Datensätze an das Bezirksamt. Diese Sozialdaten wurden sodann auf einem Datenträger (CD) an einen privaten Dienstleister übergeben, der mit der logistischen Durchführung des Rundschreibens beauftragt wurde. Grundlage für diese Zusammenarbeit war ein von dem Dienstleister in Abstimmung mit dem Bezirksamt erstelltes Konzept, das jedoch nicht schriftlich oder vertraglich fixiert wurde.

186 § 34 StGB

Die Vorgehensweisen des LAGeSo und des Bezirksamtes waren unzulässig. Das LAGeSo hätte die Sozialdaten nur dann übermitteln dürfen, wenn eine Rechtsgrundlage oder die Einwilligung der Betroffenen vorgelegen hätte. Ersteres war nicht der Fall, da die einzige gesetzlich zugelassene Möglichkeit hierfür – eine Erforderlichkeit der Übermittlung im Rahmen eines bestimmten Vorhabens der Planung im Sozialleistungsbereich – nicht hinreichend dargelegt war. Einwilligungserklärungen der Betroffenen wurden vom LAGeSo ebenfalls nicht eingeholt. Auch das Bezirksamt hätte die Daten der Menschen mit Behinderung beim LAGeSo nicht erfragen (und damit nicht erheben) dürfen, da auch hierfür keine Rechtsgrundlage ersichtlich war. Schließlich wurde nicht beachtet, dass es sich bei den abgefragten Daten um sensitive Daten handelte, die keinesfalls – wie geschehen – unverschlüsselt hätten übermittelt werden dürfen.

Wir haben gegenüber dem LAGeSo einen datenschutzrechtlichen Mangel festgestellt. Das Landesamt hat daraufhin zugesagt, uns zukünftig vor einer ähnlichen Datenübermittlung einzubeziehen.

Auch die Erhebung der Sozialdaten durch das Bezirksamt war rechtswidrig. Eine im Verantwortungsbereich des Bezirksamtes liegende gesetzliche Aufgabe, für deren Erfüllung die Kenntnis der Sozialdaten erforderlich gewesen wäre, war nicht ersichtlich. Gleichsam unrechtmäßig war die Weitergabe der Sozialdaten durch das Bezirksamt an den privaten Dienstleister. Auch hier lagen weder eine gesetzliche Grundlage noch Einwilligungen der Betroffenen vor. Die weitere Verarbeitung der Daten durch den privaten Dienstleister war ebenfalls unzulässig. Für eine Auftragsdatenverarbeitung fehlte es an einer schriftlichen Vereinbarung. Dies verstieß gegen das gesetzliche Schriftformerfordernis und unterlief die im Auftragsverhältnis vorgesehenen Kontrollmaßnahmen durch den Auftraggeber.

Aufgrund dieser Vielzahl von Verstößen gegen sozialdatenschutzrechtliche Vorschriften wurde das Vorgehen des Bezirksamtes von uns beanstandet.

Die Übermittlung von Sozialdaten zwecks Durchführung einer Befragung über die Lebenssituation einer bestimmten Bevölkerungsgruppe bedarf einer expliziten Rechtsgrundlage oder der Einwilligung der Betroffenen. Dritte (private) Stellen dürfen in eine Datenverarbeitung nur aufgrund einer adäquaten vertraglichen Vereinbarung einbezogen werden.

6.7 Keine Anforderung medizinischer Unterlagen für Schwerbehinderungs-Parkausweis

Die Vordrucke für die Beantragung von Parkerleichterungskarten für schwerbehinderte Menschen eines Bezirksamtes erweckten den Eindruck, Betroffene müssten einer Übermittlung von medizinischen Unterlagen an die Straßenverkehrsbehörde zustimmen. Die in den Antragsformularen enthaltene Einwilligungserklärung umfasste insoweit die „Übersendung einer Bescheinigung über die geprüften/festgestellten Gesundheitsschädigungen bzw. Funktionsbeeinträchtigungen". Zudem verlangte das Bezirksamt die Übersendung einer Kopie des letzten Bescheids des Versorgungsamtes.

Wir haben das Bezirksamt um Erläuterung gebeten, aus welchem Grund zum Nachweis der körperlichen Einschränkungen nicht weniger in das Recht auf informationelle Selbstbestimmung der Betroffenen eingreifende Maßnahmen ergriffen würden. Ausreichend wäre z. B. eine einfache Bescheinigung des Versorgungsamtes über den medizinischen Zustand gewesen. Das Bezirksamt teilte uns mit, es sei lediglich ein Nachweis der eine Behinderung feststellenden Merkzeichen erforderlich. Medizinische Diagnosen o. Ä. seien für den Antrag auf Erteilung einer Parkerleichterungskarte nicht mitzuteilen. Wir haben dem Bezirksamt aufgegeben, bei der Anforderung von Unterlagen – insbesondere bei solchen mit medizinischem Bezug – auf die Möglichkeit hinzuweisen, dass Schwärzungen in den zu übermittelnden Bescheiden vorgenommen werden können. Das Bezirksamt hat die infrage stehenden Vordrucke dementsprechend angepasst.

Medizinische Unterlagen können bis auf die für die Beantragung einer Parkerleichterungskarte erforderlichen Merkzeichen geschwärzt werden. Hierauf wird nun in den Vordrucken hingewiesen.

7 Beschäftigtendatenschutz

7.1 Online-Bewerbungsplattform mit Datenverarbeitung auf US-amerikanischen Servern

Ein Unternehmen nutzte für das Bewerbungsmanagement eine sog. Recruiting-Plattform,[187] die von einem Unternehmen mit Sitz in den USA betrieben wird. Die gesamte Datenverarbeitung fand auf Servern in den USA statt. Die Datenübermittlung wurde dabei hauptsächlich auf ein vorher erteiltes Einverständnis der Bewerberinnen und Bewerber gestützt. Daneben berief sich das Unternehmen auf die Erforderlichkeit der Datenübermittlung und damit auf eine Rechtsgrundlage.[188] Für die Zukunft sei ein starkes Wachstum des Unternehmens abzusehen. Zur Vereinheitlichung der Bewerbungsverfahren innerhalb des Konzerns werde daher eine Recruiting-Plattform benötigt, die ausreichend leistungsfähig und variabel einsetzbar sei.

Die Datenübermittlung konnte nicht auf eine Einwilligung gestützt werden.[189] Denn eine Einwilligung ist nur wirksam, wenn sie freiwillig erfolgt. Hier hingegen war die Einwilligung für das Bewerbungsverfahren zwingend vorgesehen und damit unfreiwillig, da Bewerbungen andernfalls nicht berücksichtigt wurden. Gerade im Bewerbungsverfahren ist von einer strukturellen Unterlegenheit der Bewerberinnen und Bewerber gegenüber der Beschäftigungsstelle auszugehen.[190]

Auch konnte die Erhebung und Nutzung von Bewerberdaten nicht auf das Bundesdatenschutzgesetz gestützt werden.[191] Dieses Gesetz knüpft die Rechtmäßigkeit der Verarbeitung von Beschäftigtendaten an deren Erforderlichkeit für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses.

187 Programm zur Auswahl von Bewerberinnen und Bewerbern
188 § 32 Abs. 1 Bundesdatenschutzgesetz (BDSG)
189 § 4a BDSG
190 BVerfG, Beschluss vom 23. November 2006 – BvR 1909/06
191 § 32 Abs. 1 BDSG

Das Prinzip der Erforderlichkeit dient der Abwägung der beiderseitigen Rechtspositionen mit dem Ziel, sie im Wege eines angemessenen Ausgleichs miteinander in Einklang zu bringen. Das bedeutet in diesem Fall, dass die Verarbeitung von personenbezogenen Daten der Beschäftigten geeignet und das relativ mildeste Mittel sein muss, um den Interessen der Beschäftigungsstelle bei der Begründung, Durchführung oder Beendigung von Beschäftigungsverhältnissen Rechnung zu tragen. Das grundsätzlich nachvollziehbare Interesse von Unternehmen an einer konzernweiten Personalpolitik legitimiert jedoch nicht automatisch eine Übermittlung von Personaldaten an Dritte. Zu berücksichtigen sind vielmehr die Risiken einer Datenverarbeitung auf Servern in den USA sowie der Umstand, dass in Bewerbungsschreiben nicht selten besonders schützenswerte sensitive Daten[192] enthalten sind.

Eine Möglichkeit zur rechtmäßigen Datenübermittlung ist der Abschluss einer Betriebsvereinbarung. Damit gäbe es eine Rechtsvorschrift im Sinne des Bundesdatenschutzgesetzes,[193] einer Einwilligung bedürfte es dann nicht mehr. Diese müsste allerdings gleichartige Schutzvorkehrungen aufweisen wie das Bundesdatenschutzgesetz selbst. So müssten beispielsweise die Betroffenen das Recht erhalten, alle in Frage kommenden Ansprüche (Auskunfts- und Schadensersatzansprüche wegen Datenschutzverstößen) auch direkt gegenüber der Beschäftigungsstelle geltend zu machen. Zusätzlich ist die datenverarbeitende Stelle – ähnlich wie ein Auftragnehmer[194] – durch eine Datenschutzvereinbarung zu verpflichten und zu kontrollieren. Die Kontrollen sind von der verantwortlichen Stelle zu veranlassen und von ihr selbst oder durch von ihr beauftragte Unternehmen in den USA durchzuführen. Durch diese zusätzlichen Sicherungsmaßnahmen wäre gewährleistet, dass die schutzwürdigen Interessen der Beschäftigten nicht verletzt werden.

Datenübermittlungen in die USA bedürfen besonderer Schutzvorkehrungen in Betriebs- bzw. Datenschutzvereinbarungen.

192 § 3 Abs. 9 BDSG
193 § 4 Abs. 1 BDSG
194 § 11 BDSG

7.2 Nutzung von Skype im Bewerbungsverfahren

Die behördliche Datenschutzbeauftragte des Bezirksamts Friedrichshain-Kreuzberg teilte uns mit, dass die Personalverwaltung prüfe, ob für bestimmte Bewerbungsverfahren die Nutzung von Skype mit Ton- und Bildübertragung während des Vorstellungsgesprächs ermöglicht werden kann. Insbesondere im ärztlichen Bereich gebe es häufig Bewerbungen aus dem „fernen" Ausland. Die Anreise für ein Vorstellungsgespräch sei kostspielig und zeitaufwendig.

Personenbezogene Daten über Bewerberinnen und Bewerber dürfen nur erhoben, verarbeitet oder genutzt werden, wenn dies zur Begründung des Beschäftigungsverhältnisses erforderlich ist.[195]

Dabei hat sich die Erforderlichkeit an den berechtigten Interessen der Beschäftigungsstelle und an den schutzwürdigen Belangen der Bewerberinnen und Bewerber zu orientieren. In objektiver Hinsicht muss daher der Einsatz von Skype unbedingt geboten sein, um überhaupt die entsprechende Stelle besetzen zu können. Dies dürfte regelmäßig nicht der Fall sein. Wünschen die Betroffenen selbst die Nutzung von Skype, wird zwar grundsätzlich von einer Freiwilligkeit[196] auszugehen sein. Allerdings sind nach beiden Vorschriften die Betroffenen über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten sowie den Zweck der Übermittlung.

Nach den Nutzungsbedingungen von Skype werden Chat-Protokolle auf den Servern von Microsoft in den USA bis zu 90 Tage zwischengespeichert. Es findet demnach eine Datenübermittlung dorthin statt.

Nach den entsprechenden Datenschutzbestimmungen von Microsoft erhebt, verarbeitet und nutzt auch Microsoft personenbezogene Daten (Kommunikationsnutzerdaten). Also kann auch Microsoft ebenso auf die Daten der Nutzerinnen und Nutzer von Skype zugreifen, diese offenlegen und aufbewahren.

195 § 2 Abs. 2 BlnDSG i. V. m. § 32 Abs. 1 BDSG
196 § 6 Abs. 3 – 6 BlnDSG sowie § 4a Abs. 1 BDSG

Die Datenerhebungen, -übermittlungen und -nutzungen sind nicht erforderlich. Sie können auch nicht auf eine Einwilligung gestützt werden. Denn selbst wenn auf Bewerberseite alle Datenerhebungen und -flüsse von einer Einwilligung gedeckt wären, bliebe das Datenschutzproblem hinsichtlich der Beschäftigten im Auswahlgremium. Hier ist ein Unterstellen der Freiwilligkeit in Bezug auf die Datenübertragung nicht möglich.

Wir haben dem Bezirksamt Friedrichshain-Kreuzberg empfohlen, von der Nutzung von Skype in Bewerbungsverfahren abzusehen.

7.3 Videounterstützte Befragungen im Rahmen von Einstellungsverfahren

Ein Unternehmen ließ aufgrund einer Vereinbarung über die Datenverarbeitung im Auftrag Videointerviews für die Personalauswahl durchführen. Gegenstand dieser Vereinbarung waren die Bereitstellung und Pflege einer Software durch die Auftragnehmer zur Durchführung von zeitversetzten Videointerviews für Personalauswahlprozesse.

Auch Videointerviews im Rahmen von Einstellungsverfahren sind unzulässig. Daten sich bewerbender Personen dürfen nur für Zwecke des Bewerbungsverfahrens erhoben, verarbeitet oder genutzt werden, wenn dies für die Begründung des Beschäftigungsverhältnisses erforderlich ist.[197]

Das Gebot der Erforderlichkeit resultiert dabei auch aus der Verfassung, die den Schutz des Grundrechts der Beschäftigten auf informationelle Selbstbestimmung gewährleisten soll.[198] Insoweit sind nur Verarbeitungen erlaubt, die für das Arbeitsverhältnis geboten und nicht nur nützlich sind. Ein Erfordernis besteht daher nicht, wenn von mehreren gleichsam geeigneten und wirksamen Maßnahmen diejenige gewählt wird, die in die Rechte der Beschäftigten tiefer eingreift.

197 § 32 Abs. 1 i. V. m. § 3 Abs. 11 Nr. 7 BDSG

198 Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG)

Die zusätzliche Erhebung und Nutzung von Bild- und Tonaufzeichnungen der Bewerberinnen und Bewerber stellt einen wesentlich intensiveren Eingriff in deren informationelles Selbstbestimmungsrecht dar als die übliche Beantwortung von Fragebögen o. Ä. In diesem Zusammenhang ist auch auf das Gebot der Datensparsamkeit hinzuweisen.[199] Weshalb die Nutzung videogestützter Befragungen von Bewerberinnen und Bewerbern für die Begründung eines Beschäftigungsverhältnisses mit dem Unternehmen erforderlich sein soll, war weder ersichtlich noch wurde es dargelegt.

Eine videogestützte Befragung bzw. eine zeitversetzte Auswertung der Videointerviews für eine Bewerberauswahl ist in keiner Hinsicht notwendig. Derartige Videointerviews sind rechtswidrig.

7.4 Angabe zur Verdiensthöhe bei Anmeldung einer Nebentätigkeit

Von einem Beschäftigten eines Krankenhauses erhielten wir die Anfrage, ob ein Formular für die Beantragung einer Nebentätigkeit die Frage nach dem Stundenlohn enthalten darf.

Bei Beamtinnen und Beamten im Landesdienst besteht eine Antragspflicht bei genehmigungspflichtigen (entgeltlichen) Nebentätigkeiten.[200] Dabei hat die Beamtin oder der Beamte die für die Entscheidung erforderlichen Nachweise zu führen, insbesondere in Bezug auf Art und Umfang der Nebentätigkeit sowie die Entgelte und geldwerten Vorteile hieraus.[201]

Für die Tarifbeschäftigten im Öffentlichen Dienst ist die Ausübung von Nebentätigkeiten weitgehend einheitlich, jedoch in verschiedenen tariflichen Normen geregelt. Welcher Tarifvertrag dabei als Grundlage herangezogen werden kann, richtet sich nach der Verbandszugehörigkeit der jeweiligen Beschäftigungsstelle.

199 § 3a BDSG
200 § 62 Landesbeamtengesetz (LBG)
201 § 62 Abs. 5 LBG

Nach dem Tarifvertrag für den Öffentlichen Dienst der Länder[202] ist die Nebentätigkeit der Beschäftigungsstelle vorher schriftlich anzuzeigen, sofern sie entgeltlich ausgeübt wird. Eine Angabe zur Höhe des Entgelts wird nicht mehr gefordert. Besonderheiten bestehen allerdings bei Teilzeitbeschäftigten. Dort stehen Nebentätigkeiten unter Genehmigungsvorbehalt, da je nach Zeit und Umfang der Nebentätigkeit dienstliche bzw. arbeitsvertragliche Interessen der Beschäftigungsstelle tangiert sein können.

Die Angabe des Entgelts könnte aber auch dann relevant und erforderlich sein, wenn es sich bei der Nebentätigkeit um ein Arbeitsverhältnis handelt, da die Betroffenen in diesem Fall von der Beschäftigungsstelle in der Sozialversicherung als mehrfach beschäftigt zu melden sind. Zur Ermittlung der konkreten Sozialversicherungsbeiträge bräuchte die Personalstelle dann u. a. die vereinbarte Arbeitszeit und die Höhe des sozialversicherungspflichtigen Entgelts aus der Nebentätigkeit.

Im Gegensatz zu Beamtinnen und Beamten sind Tarifbeschäftigte grundsätzlich nicht zur Auskunft über die Höhe des Entgelts für eine Nebentätigkeit verpflichtet. Im Einzelfall kann eine Auskunftspflicht jedoch auch bei Tarifbeschäftigten bestehen.

7.5 Vorlage amtsärztlicher Untersuchungsbefunde an die Dienstbehörde

Eine Beamtin kritisierte ein amtsärztliches Gutachten zu ihrer Dienstunfähigkeit im Rahmen einer amtsärztlichen Untersuchung. Das Gutachten enthielt die Diagnosen zu einer psychischen Erkrankung. Die Beamtin beschwerte sich auch über den Untersuchungsauftrag, der die Frage enthielt, welche ärztlichen Diagnosen den ärztlichen bzw. medizinischen Feststellungen zugrunde liegen. Sie hielt sowohl diese Frage als auch die Nennung von Diagnosedaten im amtsärztlichen Gutachten für rechtswidrig.

202 § 3 Abs. 4 TV-L

Die Frage nach ärztlichen Diagnosen darf von der Dienststelle nur in Einzelfällen, nach entsprechender Anforderung und nur soweit dies für die zu treffende Entscheidung erforderlich ist, gestellt und vom ärztlichen Personal beantwortet werden.[203] Kommt die Ärztin oder der Arzt zu dem Ergebnis, dass weiterhin Dienstfähigkeit bei den Betroffenen besteht, dürfen nur etwaige Funktionseinschränkungen mitgeteilt werden. Diagnosedaten sind dagegen regelmäßig nicht erforderlich. Diese Frage wird erst dann relevant, wenn das begutachtende Personal im ärztlichen Dienst feststellt, dass aus medizinischer Sicht eine Dienstunfähigkeit vorliegt.[204] Erst in diesem Fall sind Diagnosedaten (aber nur im erforderlichen Umfang) der Dienststelle mitzuteilen, damit diese konkret begründen kann, weswegen die oder der Betroffene in den Ruhestand versetzt wird. Dabei kann die Nennung von Diagnosedaten erforderlich sein, um die Betroffenen in die Lage zu versetzen, gegen den Bescheid ggf. rechtlich vorzugehen. Voraussetzung dafür ist, dass die Betroffenen wissen, auf welchen Diagnosen die Versetzung in den Ruhestand beruht.

Bei der Frage, ob der amtsärztliche Dienst Diagnosen mitteilen darf, ist stets auf den Einzelfall abzustellen.

7.6 Offenbarung von Diagnosedaten vor Anordnung einer amtsärztlichen Untersuchung

Aus der Praxis

Ein Petent beschwerte sich darüber, dass er von seinem Dienstherrn ein Schreiben erhalten habe mit der Aufforderung, die seinen Fehlzeiten zugrunde liegenden Erkrankungen mitzuteilen. Begründet wurde dies damit, dass der Untersuchungsauftrag an den Amtsarzt auf den notwendigen Umfang beschränkt werden solle und dafür diese Angaben erforderlich seien. Nach dem Grundsatz der Verhältnismäßigkeit sei er zur entsprechenden Auskunft verpflichtet.

Beamtinnen und Beamte sind verpflichtet, sich nach Weisung der Dienststelle durch einen von dieser bestimmten Person im ärztlichen Dienst untersuchen zu

203 § 45 Abs. 1 LBG

204 § 26 Beamtenstatusgesetz bzw. § 39 LBG

lassen, wenn Zweifel an der Dienstfähigkeit bestehen und dies für erforderlich gehalten wird.[205] Voraussetzung ist jedoch eine Untersuchungsaufforderung, die aus Gründen der Verhältnismäßigkeit sowohl inhaltliche als auch formelle Anforderungen erfüllen muss. So muss sie insbesondere Angaben zu Ort und Umfang der ärztlichen Untersuchung enthalten, was nicht im Belieben des ärztlichen Fachpersonals steht. [206]

Dementsprechend muss sich der Dienstherr bereits im Vorfeld der Untersuchungsaufforderung nach entsprechender sachkundiger ärztlicher Beratung zumindest in den Grundzügen darüber klar werden, in welcher Hinsicht Zweifel am körperlichen Zustand oder der Gesundheit der Beamtin oder des Beamten bestehen und welche ärztlichen Untersuchungen zur endgültigen Klärung geboten sind. Dabei ist dem Dienstherrn keineswegs untersagt, entsprechende Fragen an die Bediensteten zur Ursache der Erkrankungszeiten zu stellen. Das Landesbeamtengesetz[207] steht derartigen Fragen nicht entgegen.

Ein Recht des Dienstherrn auf Anforderung von Diagnosedaten oder auf Herausgabe der Krankenakte besteht dagegen nicht.

Der Dienstherr kann Betroffene im Rahmen der Anordnung einer amtsärztlichen Untersuchung in Einzelfällen auch nach den Ursachen ihrer Erkrankung fragen.

205 § 39 Abs. 1 Satz 2 LBG
206 Verwaltungsgericht Berlin, Beschluss vom 4. Dezember 2014 – 26 L 301.14
207 § 84 Abs. 1 Satz 1 LBG

8 Wirtschaft

8.1 Start-ups

Aus der Praxis

Berlin ist in den letzten Jahren als „Start-up-City" in aller Munde. Der Presse war sogar zu entnehmen, dass Londoner Start-ups nach dem Brexit-Votum per Werbung aufgefordert wurden, nach Berlin umzuziehen![208] Es wird geschrieben, getwittert und gepostet, dass Berlins Start-up-Ökosystem rasant wächst, Gründerinnen und Gründer aus anderen Ländern sich in Berlin niederlassen und ein großer Anteil des investierten Risikokapitals hierhin fließt.

Der „Deutsche Startup Monitor (DSM)"[209] aus dem Jahre 2015 definiert Start-ups als Unternehmen, die jünger sind als zehn Jahre, mit ihrer Technologie und/oder ihrem Geschäftsmodell (hoch) innovativ sind und ein signifikantes Beschäftigten- und/oder Umsatzwachstum haben bzw. anstreben. Weiter zeichnen sich Start-ups nach den Darstellungen in der Literatur dadurch aus, dass Produkte und Geschäftsmodelle stetig angepasst und weiterentwickelt werden.[210] Das „Fehlermachen" ist dabei Teil des Prozesses und produziert als „Gewinn" Daten, die genutzt werden, um die Geschäftsidee für das Nutzungsbedürfnis zu optimieren. Instrumente für dieses agile und experimentierende Vorgehen sind häufig datenschutzinvasive Methoden, z. B. Big-Data-Analysen. Konflikte mit Datenschutzgrundsätzen, wie etwa der Vorhersehbarkeit, Zweckbestimmung, Erforderlichkeit und Datensparsamkeit, scheinen dabei vorprogrammiert. Vor diesem Hintergrund ist es nicht verwunderlich, dass Datenschutzvorschriften bei Umfragen unter Gründerinnen und Gründern zum Teil als Hemmnis wahrgenommen werden. Zugleich besteht bei ihnen nach unseren Erfahrungen aber

208 Süddeutsche Zeitung vom 21. Juli 2016, S. 16

209 Jährliche Onlinebefragung der Start-ups in Deutschland, initiiert durch den Bundesverband Deutscher Startups e. V., abrufbar unter www.deutscherstartupmonitor.de

210 Richter/Schildhauer, Innovation, Gründungskultur und Start-ups Made in Germany, 15. April 2016, Bundeszentrale für politische Bildung, APUZ 16-17/2016

auch durchaus das Bedürfnis, den Datenschutz zu beachten – nicht selten aus Überzeugung oder aufgrund der Anforderungen, die von großen Unternehmen, mit denen sie kooperieren wollen, an sie gestellt werden.

Bei Beratungen von Start-up-Unternehmen stellen wir regelmäßig fest, dass es sinnvoll ist, die Gründerinnen und Gründer frühzeitig mit den rechtlichen Rahmenbedingungen ihres Schaffens vertraut zu machen. In der Anfangsphase besteht größerer Spielraum, Ideen und Geschäftsmodelle datenschutzkonform zu gestalten, sodass die Datenschutzvorgaben auch bei der Fortentwicklung der Produkte beachtet werden. Typische Beratungsthemen sind etwa Hilfestellungen zum Verständnis des Personenbezugs von Daten, z. B. im Zusammenhang mit gerätebezogenen Daten wie etwa MAC-Adressen. Darüber hinaus sind der Einsatz von Instrumenten für die Nutzungsverfolgung (Tracking) und Profilerstellung konkrete Themen. Häufig stellt sich schlicht die Frage, welche Infrastrukturen zur Speicherung von personenbezogenen Daten genutzt werden können. Insbesondere bei der Nutzung von Cloud-Diensten ist zu beachten, dass Auftragsdatenverarbeitungsverträge zu schließen sind. Darüber hinaus führt der Standort des Cloud-Servers im Drittstaat bzw. die Nutzung von Analyseprogrammen, die von Anbietern mit Sitz im Drittstaat zur Verfügung gestellt werden, dazu, dass die Start-ups sich auch mit Fragen des Drittstaatentransfers auseinandersetzen und die datenschutzkonforme Übermittlung von Daten an Stellen außerhalb der Europäischen Union sicherstellen müssen.

Um die Start-up-Szene in Berlin zu unterstützen, beabsichtigen wir, das Beratungsangebot für Start-ups in Berlin auszubauen. Deshalb werden wir ab März 2017 zweimal monatlich eine Start-up-Sprechstunde anbieten. Zu dieser Sprechstunde können die Gründerinnen und Gründer auch ohne Termin kommen und dann ggf. weitere Beratungen mit uns vereinbaren.

Wir empfehlen den Start-ups, Berührungsängste mit dem Datenschutz abzubauen und sich von uns beraten zu lassen. Wer frühzeitig kommt, spart sich möglicherweise aufwendige oder kostenintensive nachträgliche Anpassungen von Systemen zur Verarbeitung personenbezogener Daten, die in der Anfangsphase leicht umzusetzen gewesen wären.

8.2 „Best-Practice“ bei Apps

Unter diesem Stichwort hatte das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) verschiedene Interessenvertretungen, u. a. App-Entwickler, Smartphone-Betriebssystemhersteller, App-Store-Betreiber, Verbraucherschützerinnen und Verbraucherschützer sowie Datenschützerinnen und Datenschützer, zu Gesprächen geladen. Ziel der Gespräche sollte es sein, einen sog. Best-Practice-Leitfaden für Apps zu erstellen, also freiwillige Qualitäts-Standards zu definieren.

Diese Runde traf sich mehrfach und versuchte sich über die drei Themenblöcke „Transparenz“, „Selbstbestimmung und Wahlfreiheit“ sowie „verbraucherfreundliche Bedingungen“ dem Thema anzunähern und zu gemeinsamen Standpunkten zu gelangen.

Im Bereich der Transparenz wurde vor allen Dingen der sog. One-Pager diskutiert. Dabei handelt es sich um ein Muster für Datenschutzhinweise, das im Rahmen des Nationalen IT-Gipfels 2015 vom BMJV vorgestellt worden war. Der One-Pager zeichnet sich dadurch aus, dass die wesentlichen Aussagen zur Datenverarbeitung auf einer Seite zusammengefasst werden und die Nutzerinnen und Nutzer bei Bedarf weitere Details aufrufen können. Dies erhöht die Wahrscheinlichkeit, dass die Datenschutzhinweise auch tatsächlich zur Kenntnis genommen werden, da man nicht mehr, wie derzeit üblich, in seitenlangen kleingedruckten Ausführungen zu allen nur denkbaren Fällen versinkt. Ein solcher mehrstufiger Ansatz für die Aufbereitung von Informationen wird von uns grundsätzlich unterstützt und bietet sich insbesondere im Bereich der Apps an, wo die limitierte Größe der Smartphone-Displays mitunter die vollständige Anzeige aller relevanten Informationen erschwert. Primär kommt es dabei auf die Ausgestaltung des Konzepts an, also z. B. auf die Auswahl derjenigen Informationen, die für wesentlich gehalten werden und die auf der ersten Stufe erscheinen sollen, sowie auf die Gestaltung der Weiterleitung der Nutzenden auf die jeweils relevanten Passagen in der vollständigen Datenschutzerklärung.

Im Bereich der Selbstbestimmung und Wahlfreiheit drehte sich die Diskussion vor allem um die Frage, wie die Nutzerinnen und Nutzer verbesserte Möglichkeiten

erhalten können, auf die von den Apps verlangten Zugriffsberechtigungen einzuwirken. Darüber hinaus wurden auch die Nutzung und Übermittlung von personenbezogenen Daten (insbesondere auch MAC-Adresse, Werbe-IDs oder sonstige Geräteidentifizierungsnummern) an Dritte im Rahmen der Teilnahme an Werbenetzwerken erörtert.

Im dritten Themenblock fokussierte sich die Diskussion auf die Frage, ob und wie das Angebotsmanagement im App-Store aus Sicht des Verbraucher- und Datenschutzes verbessert werden kann und welche Rolle die App-Store-Betreiber dabei spielen.

Der Düsseldorfer Kreis hatte bereits im Juni 2014 eine Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter[211] herausgegeben, die von den Datenschutzaufsichtsbehörden in die Diskussionsrunde eingebracht wurde.

Die Gespräche dauern noch an. Die bisherigen Ergebnisse zeigen, dass die typischen Meinungsverschiedenheiten zwischen der Wirtschaft und den Datenschutzaufsichtsbehörden zu Fragen des Personenbezugs von Daten, der Freiwilligkeit einer Einwilligung, der Koppelung der Einwilligung mit Vertragsschlüssen, der Verantwortlichkeiten für die Datenübermittlungen im Rahmen von Werbenetzwerken sowie der Herstellung von Transparenz über die Übermittlung zu Werbezwecken auch in diesen Gesprächen eine Rolle spielen. Darüber hinaus gab es Zweifel, ob die Möglichkeiten nicht eher begrenzt sind, angesichts international agierender Unternehmen, die den Markt bestimmen, und solcher Akteure, die keine Niederlassung in Europa haben, rein nationale freiwillige Qualitäts-Standards aufzustellen. Es bleibt zu hoffen, dass trotz der unterschiedlichen Perspektiven und Ansätze in bestimmten Fragen dennoch ein Konsens hergestellt werden kann.

211 Veröffentlicht unter https://datenschutz-berlin.de/content/service/orientierungshilfen-merkblaetter

8.3 Zahlartensteuerung

Aus der Praxis

Um die Ausfallrisiken riskanter Zahlungsmethoden, insbesondere beim Kauf auf Rechnung, zu minimieren, bedienen sich immer mehr Unternehmen im Online-Handel einer sog. aktiven Zahlartensteuerung. Dabei wird abhängig von der jeweiligen Bonitätsbewertung eine Vorabauswahl der Zahlungsarten vorgenommen, die Kundinnen und Kunden bei der Online-Bestellung angeboten werden.

Hierfür erfolgt während des Bestellvorgangs nach Eingabe der Kundendaten eine unmittelbare Bonitätsprüfung bei einer oder mehreren Auskunfteien. Das Ergebnis der Prüfung entscheidet darüber, ob den Betroffenen wirtschaftlich riskante Zahlungsmethoden, wie z. B. der Kauf auf Rechnung oder Ratenzahlung, überhaupt im weiteren Bestellvorgang angezeigt werden.

Eine Bonitätsabfrage bei einer Bestellung ist nur zulässig, soweit diese erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen überwiegen.[212]

Die Notwendigkeit einer Bonitätsabfrage kann nur bestehen, wenn ein sog. kreditorisches Risiko für das Unternehmen vorliegt. Ein solches kann allerdings noch nicht vor der Auswahl der Zahlungsart bestehen. Den Kundinnen und Kunden eine geeignete Zahlungsmöglichkeit anzubieten und ihr bzw. ihm eine Enttäuschung zu ersparen, stellt kein berechtigtes Interesse des Unternehmens dar. Das Verfahren der antizipierten Bonitätsabfrage vor Auswahl der Zahlart ist insbesondere dann problematisch, wenn die Kundin oder der Kunde von vornherein eine Zahlungsmethode ohne kreditorisches Risiko – wie etwa die Zahlung mit Kreditkarte – ansteuert. Denn die Anzahl der durchgeführten Abfragen kann negative Folgen für die Betroffenen haben, da die Häufigkeit der Anfragen teilweise in die Bonitätsbewertungen der Auskunfteien einbezogen wird. Damit sind schutzwürdige Interessen der Betroffenen tangiert.

Vor dem Hintergrund des Transparenzgedankens ist es empfehlenswert, Kundinnen und Kunden vor der Auswahl der Zahlungsmethode verständlich und vollstän-

212 Siehe § 28 Abs. 1 Satz 1 Nr. 2 i. V. m. § 29 Abs. 2 Satz 1 BDSG

dig darüber zu informieren, welche Zahlungswege aufgrund eines Ausfallrisikos für die Unternehmen zu einer Bonitätsabfrage führen. Diese sollten im Bestellvorgang deutlich gekennzeichnet werden (etwa durch einen aussagekräftigen Sternchen- oder Klammerhinweis). Idealerweise sollte dieser Hinweis mit einem Link zu den entsprechenden Stellen der Datenschutzerklärung verknüpft sein, aus der sich vertiefte Informationen für die Verbraucherinnen und Verbraucher ergeben.

Zur Wahrung der informationellen Selbstbestimmung müssen dabei alle Konsequenzen einer Bonitätsabfrage für die Kundschaft erkennbar sein. So ist beispielsweise das Einfließen der Bonitätsabfragen in zukünftige Bonitätsbeurteilungen allgemein transparent zu machen. Zudem müssen auch weitere potenziell negative Konsequenzen eindeutig benannt werden. Erst wenn die Kundin oder der Kunde sich nach vollständiger und transparenter Information für eine Zahlungsart mit nachgelagerter Zahlung (z. B. Kauf auf Rechnung) und damit für eine Zahlungsart mit kreditorischem Risiko entscheidet, kann eine Bonitätsabfrage als erforderlich und damit zulässig angesehen werden.

Diese Lösung haben wir mit verschiedenen Unternehmen besprochen, die eine entsprechende Umstellung ihrer Verfahren in Aussicht gestellt haben.

Eine Bonitätsabfrage im Rahmen eines Online-Bestellvorgangs ist nur dann zulässig, wenn die durch die Verbraucherin oder den Verbraucher ausgewählte Zahlungsart tatsächlich ein Ausfallrisiko mit sich bringt. Diese Zahlungsarten müssen deutlich gekennzeichnet und die Konsequenzen für die Kundinnen und Kunden ausreichend transparent gemacht werden.

8.4 Personalisierte Tickets und bargeldloses Bezahlsystem bei Festivals

Aus der Praxis

Immer mehr Festivals setzen auf bargeldloses Bezahlen durch in die Festivalbändchen integrierte RFID-Chips (d. h. Chips mit Nahfunktechnik)[213]. Die Chips verheißen kürzere Wartezeiten an Getränke- und Essensschlangen. Bei Verlust des Bandes und nach Ende des Festivals wird durch die Personalisierung gewährleistet, dass den Betroffenen das Guthaben zugewiesen werden kann.

Die Festivalgäste kaufen sich zunächst ein Ticket, erstellen sich dann einen sog. Account und aktivieren das Ticket. Das dann personalisierte Ticket wird bei Ankunft gegen ein Festivalbändchen mit integriertem RFID-Chip eingetauscht. Dabei kann das Bändchen vorab online oder bei einer Aufladestation auf dem Festivalgelände mit Geld aufgeladen werden. Auf diese Weise ist nicht ausgeschlossen, dass bereits vor dem Besuch des Festivals ein Persönlichkeitsprofil von den Gästen (Name, Anschrift, E-Mail-Adresse) erstellt wird, welches sich mit dem individuellen Ess- und Trinkverhalten (Art der Getränke und Speisen, Uhrzeit und Ort des Kaufs) verknüpfen lässt. Das in einem von uns geprüften Fall veranstaltende Unternehmen gab allerdings an, dass auch eine Aufladung vor Ort ohne vorherige Personalisierung möglich sei.

Das Unternehmen hat sich dafür entschieden, dass die Personalisierung der Tickets und damit der personalisierte Chip auf eine Einwilligung gestützt werden soll, und hierzu auf die Datenschutzbestimmungen verwiesen. Eine Einwilligung ist allerdings nur rechtmäßig, wenn diese eindeutig, klar und verständlich die Betroffenen über die Datenverarbeitung aufklärt. In den allgemeinen Geschäftsbedingungen und in den Datenschutzbestimmungen fand sich demgegenüber weder ein Hinweis auf eine mögliche Einwilligung zur Personalisierung der Tickets und der damit verbundenen Konsequenzen noch wurde eine solche Einwilligung in den Datenschutzbestimmungen textlich hervorgehoben. Die uns präsentierte Einwilligungslösung wurde daher dem Erfordernis einer informierten Einwilligung nicht

213 RFID ist eine Technik, um Daten mit Hilfe von Funkwellen berührungslos und ohne Sichtkontakt auf einem Chip lesen und speichern zu können.

gerecht. Darüber hinaus wies die eingesetzte Chiptechnik Sicherheitslücken aufgrund eines mangelhaften Verschlüsselungsalgorithmus auf.

Diese Mängel haben wir in Gesprächen mit der veranstaltenden Unternehmensgruppe thematisiert. Aufgrund unserer umfangreichen Hinweise versprach die verantwortliche Stelle, die Einwilligung zur Personalisierung im Rahmen des Onlineprozesses einzuholen und insgesamt transparenter zu gestalten.

Die Überarbeitung des Registrierungsprozesses war bisher nicht zufriedenstellend. Zwar ist nunmehr geplant, eine Einwilligung in die Personalisierung der Tickets bzw. der Chips direkt bei Aktivierung des Tickets und nicht durch versteckte Einwilligungserklärungen in den Datenschutzbestimmungen einzuholen. Allerdings ist aus der geplanten Einwilligungserklärung nicht ersichtlich, was der eigentliche Inhalt der Einwilligung sein soll. Nach wie vor werden den Betroffenen weder die Personalisierung der Tickets und die damit verbundene Zuordnung zum Chip noch die Folgen vor Augen geführt. Es wird auch nicht darauf hingewiesen, dass anstelle der Personalisierung auch eine (anonyme) Aufladung vor Ort möglich ist. Die Betroffenen müssen jedoch bei Erteilung einer Einwilligung grundsätzlich wissen, wozu sie ihr Einverständnis erteilen und was mit ihren Daten geschieht.[214]

Aufgrund unserer Hinweise und der praktischen Probleme, die sich 2015 ergeben haben, wurde im Berichtszeitraum auf den Einsatz der personalisierten Tickets sowie des bargeldlosen Bezahlsystems verzichtet.

Entscheiden sich Veranstalter für die Personalisierung von Tickets und ein damit verbundenes bargeldloses Bezahlsystem, müssen Festivalgäste umfassend, klar und verständlich informiert werden, damit sie die Tragweite ihrer Einwilligung in die Datenverarbeitung erkennen können. Zur Wahrung der Freiwilligkeit muss es eine echte Wahlmöglichkeit zwischen einem anonymen Besuch des Festivals ohne Aktivierung des Tickets oder einer Personalisierung des Tickets geben. Hierauf muss deutlich hingewiesen werden.

214 § 4 a Abs. 1 Satz 2 BDSG

8.5 Kundendaten beim Unternehmenskauf

Aus der Praxis

Kundendaten sind Gold wert. Das zeigt sich insbesondere dann, wenn sie im Rahmen von Insolvenzen an ein Nachfolgeunternehmen gewinnbringend verkauft werden. Dabei ist Vorsicht geboten. In einem der von uns überprüften Fälle war die Übermittlung sehr problematisch, da rechtlich besonders geschützte, nämlich sensitive Daten betroffen waren.[215]

Sofern keine sensitiven Daten betroffen sind, können Namen und Postanschriften von Kundinnen und Kunden[216] grundsätzlich auch ohne Einwilligung der Betroffenen übermittelt (und genutzt) werden, wenn das veräußernde Unternehmen die Übermittlung dokumentiert hat. Bei den übrigen Daten ist eine Weitergabe nur zulässig, wenn die betreffenden Kundinnen und Kunden in die Übermittlung solcher Daten eingewilligt haben oder auf die geplante Übermittlung hingewiesen worden sind, ihnen ein Widerspruchsrecht eingeräumt wurde und sie nicht widersprochen haben. Eine nachträgliche Information der Kundschaft genügt nicht.

Ein Sonderproblem stellt jedoch die Übermittlung von E-Mail-Adressen und Telefonnummern dar. Wenn diese Daten vom erwerbenden Unternehmen für eigene Werbezwecke genutzt werden sollen, ist dies im Ergebnis selbst bei Befolgung der Widerspruchslösung nicht möglich. Dies hat seinen Grund im Wettbewerbsrecht,[217] das die Telefon- und E-Mail-Werbung nur mit ausdrücklicher Einwilligung für zulässig erachtet. Eine gegenüber dem Alt-Unternehmen erteilte Einwilligung zur E-Mail-Werbung geht nicht auf das erwerbende Unternehmen über. Anders ist es bei Kundinnen und Kunden, die zwischenzeitlich einen Vertrag mit dem erwerbenden Unternehmen eingegangen sind: Gegenüber dieser Kundschaft darf das erwerbende Unternehmen unter den Voraussetzungen des Wettbewerbsrechts[218] E-Mail-Werbung versenden.

215 § 3 Abs. 9 BDSG
216 Sog. Listendaten
217 § 7 Abs. 2 Nr. 2 und Nr. 3 UWG
218 § 7 Abs. 3 UWG

Im Falle der Übertragung sensitiver Daten ist der Übergang bestehender Vertragsverhältnisse und offener Forderungen zulässig, da dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen überwiegen.[219] Werden sensitive Daten von Kundinnen und Kunden über diesen Zweck hinaus z. B. für Werbung übertragen, bedarf es hierfür allerdings einer ausdrücklichen Einwilligung.[220] Eine solche ist selbst bei postalischer Werbung erforderlich.

Eine Übermittlung aller bisherigen Bestelldaten (sog. Bestellhistorie) mit Ausnahme der aktuellen Vertragsverhältnisse ist im Regelfall nicht erforderlich.

Bei der Übertragung von Daten der Kundschaft beim Unternehmenskauf ist Vorsicht geboten. Um rechtssicher vorzugehen, sollte für die geplante Nutzung für Werbung eine ausdrückliche Einwilligung durch das erwerbende Unternehmen bzw. durch die Insolvenzverwaltung eingeholt werden. Generell sollte der Kundschaft transparent dargelegt werden, welche Daten zu welchen Zwecken übermittelt werden.

8.6 Spam-E-Mails

Seit vielen Jahren erreichen uns Beschwerden über Unternehmen, die mit massenhafter E-Mail-Werbung versuchen, neue Kundschaft zu gewinnen. Dabei geben die Unternehmen oft an, diese E-Mail-Adresse der Kundinnen und Kunden über ein Internet-Gewinnspiel erhalten zu haben, bei dem diese eine Werbeeinwilligung erteilt haben sollen.

Ein neues Phänomen ist die sog. Adressmiete. Im (europäischen) Ausland ansässige Firmen bieten ein Komplettpaket aus Adressgenerierung, Werbefläche zur Miete sowie Versand der Werbe-E-Mails. Unternehmen, die für sich werben wollen, stellen nur die Inhalte für die Werbeflächen zur Verfügung und erheben, ver-

219 § 28 Abs. 6 Nr. 3 BDSG

220 Nach Maßgabe des § 4 a Abs. 3 BDSG

arbeiten oder nutzen selbst keine personenbezogenen Daten der Betroffenen. In den Newslettern tritt nicht das Unternehmen, für das beworben wird, als verantwortliche Stelle auf, sondern das sog. adressvermietende Unternehmen.

Die Erhebung von personenbezogenen Daten für Zwecke der E-Mail-Werbung bedarf grundsätzlich einer Einwilligung der Betroffenen, da ansonsten (wettbewerbsrechtlich) von einer unzumutbaren Belästigung der E-Mail-Empfangenden auszugehen ist.[221]

Eine beliebte Quelle für derartige Einwilligungen stellen Internet-Gewinnspiele dar. Regelmäßig erhalten wir Beschwerden, dass auf Nachfrage als Herkunft der Daten auf ein ominöses Gewinnspiel verwiesen werde, bei dem die Betroffenen eine Einwilligung in die Übermittlung von Werbung erteilt haben sollen. Eine Teilnahme an dem Gewinnspiel können die Betroffenen meist ausschließen. Diese Gewinnspiele weisen zudem offensichtliche Fehler auf: So sollte z. B. monatlich ein zum Prüfzeitpunkt bereits veraltetes Navigationsgerät verlost werden. Obwohl die angebliche Gewinnspielteilnahme bereits über ein halbes Jahr zurücklag, habe es nach Aussage der Webseite bisher noch keine Auslosung gegeben.

Bei der Adressmiete wird der gesamte Versendungsvorgang von dienstleistenden Unternehmen durchgeführt. Das beworbene Unternehmen hat dabei keinen Kontakt zu personenbezogenen Daten. Kommt es zu Beschwerden der Kundschaft, soll sich diese nicht an das beworbene, sondern direkt an das dienstleistende Unternehmen wenden. In dieser Konstellation ist es für uns schwierig, ordnungsrechtliche Maßnahmen zu ergreifen, wenn die Daten im Besitz ausländischer Unternehmen sind. Die werbenden Unternehmen in unserer Zuständigkeit weisen jegliche Verantwortung von sich mit der Begründung, dass ausschließlich das beauftragte Unternehmen gehandelt habe und sie die E-Mail-Adressen nicht einmal zur Kenntnis genommen hätten. Daher könnten sie auch nicht als Auftraggeber der Datenverarbeitung zur Verantwortung gezogen werden.[222] In diesen Fällen blieb uns nur die Abgabe der Verfahren an die britische Datenschutzbehörde, in

221 § 28 Abs. 3 BDSG i. V. m. § 7 Abs. 2 Nr. 3 UWG; zu den Einzelheiten siehe Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke vom September 2014, abrufbar unter https://www.lda.bayern.de/media/ah_werbung.pdf

222 Siehe § 11 BDSG

deren Zuständigkeit die adressvermietenden Unternehmen meistenteils niedergelassen sind.

Allerdings haben die hier betroffenen werbenden Unternehmen im Zuge unseres Einschreitens ihre Verträge mit den dienstleistenden Unternehmen angepasst. Nunmehr übernehmen sie die Haftung, sollten die für Werbezwecke genutzten E-Mail-Adressen über keine ausdrückliche Einwilligung zum Erhalt von Werbung verfügen.[223] Darüber hinaus wurden weitere Zusicherungen, eine Vertragsstrafenregelung sowie ein Sonderkündigungsrecht für das beworbene Unternehmen eingeräumt.

Insgesamt ist allerdings festzustellen, dass die Werbung neuer Kundschaft durch massenhafte E-Mail-Versendung langsam nachlässt. In aller Regel erhalten wir zu jedem Unternehmen nur einmalige Beschwerden. Wiederholt wurde uns auch mitgeteilt, dass man aufgrund der nicht zufriedenstellenden Ergebnisse diese Werbeform nicht mehr einsetzen werde.

Bei der sog. Adressmiete sollen mit den dienstleistenden Unternehmen Haftungs- sowie zusätzliche Vertragsstrafen- und Sanktionsregelungen vereinbart werden für Fälle unrechtmäßiger Adressgewinnung und Nutzung von E-Mail-Adressen für Werbung ohne rechtmäßige Einwilligung.

8.7 Tele- oder Heimarbeit – was muss beachtet werden?

Die Anfragen häufen sich. Immer mehr Arbeitgeber erkundigen sich bei uns nach den Anforderungen bei Tele- oder Heimarbeit. Welche Maßnahmen müssen zum Schutz der zu verarbeitenden Daten ergriffen werden?

223 Für das elektronische Erklären einer Einwilligung ist – zur Verifizierung der Willenserklärung der oder des Betroffenen – ein zweistufiges Zustimmungsverfahren geboten, bei dem die Betroffenen ihre Anmeldung durch eine zweite E-Mail bestätigen müssen.

Bei der Telearbeit wird die Arbeit ausschließlich oder zeitweise außerhalb der Gebäude des Arbeitgebers erledigt. Es gibt verschiedene Formen der Telearbeit. Sie kann als heimbasierte Telearbeit in der Wohnung der Mitarbeiterin oder des Mitarbeiters oder auch von unterwegs erbracht werden. Im Folgenden wird der Schwerpunkt auf die heimbasierte Telearbeit gelegt.

Zur Sicherung der Telearbeit sind weitergehende Sicherheitsmaßnahmen zu ergreifen. Sie haben sich am Schutzbedarf der zu verarbeitenden Daten zu orientieren. Hinweise zur Feststellung des Schutzbedarfs werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gegeben.[224]

Wird Telearbeit im Rahmen von Dienst- oder Arbeitsverhältnissen vereinbart, handelt es sich um eine Datenverarbeitung des Dienstherrn bzw. des Arbeitgebers. Dieser bleibt weisungsbefugt und bestimmt die Art und Weise der Aufgabendurchführung. Insbesondere hat er die erforderlichen Maßnahmen zu ergreifen, um den Schutz personenbezogener Daten sicherzustellen. Grundsätzlich sollte stets vorab geprüft werden, ob eine Beschränkung auf pseudonymisierte oder anonymisierte Daten möglich ist. In diesem Fall wäre Telearbeit uneingeschränkt zulässig.

Dagegen bestehen bei der Verarbeitung besonders schutzwürdiger Informationen wie Personalaktendaten oder gar sensitiver Daten[225] besondere Risiken, die einen besonderen Schutz durch angemessene technisch-organisatorische Maßnahmen und zusätzliche Kontrollen des Arbeitgebers vor Ort erfordern. Zu den besonders schützenswerten Daten im Beschäftigungsverhältnis zählen Personalaktendaten, die dem Personalaktengeheimnis unterliegen.

Gesundheitsdaten sollten wegen ihrer besonderen Sensitivität nicht für Telearbeit zugelassen werden. Ebenso sollte auch eine Auftragsdatenverarbeitung nicht in Telearbeit erfolgen, da die Einwirkungs- und Kontrollmöglichkeiten des Arbeitgebers bzw. Dienstherrn dabei beschränkt sind.

224 Siehe BSI-Standard 100-2, Kap. 4.3

225 Sensitive Daten unterliegen einer nochmals gesteigerten Geheimhaltungspflicht und daher auch strengen gesetzlichen Vorgaben zur Erhebung und Verarbeitung. Zu diesen „besonderen Arten personenbezogener Daten" gehören z. B. politische und religiöse Überzeugungen, Gesundheit sowie Rasse und Ethnie (§ 3 Abs. 9 bzw. § 6a BDSG).

Empfehlenswert ist der Abschluss von Dienst- bzw. Betriebsvereinbarungen, in denen konkrete Festlegungen zur Geeignetheit, zu Art, Umfang und zur Durchführung von Telearbeit getroffen werden.

Grundsätzlich sollte ein abschließbares Arbeitszimmer, das ausschließlich für die Telearbeit genutzt wird, vorhanden sein. Hierzu dürfen Dritte – auch Familienmitglieder – keinen Zutritt haben. Der Einblick in dienstliche Unterlagen muss für Unberechtigte ausgeschlossen sein.

Die für die Telearbeit erforderlichen technischen Geräte und die Software sollten vom Arbeitgeber zur Verfügung gestellt und von dessen System-Administration eingerichtet werden. Hierbei muss die Konfiguration so vor Manipulationen geschützt sein, dass weder unerlaubte Software- noch Hardware-Installationen möglich sind. Dafür müssen u. a. entsprechende Benutzer- und Zugriffsrechte, eine Sicherheitssoftware sowie eine Festplattenverschlüsselung eingerichtet werden. Ein Schutz vor schadhaftem Code und der Einsatz einer Firewall sind obligatorisch. Die Technik darf ausschließlich für dienstliche Zwecke genutzt werden, damit eine problematische Vermischung von privaten und beruflichen Daten ausgeschlossen ist. Soweit nicht alle Maßnahmen technisch umgesetzt werden können, sind organisatorische Regelungen z. B. in den Dienstvereinbarungen aufzunehmen.

Da für die Datenübermittlung heutzutage regelmäßig das Internet genutzt wird, muss die Kommunikation mit der Arbeits- oder Dienststelle über eine verschlüsselte Verbindung erfolgen. Hierzu sollte eine VPN-Verbindung[226] genutzt werden. Unter den verschiedenen VPN-Technologien sollten die sicheren Protokolle wie IPSec oder OpenVPN, das auf SSL/TLS[227] aufbaut, genutzt werden. Der Einsatz von Zertifikaten, Chipkarten und/oder Hardwaretoken[228] sorgen für eine sichere Identifikation und Authentifizierung beim Arbeitgeber. Die Zertifikate sollten regelmäßig erneuert und auf Schwachstellen überprüft werden. Auch hier gibt das

226 Virtuelles privates Netzwerk

227 Secure Sockets Layer/Transport Layer Security ab Version 1.2

228 Das sind separate Komponenten, die z. B. stetig wechselnde und zeitlich begrenzt gültige Zahlenkombinationen für die einmalige Verwendung beim Aufbau einer Verbindung anzeigen.

BSI wertvolle Hinweise und veröffentlicht regelmäßig, welche Verschlüsselungsmethoden derzeit in welcher Version als hinreichend sicher angesehen werden.[229]

Die zu verarbeitenden Daten sollten ausschließlich im Netzwerk des Arbeitgebers verbleiben. Hier sind technische Entwicklungen wie Terminalserver oder die Virtualisierung von Desktops von Bedeutung. So kann ein virtueller Arbeitsplatz zur Verfügung gestellt werden, der das Arbeiten wie in der Dienststelle nachstellt. Die zu bearbeitenden Daten bleiben jedoch beim Arbeitgeber. Weiterhin kann die Nutzung eines speicherlosen Telearbeitsplatzes vorteilhaft sein, da auch hier keine dezentrale Speicherung erfolgen kann. Wenn Daten für die Verarbeitung nicht mehr notwendig sind, entfällt somit eine möglicherweise aufwendige Datenlöschung auf dem Telearbeitsplatz. Sollte jedoch eine Speicherung auf dem Telearbeitsplatz notwendig sein, muss nicht nur die Datenlöschung, sondern auch eine regelmäßige Datensicherung und deren spätere Löschung umgesetzt werden. Zusätzlich sind die Daten verschlüsselt zu speichern, damit durch einen unbefugten Zugriff der Einblick in die gespeicherten Daten wirkungsvoll verhindert wird.

Sollten zusätzlich zu den elektronischen Daten noch papiergebundene Unterlagen benötigt werden, sind entsprechende Regelungen für den Transport und die weitere Aufbewahrung außerhalb der Arbeitsstätte zu treffen. Unterlagen sollten ausschließlich in verschlossenen Behältnissen transportiert und dabei ständig beaufsichtigt werden. Für die Aufbewahrung am Telearbeitsplatz sollte ein verschließbarer Schrank zur Verfügung stehen.

Anfallende Notizen oder auch Fehlausdrucke müssen so vernichtet werden, dass eine Wiederherstellung nicht möglich ist.

Die umzusetzenden Sicherheitsmaßnahmen sind in einer Sicherheitsrichtlinie zu dokumentieren. Außerdem müssen die Pflichten der Telearbeitenden enthalten sein und in geeigneter Weise bekanntgegeben werden. Weiterhin sind entspre-

229 BSI TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen

chende Schulungen durchzuführen. Darüber hinausgehende Informationen stellt das BSI im Baustein 5.8. Telearbeit zur Verfügung.[230]

Soweit keine Rechtsgrundlagen entgegenstehen, kann bei entsprechender Ausgestaltung der Sicherheitsmaßnahmen eine datenschutzkonforme Telearbeit realisiert werden.

8.8 Datenschutzprobleme bei Online-Finanzdienstleistern

Die Finanzwirtschaft hat sich in den letzten Jahren sehr verändert. Während früher Finanzgeschäfte in Bankfilialen abgewickelt wurden, ist es inzwischen zur Normalität geworden, Bankkonten online zu eröffnen, sich mit wenigen Klicks einen Online-Kredit zu beschaffen und möglichst vorher über ein Vergleichsportal verschiedene Angebote zu prüfen. Auch gibt es Unternehmen, in denen Privatleute anderen Privatleuten Kredite zur Verfügung stellen. In den Markt drängen neben den klassischen Online-Banken immer mehr innovative sog. FinTech-Start-up-Unternehmen. Aber auch die klassischen Banken versuchen, sich den Bedürfnissen der jüngeren Kundschaft anzupassen. Durch das Fehlen eines persönlichen Kontakts entstehen neue datenschutzrechtliche Probleme.

Online-Anbieter von Finanzdienstleistungen haben sicherzustellen, dass sie den Kundinnen und Kunden sichere Kommunikationswege anbieten. So sollte etwa auf die Kommunikation mit unverschlüsselten E-Mails verzichtet werden. Die Nutzung unsicherer Kommunikationswege wird auch nicht dadurch rechtmäßig, dass die Kundinnen und Kunden hierauf hingewiesen werden, wie dies ein FinTech-Unternehmen machte.

Während in einer Bankfiliale die zur Vermeidung von Geldwäsche notwendige Identifizierung problemlos durch Vorlage des Personalausweises möglich ist, setzt sich im Online-Bereich immer mehr die Video-Identifizierung gegenüber dem auf-

230 https://www.bsi.bund.de/DEThemen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05008:html

wendigeren Post-Ident-Verfahren durch. Die Identifizierung wird meist von hierauf spezialisierten Dienstleistern als Auftragsdatenverarbeitung durchgeführt. Ein Dienstleister führte jedoch nur dann Video-Identifizierungen durch, wenn die Betroffenen darin einwilligten, dass der Dienstleister die Identifizierungsdaten bei sich als eigene Daten für weitere Identifizierungen speichern durfte. Hier haben wir durchgesetzt, dass der Kunde während des Identifizierungsverfahrens verlangen kann, dass seine Daten unverzüglich nach Beendigung des Identifizierungsprozesses gelöscht werden.

Ein FinTech-Unternehmen hat einem Kunden während des Kontoeröffnungsverfahrens mitgeteilt, er käme auf eine Warteliste. Es ließ sich nicht genau ermitteln, warum der Kunde nicht angenommen wurde. Hier wie auch bei anderen offenen Fragen des Online-Bankings zeigt sich das zusätzliche Problem, dass Kunden keine qualifizierten Ansprechpartner mehr haben. Die Hotline- oder Qualitätsmanagement-Beschäftigten sind in der Regel nicht dazu qualifiziert, datenschutzrechtliche Fragen zu beantworten, und die betrieblichen Datenschutzbeauftragten bleiben gerne „im Hintergrund".

Besondere Probleme entstehen bei datenschutzrechtlichen Einwilligungen, etwa der SCHUFA-Erklärung. Um einen Medienbruch zu vermeiden, ist es akzeptabel, dass auf das grundsätzlich geltende Schriftformerfordernis verzichtet wird. Es ist aber sicherzustellen, dass die mit dem Schriftformerfordernis verbundene Warnfunktion erhalten bleibt. Hierfür reicht es z. B. nicht aus, wenn die Betroffenen nur bestätigen, die allgemeinen Geschäftsbedingungen (AGB) und die Datenschutzerklärungen gelesen zu haben, ohne dass sie den Text auch nur einmal aufrufen mussten. Teilweise findet man Einwilligungserklärungen in sehr langen AGB-Texten; damit sind sie kaum auffindbar. Auch wird häufig übersehen, dass Einwilligungserklärungen nicht zusammen mit anderen Erklärungen aufgeführt werden dürfen, wie etwa Informationen zum Kredit. Es ist demgegenüber anzustreben, dass die Kundinnen und Kunden auf dem Weg zum gewünschten Vertrag die jeweiligen datenschutzrechtlichen Einwilligungserklärungen wenigstens einmal anklicken und damit inhaltlich zur Kenntnis nehmen müssen – unabhängig davon, wie eilig sie es gerade haben. Hierdurch wird sichergestellt, dass die Betroffenen die Einwilligungserklärung nicht auf der Internetseite des Unternehmens suchen müssen und im Anmeldeprozess wenigstens einmal zu der Seite geführt werden, die über die aufgrund der Einwilligung

möglichen Datenflüsse informiert. Leider wird die Umsetzung ausreichender datenschutzrechtlicher Standards bei Einwilligungserklärungen teilweise dadurch erschwert, dass Online-Finanzdienstleister (wie andere Online-Unternehmen auch) versuchen, Kundinnen und Kunden mit möglichst wenigen Klicks zum Vertragsabschluss zu führen, da mit jedem zusätzlichen Klick die Gefahr besteht, dass die Seite verlassen wird.

Neben den Problemen bei der Einwilligung ist auch allgemein die Transparenz der Datenverarbeitung nicht ausreichend gewährleistet. So war ein Kunde, der einen Kredit bei einer bestimmten Bank über ein Portal wünschte, überrascht, dass das Bewertungsportal seine personenbezogenen Daten an verschiedene Banken übermittelt hatte.

Gerne wird im Online-Geschäft auch übersehen, dass Kunden bei automatisierten Einzelentscheidungen grundsätzlich eine Remonstrationspflicht einzuräumen ist. Eine Bank hat in ihren AGB festgelegt, dass der Betroffene auf sein Remonstrationsrecht verzichtet, dabei aber übersehen, dass die Betroffenen nicht in die Beschränkung von Schutzrechten einwilligen können.

Wir befinden uns auch im Bankenbereich auf dem Weg in das digitale Zeitalter. Hierdurch darf jedoch das Datenschutzniveau gegenüber dem klassischen Bankengeschäft nicht verschlechtert werden.

8.9 Der eifrige Praktikant

Eine Bankfiliale freute sich über einen besonders eifrigen und interessierten Praktikanten. Eine Kundin bedankte sich per E-Mail für den guten Service, an dem der Praktikant beteiligt war; der Filialleiter leitete das Dankschreiben an die private E-Mail-Adresse des Praktikanten weiter. Nachdem eine Angestellte ihm das Kundeninformationssystem erklärt hatte, nutzte der Praktikant ihre Abwesenheit vom Arbeitsplatz, indem er die Finanzdaten seiner Lehrerin abrief. Darüber informierte er seine Lehrerin, die hiervon keineswegs begeistert war. Am Ende seines Praktikums beschwerte sich der Praktikant über den mangelnden Datenschutz in der Bankfiliale.

Der Praktikant beschwerte sich zurecht über ein schlechtes Datenschutzniveau in der Bankfiliale. Die E-Mail der Kundin enthielt im Anhang auch Kontodaten, deren Übermittlung durch den Filialleiter an den Praktikanten rechtswidrig war. Nachdem der Praktikant den Umgang mit dem Kundeninformationssystem beherrschte, war sicherzustellen, dass er seine Kenntnisse nicht rechtswidrig nutzt. Die Mitarbeiterin hätte deshalb auch bei einer kurzen Abwesenheit ihren Bildschirm sperren müssen.

Die Beschäftigten der Bank haben Fehler eingeräumt. Die Bank hat ihre Richtlinien für den Einsatz von Praktikantinnen und Praktikanten verbessert.

Werden Externe wie Praktikantinnen und Praktikanten eingesetzt, ist eine besondere datenschutzrechtliche Umsicht der Beschäftigten erforderlich.

8.10 Für die gute Sache? – Datenschutz im Spendenwesen

Aus der Praxis

Immer mehr Personen wenden sich an uns, um auf Datenschutzverstöße bei gemeinnützigen Organisationen aufmerksam zu machen. Dabei erhalten Betroffene Werbepost oder werden unerwünscht telefonisch kontaktiert. Zum Teil werden auch Kontoabbuchungen vorgenommen, ohne dass eine Lastschriftermächtigung vorliegt. Woher die Verantwortlichen die Daten der Betroffenen haben, bleibt meist unbekannt.

Gemeinnützige Organisationen sind regelmäßig auf Spenden angewiesen und daher bestrebt, neue Spenderinnen und Spender zu gewinnen. Hinter einigen gemeinnützigen Organisationen stecken aber unseriöse Vereine, die unerwünscht Bürgerinnen und Bürger telefonisch kontaktieren und auf Spenden dringen. Zum Teil werden auch Abbuchungen von den Konten der Betroffenen vorgenommen. Viele von ihnen verlangen daraufhin von den Organisationen Auskunft über die Herkunft ihrer Daten,[231] was in der Regel verweigert wird. Die Sorge, dass ggf. die Daten aus der Selbstauskunft im Internet veröffentlicht werden könnten und

231 Siehe § 34 Abs. 1 Satz 1 Nr. 1 BDSG

damit der Ruf der Organisation geschädigt wird, kann jedoch nicht als Argument herangezogen werden, den Betroffenen die Auskunft zu verweigern.

Als Antwort auf die Herkunft der Daten geben die betroffenen Spendenorganisationen an, dass diese Daten durch Call-Center im Ausland (in den von uns geprüften Fällen ansässig in der Türkei) erworben worden seien. Dabei entziehe sich ihrer genauen Kenntnis, auf welche Weise die Call-Center insbesondere die Telefon- und Bankdaten erheben und verarbeiten.

Damit die entsprechenden Call-Center-Werbeanrufe (sog. Cold Calls) durchgeführt werden dürfen, bedarf es einer Einwilligung der Betroffenen z. B. auf der Homepage der Spendenorganisation.[232] Uns gegenüber wurde angegeben, dass mit den türkischen Call-Centern mündlich vereinbart wurde, dass für jeden dieser Fälle eine schriftliche bzw. elektronische Einwilligung zur Entgegennahme der Anrufe vorliegen müsse.

Die sich an die Telefonate anschließende Erhebung der Bankdaten und die Abbuchungen vom Konto werden durch die Organisationen auf ein vermeintliches mündliches Einverständnis der Betroffenen gestützt. Diese Argumentation deckt sich allerdings nicht mit den Angaben der Betroffenen, die sich vor allem aufgrund der Kenntnis der Bankdaten empört an uns wenden. Da die verantwortliche Stelle die Beweislast für die erbrachte Einwilligung trägt, müsste sie uns eine Einwilligung nachweisen können.

Rechtmäßige Einwilligungen konnten uns bisher weder für die Telefonwerbung noch für die Abbuchungen vorgelegt werden, sodass wir weitere sanktionsrechtliche Maßnahmen prüfen.

Für die Kontaktaufnahme per Telefon und die Abbuchung vom Konto muss eine ausdrückliche Einwilligung vorliegen. Sobald eine Abbuchung ohne schriftliche Lastschriftermächtigung vorgenommen wurde und die Gefahr eines rechtswidrigen Datenhandels gegeben ist, ist Betroffenen zu raten, Strafanzeige zu erstatten.

232 Siehe § 7 Abs. 2 Nr. 2 UWG

8.11 Petitionsplattformen

Wir haben eine Reihe von Anfragen zu Petitionsplattformen erhalten, die von Vereinen oder Unternehmen betrieben werden. Solche Plattformen bieten in der Regel nicht nur eine Infrastruktur dafür, dass Personen Petitionen initiieren und online Unterstützerinnen und Unterstützer für diese gewinnen können. Vielmehr verwenden die Betreiber personenbezogene Daten, die über die Plattform erhoben werden, z. B. auch dazu, um Nutzerinnen und Nutzer für andere Petitionen zu „mobilisieren" oder zu bewerben.

Auf den Webseiten erhalten die Nutzerinnen und Nutzer häufig die Möglichkeit, politische Petitionen zu unterstützen. Hierbei werden Angaben erhoben, die Aufschluss über politische Meinungen oder philosophische Überzeugungen geben können. Bei diesen Daten handelt es sich um besondere Arten personenbezogener Daten, die in der Regel nur mit Einwilligung verarbeitet werden dürfen.[233]

Im Petitionsverfahren werden naturgemäß die Daten der Unterstützerinnen und Unterstützer den Initiatoren der Petition preisgegeben, damit diese den Nachweis über die Anzahl der Unterstützerinnen und Unterstützer führen können. Damit ist aber nicht zwingend verbunden, dass die Daten zusätzlich auch auf der Webseite, auf der die Petition gelistet ist, veröffentlicht werden. Insofern kann nicht argumentiert werden, dass die Betroffenen die Daten im Rahmen der Mitzeichnung offenkundig öffentlich gemacht haben und daher keine gesonderte Zustimmung eingeholt werden muss. Die Veröffentlichung ist daher von der Einwilligung abhängig, die sich ausdrücklich auf die besonderen Arten personenbezogener Daten beziehen muss. Dabei entspricht es nicht den Anforderungen an eine ausdrückliche Erklärung, wenn die Einwilligung bereits „vorausgewählt" ist, indem das entsprechende Häkchen im Auswahlkästchen schon gesetzt wurde.

Nutzen die Webseitenbetreiber Informationen über die unterstützten Petitionen bzw. andere personenbezogene Angaben, um mit weiteren Petitionen oder gar mit eigenen Inhalten zu werben, ist ebenfalls die Einwilligung der Betroffenen erforderlich.

233 § 3 Abs. 9 i. V. m. § 4a Abs. 3 BDSG

Darüber hinaus bieten die Petitionsplattformen wie auch andere Online-Portale häufig die Möglichkeit an, dass sich die Nutzerinnen und Nutzer über ihre Konten bei sozialen Netzwerken auf den Plattformen registrieren können. Mit der Anmeldung im sozialen Netzwerk erfolgt dann auch die Anmeldung bei der Petitionsplattform. Bestimmte Daten aus dem Profil des sozialen Netzwerks werden dabei von der Petitionsplattform übernommen. Zugleich ist davon auszugehen, dass auch das soziale Netzwerk Informationen dazu erhält, dass sich die Nutzerinnen oder Nutzer bei einer Petitionsplattform angemeldet haben.

Derzeit stehen wir mit zwei Betreibern von Petitionsplattformen in Kontakt, deren Fälle noch nicht abgeschlossen sind. Hier geht es insbesondere um Fragen der Einwilligung und deren Gestaltung, um die Nutzung zu Werbezwecken, um die Herstellung von Transparenz über die Datenverarbeitungen und -flüsse im Rahmen der Datenschutzerklärung sowie um den Einsatz von Analysewerkzeugen zur Verfolgung des Nutzerverhaltens (Trackingtools), welches über sog. Third-Party-Cookies[234] auch Dritten zugänglich gemacht wird.

Die Nutzerinnen und Nutzer sollten sich bewusst machen, welche Daten sie bei der Unterstützung von Petitionen preisgeben und welche Informationen damit über sie transportiert werden. Petitionen können häufig auch sensible Sachverhalte betreffen und damit z. B. Aufschluss über politische oder weltanschauliche Überzeugungen geben.

234 Das sind Cookies, die nicht von den Webseitenbetreibern selbst, sondern von Dritten gesetzt werden, um Nutzerinnen und Nutzer webseitenübergreifend zu verfolgen und webrelevante Informationen (Interessen, Aktivitäten im Netz) einzusammeln.

9 Finanzen

9.1 Eintreibung ausstehender Rundfunkbeiträge: Finanzamt als Vollstreckungsbehörde

Aus der Praxis

Zur Eintreibung einer Forderung wegen rückständiger Rundfunkbeiträge bat die Rundfunkanstalt Berlin-Brandenburg (rbb) ein Berliner Finanzamt um Amtshilfe bei der Vollstreckung. Vom Finanzamt wurden daraufhin die Kontodaten des Schuldners an den Beitragsservice des rbb übermittelt. Der Schuldner vertrat die Auffassung, dass die Übermittlung der Daten durch die Melde- und Finanzbehörden unzulässig gewesen sei.

Der Rundfunkbeitragsstaatsvertrag (RBStV) ist als Landesgesetz erlassen worden.[235] Die Regelungen des RBStV sind damit gesetzliche Vorschriften, die nach dem Berliner Datenschutzgesetz[236] Rechtsgrundlagen für die Übermittlungen personenbezogener Daten darstellen können, ohne dass die Betroffenen hierin einwilligen müssen.

Der Gesetzgeber hat in § 14 Abs. 9 RBStV einen einmaligen Datenabgleich zum Zwecke der Bestands- und Ersterfassung bestimmt. Um den Abgleich zu ermöglichen, übermittelt „jede Meldebehörde für einen bundesweit einheitlichen Stichtag automatisiert innerhalb von längstens zwei Jahren ab dem Inkrafttreten des Staatsvertrages" einmalig in standardisierter Form bestimmte Daten aller volljährigen Personen an die jeweils zuständige Landesrundfunkanstalt bzw. den Beitragsservice.

Darüber hinaus bestehen weitere gesetzliche Grundlagen für die Übermittlung von Daten der Meldebehörden an die Rundfunkanstalten bzw. an den Beitragsservice. So sieht § 11 Abs. 4 RBStV vor, dass unter bestimmten Umständen Daten bei öffentlichen Stellen, d. h. auch bei Meldeämtern, erhoben werden dürfen. Zudem

235 Gesetz zum 15. Rundfunkänderungsstaatsvertrag vom 20. Mai 2011, GVBl. 2011, S. 211
236 § 6 Abs. 1 Satz 1 Nr. 2 BlnDSG

existiert das Verfahren der regelmäßigen Datenübermittlung durch die Meldebehörden bei der An- und Abmeldung von Personen, das in den Meldedaten-Durchführungsverordnungen der Länder und im RBStV geregelt ist. Vor diesem Hintergrund sind Datenübermittlungen von Meldeämtern an die Rundfunkanstalten bzw. an den Beitragsservice auch ohne Einverständnis der Betroffenen zulässig.

Nach der Abgabenordnung[237] sind die Finanzbehörden befugt, die Vermögens- und Einkommensverhältnisse von Vollstreckungsschuldnern zu ermitteln, wenn dies der Vorbereitung einer Vollstreckungsmaßnahme dient. Dabei richten sich die Verwaltungsvollstreckungsmaßnahmen von Berliner Behörden auch dann nach der Abgabenordnung, wenn sie keine Steuern betreffen, sondern andere öffentlich-rechtliche Geldforderungen. Grundlage hierfür ist das Bundesverwaltungsvollstreckungsgesetz,[238] das nach dem Berliner Verwaltungsverfahrensgesetz[239] unmittelbar für Berliner Behörden gilt. Danach wird die Anwendung der Abgabenordnung des Bundes ausdrücklich angeordnet. Der sachliche Anwendungsbereich der Abgabenordnung wird dadurch in zulässiger Weise erweitert. Zu den besagten öffentlich-rechtlichen Geldforderungen zählt auch der Rundfunkbeitrag, der aufgrund des RBStV als Abgabe erhoben wird. Das Finanzamt hatte damit die Befugnis, die Bankkontodaten bei der Bank des Schuldners abzufragen und an den Beitragsservice des rbb weiterzugeben.

Die Berliner Finanzbehörden sind befugt, die Vermögens- und Einkommensverhältnisse von Vollstreckungsschuldnern auch dann zu ermitteln, wenn es sich nicht um steuerrechtliche Forderungen handelt.

237 § 249 Abs. 2 AO
238 § 5 Abs. 1 BVwVG
239 § 8 Abs. 1 BlnVwVfG

9.2 Erhebung der Religionszugehörigkeit durch Kirchensteuerstelle

Aus der Praxis

Ein Bürger erhielt Post von der Kirchensteuerstelle bei einem Berliner Finanzamt. Die Kirchensteuerstelle schrieb den Petenten mit seiner Steuernummer an und bat um die Angabe seiner Religionszugehörigkeit. Der Petent war der Auffassung, dass das Finanzamt seine Daten nicht weitergeben dürfe, da es sich bei der Kirchensteuerstelle um keine Behörde handele.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit ist die Aufsichtsbehörde für die Verarbeitung von Daten und kontrolliert die ihrer Aufsicht unterliegenden Stellen, darunter Landesbehörden und Private, im Hinblick auf die Einhaltung datenschutzrechtlicher Vorschriften. Von der Aufsicht ausgenommen sind Stellen der Kirchen und der anderen Religionsgemeinschaften. Dies ergibt sich unmittelbar aus der Garantie der kirchlichen Selbstverwaltung gemäß Art. 140 Grundgesetz i. V. m. Art. 137 Abs. 3 Weimarer Reichsverfassung.

Das Recht der Kirchen, eigene Steuern zu erheben, beruht auf Art. 137 Abs. 6 der Weimarer Reichsverfassung und wird durch das Landesrecht ausgestaltet. Nach dem Kirchensteuergesetz[240] können die Kirchen Steuern auf der Grundlage eigener Steuerordnungen erheben. Die Verwaltung der Steuern kann den Finanzbehörden übertragen werden.[241] Mit der „Verwaltungsvereinbarung über die Verwaltung der Kirchensteuern durch die Berliner Finanzbehörden“ vom 17. November 2011, die zwischen der Senatsverwaltung für Finanzen, der Evangelischen Kirche Berlin-Brandenburg und dem Erzbistum Berlin geschlossen wurde, haben die Kirchen von dieser Möglichkeit Gebrauch gemacht und die Verwaltung der Kirchensteuer den Berliner Finanzbehörden übertragen. Aufgrund dieser Verwaltungsvereinbarung sind die Kirchen berechtigt, gemeinsame Kirchensteuerstellen bei den Berliner Finanzämtern zu unterhalten. Die Aufgaben der „allgemeinen Mitwirkung und Unterstützung“, darunter die Feststellung der subjektiven

240 § 1 Abs. 1 KiStG
241 § 1 Abs. 2 KiStG

Kirchensteuerpflicht,[242] nehmen die Kirchen weiterhin durch ihre Kirchensteuerstellen selbstständig wahr.

Die Kirchensteuerstellen bei den Finanzämtern handeln kraft Kirchenrecht und gehören rechtlich und organisatorisch den Kirchen an. Als Organ der Kirchen kann ihr Handeln den Finanzbehörden des Landes nicht zugerechnet werden. Ihre Handlungen unterfallen daher nicht der Kontrolle der Berliner Beauftragten für Datenschutz und Informationsfreiheit.

Die Annahme des Petenten, die Kirchensteuerstellen seien keine Behörden, ist damit richtig. Die Erhebung von Daten zur Religionszugehörigkeit kann deshalb nicht auf Art. 136 Abs. 3 S. 2 Weimarer Reichsverfassung gestützt werden. Stattdessen können die Kirchen im Rahmen ihrer Selbstverwaltung gemäß Art. 137 Abs. 3 Weimarer Reichsverfassung eigene Angelegenheiten[243] durch eigenes Recht regeln. Ob dies im Fall der Erhebung von Daten zur Religions- und Konfessionszugehörigkeit geschehen ist, obliegt – wie oben erläutert – nicht unserer Prüfungskompetenz. Gleiches gilt für Fragen bezüglich der Aufbewahrungsdauer und Löschung dieser Daten, da auch deren weitere Verarbeitung in den Bereich der kirchlichen Selbstverwaltung fällt.

Die Weiterleitung der Steuernummer durch die Finanzämter an die Kirchen im Rahmen des Kirchensteuerverfahrens kann u. a. auf § 31 Abs. 1 AO i. V. m. § 7 Satz 1 KiStG gestützt werden. Nach § 31 AO sind die Finanzbehörden auch verpflichtet, den Kirchen die Besteuerungsgrundlagen, Steuermessbeträge und Steuerbeträge zur Festsetzung von Abgaben mitzuteilen, die an diese Daten anknüpfen.

Die Kirchensteuerstellen bei den Finanzämtern sind keine Berliner Behörden und unterliegen nicht unserer Aufsicht.

242 Nr. 4 Abs. 1 Satz 2 lit. a Verwaltungsvereinbarung über die Verwaltung der Kirchensteuern durch die Berliner Finanzbehörden

243 Das sind in aller Regel solche, die ihre eigenen Mitglieder betreffen.

9.3 Das Finanzamt und die Putzfrau – Probleme bei der Gewerbeanmeldung

Aus der Praxis

Anlässlich der Anmeldung für ein Gewerbe als Putzfrau wurde eine Petentin vom Finanzamt gebeten, eine Kopie ihres privaten Mietvertrages, einen Zahlungsnachweis über die entrichtete Miete sowie jeweils eine Kopie ihres Passes und ihrer Anmeldung vorzulegen. Die Petentin gab an, dass sie in Berlin keinen Betriebsstandort habe. Sie habe keinen festen Ort für ihre Arbeit, sondern sei für verschiedene Auftraggeber innerhalb der Stadtgrenzen von Berlin tätig.

Die Senatsverwaltung für Finanzen teilte uns auf Nachfrage mit, dass für die Erteilung der Steuernummer zu klären sei, welches Finanzamt zuständig ist. Für die Besteuerung von gewerblichen Einkünften sei grundsätzlich das Finanzamt zuständig, in dessen Bezirk sich der Ort der Geschäftsleitung befinde. Dieser könne auch der Wohnsitz der oder des Steuerpflichtigen sein. Zwar könne die Anmeldung bei der Ordnungsbehörde im Regelfall als Indiz dafür angesehen werden, dass die oder der Steuerpflichtige unter der angegebenen Adresse auch den Wohnsitz habe. In außergewöhnlichen Fällen mit erhöhtem Aufklärungsbedarf sei die Anmeldung jedoch nicht ausreichend. Dies sei z.B. dann gegeben, wenn geklärt werden müsse, ob die Wohnung für eine ordentliche Geschäftsführung geeignet sei und ob dort tatsächlich ein Geschäftsbetrieb geführt werde.

Dem steht entgegen, dass die Petentin hier selbst gegenüber dem Finanzamt angegeben hatte, dass sie als freiberufliche Putzfrau innerhalb der Stadtgrenzen von Berlin für verschiedene Auftraggeber an unterschiedlichen Orten tätig und dass ihre Wohnadresse eben nicht ihre Arbeitsadresse sei. Warum es sich dabei um einen außergewöhnlichen Steuersachverhalt mit erhöhtem Aufklärungsbedarf handelt, bei dem die Anmeldebescheinigung als Nachweis des Wohnsitzes und Ort der Geschäftsleitung nicht ausreicht, wurde von der Senatsverwaltung trotz mehrfacher Nachfrage nicht dargelegt.

Unbestritten kann die Finanzbehörde nach der Abgabenordnung[244] Art und Umfang der Ermittlungen in einem Steuersachverhalt bestimmen. Dies gilt jedoch

244 § 88 Abs. 1 Satz 2, 2. Hbs. AO

nicht uneingeschränkt. Die Finanzbehörde hat dabei die Umstände des Einzelfalls zu berücksichtigen[245] und darf sich nur der Beweismittel bedienen, die sie zur Ermittlung des Sachverhalts für erforderlich hält.[246] Korrespondierend dazu haben die an einem Steuerverfahren Beteiligten den Finanzbehörden nur die zur Feststellung des erheblichen Sachverhalts erforderlichen Auskünfte zu erteilen.[247] Daraus ergibt sich zwingend, dass die Finanzbehörden bei der Erhebung von personenbezogenen Daten zur Ermittlung des Sachverhaltes von Amts wegen an die Grundsätze der Verhältnismäßigkeit und Erforderlichkeit gebunden sind.

Diese Grundsätze gelten auch im Fall der Petentin. Warum in diesem konkreten Fall die Erhebung „vollständiger" Mietvertragsunterlagen, die zum Teil auch Daten Dritter (z. B. Mitmieter) betreffen, außerdem Nachweise regelmäßiger Mietzahlungen und eine Passkopie für die Vergabe der beantragten Steuernummer für Umsatzsteuerzwecke zwingend erforderlich sind, konnte die Senatsverwaltung nicht nachvollziehbar begründen. Wir haben daher einen datenschutzrechtlichen Mangel festgestellt.[248]

Die Steuerbehörden sind bei der Erhebung von personenbezogenen Daten zur Aufklärung eines Sachverhaltes an die Grundsätze der Verhältnismäßigkeit und Erforderlichkeit gebunden. Diese sind für den konkreten Einzelfall zwingend zu begründen. Allgemeine Hinweise auf gesetzliche Bestimmungen sind dafür nicht ausreichend.

245 § 88 Abs. 1 Satz 3 AO
246 § 92 Abs. 1 Satz 1 AO
247 § 93 Abs. 1 Satz 1 AO
248 § 26 Abs. 2 Berliner Datenschutzgesetz (BlnDSG)

10 Aus der Arbeit der Sanktionsstelle

Wir haben 24 Buß- oder Verwarnungsgelder in Höhe von insgesamt 24.020 Euro festgesetzt. In vier Fällen haben wir einen Strafantrag gestellt. Daneben haben wir drei Anordnungsverfahren eingeleitet.

Wie bereits in den Vorjahren mussten wir eine Reihe von Geldbußen verhängen, weil verantwortliche Stellen ihrer gesetzlichen Auskunftspflicht nicht oder nicht in der vorgeschriebenen Weise nachgekommen sind.[249] Ziel unserer Arbeit ist es, im Gespräch mit verantwortlichen Stellen Mängel zu beheben und datenschutzgerechte Lösungen zu erarbeiten, die für alle Seiten tragfähig sind, sodass sanktionsrechtliche Maßnahmen gar nicht erst erforderlich werden. Bei der Aufklärung von Sachverhalten sind wir jedoch auf die Mitwirkung von Unternehmen angewiesen. Durch nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilte Auskünfte[250] können wir Bürgereingaben oft nicht abschließend bearbeiten. Damit werden nicht nur wir in der Erfüllung unseres gesetzlichen Auftrags beeinträchtigt. Auch die Menschen, die sich mit ihrem Anliegen an uns wenden, werden dadurch bei der Durchsetzung ihres Rechts auf informationelle Selbstbestimmung behindert. Wir werden Verstöße gegen die Auskunftspflicht daher weiterhin konsequent mit angemessenen Geldbußen ahnden. Daneben werden wir künftig auch verstärkt von der Möglichkeit Gebrauch machen, Zwangsgelder für nicht erteilte Auskünfte festzusetzen. Der sog. Heranziehungsbescheid[251] steht uns neben den Anordnungsbefugnissen[252] als Zwangsmittel zur Verfügung.

249 § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG)
250 § 43 Abs. 1 Nr. 10 BDSG
251 § 38 Abs. 3 Satz 1 BDSG
252 § 38 Abs. 5 Satz 1 BDSG

10.1 Auskunftspflicht des Pflegedienstes einer Religionsgemeinschaft

Die Leitung des Pflegedienstes einer Religionsgemeinschaft soll unrechtmäßig Kranken- und Beschäftigtendaten an Dritte weitergegeben haben. So jedenfalls lautete der Vorwurf in einer Eingabe. Zur Aufklärung des Sachverhalts baten wir den privatrechtlich organisierten Pflegedienst um Stellungnahme, die er unter Verweis auf das Selbstverwaltungsrecht der Religionsgemeinschaften verweigerte.

Das Selbstverwaltungsrecht der Religionsgemeinschaften besagt, dass sie ihre Angelegenheiten selbstständig, d. h. ohne staatliche Einmischung, jedoch „innerhalb der Schranken des für alle geltenden Gesetzes" ordnen und verwalten.[253] Diese Regelung soll sowohl die Selbstverwaltung der Religionsgemeinschaften als auch den staatlichen Schutz anderer für das Gemeinwesen bedeutsamer Rechtsgüter, wie das Recht auf informationelle Selbstbestimmung, gewährleisten. Der hierdurch bedingten Wechselwirkung zwischen Religionsfreiheit und Schrankenzweck ist durch eine entsprechende Güterabwägung Rechnung zu tragen.[254] Bei der Abwägung zwischen den Rechtsgütern ist zu berücksichtigen, dass eine gesetzliche Regelung dem Selbstverwaltungsrecht der Religionsgemeinschaften insoweit Schranken setzen darf, als sie nicht deren Besonderheit als Religionsgemeinschaft, insbesondere ihren geistig-religiösen Auftrag beschränkt.[255]

Unser Auskunftsverlangen gegenüber dem Pflegedienst stützt sich auf das Bundesdatenschutzgesetz,[256] das als allgemeines Gesetz das Recht des Einzelnen auf informationelle Selbstbestimmung ausgestaltet.

Das BDSG ist im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts bei der Datenverarbeitung durch Religionsgemeinschaften nur dann nicht anwendbar, wenn es dabei ausschließlich um die Religionsmitgliedschaft, um

253 Art. 140 Grundgesetz (GG) i. V. m. Art. 137 Abs. 3 Satz 1 Weimarer Reichsverfassung (WRV)
254 BVerfG, Beschluss vom 25. März 1980 – 2 BvR 208/76, Rn. 142 – zitiert nach juris
255 BVerfG, Beschluss vom 21. September 1976 – 2 BvR 350/75 – zitiert nach juris
256 § 38 Abs. 3 Satz 1 BDSG

Angelegenheiten der Religionsausübung, das Innehaben und Ausüben religionsspezifischer Ämter und Funktionen oder vergleichbare Angelegenheiten geht.[257] In diesem Sinn hat auch der Gesetzgeber bei der Neufassung des BDSG bewusst darauf verzichtet, die öffentlich-rechtlichen Religionsgemeinschaften aus dem Anwendungsbereich herauszunehmen, und hat vor allem davon abgesehen, den privatrechtlich organisierten religionsgemeinschaftlichen Einrichtungen einen Sonderstatus einzuräumen.[258]

Zu berücksichtigen ist dabei, dass die Regelungen des BDSG nicht auf eine Veränderung der organisatorischen Struktur von Religionsgemeinschaften abstellen, sondern die innerhalb dieser Struktur stattfindenden Prozesse der Datenverarbeitung an bestimmte Voraussetzungen knüpfen. Die Verarbeitungsmotive sind hierfür nicht von Belang, es sei denn, die Datenverarbeitung hängt unmittelbar mit der Besonderheit religionsgemeinschaftlicher Tätigkeit – etwa die Verarbeitung von Patientendaten zu seelsorgerischen Zwecken durch den Krankenhausgeistlichen – zusammen.[259] Soweit, wie hier, Religionsgemeinschaften lediglich am allgemeinen Geschäftsverkehr teilnehmen und im kommerziellen Wettbewerb mit anderen Unternehmen stehen, gelten deshalb für sie die Regelungen des BDSG.[260]

Auch die Europäische Datenschutzrichtlinie,[261] auf der das BDSG beruht, enthält keine Bestimmungen, die Religionsgemeinschaften von ihrem Anwendungsbereich ausnehmen. Zugleich hat der Europäische Gerichtshof in seiner sog. Lindqvist-Entscheidung ausdrücklich betont, dass religionsgemeinschaftliche Tätigkeiten dem Anwendungsbereich der Europäischen Datenschutzrichtlinie unterliegen.[262] Die Auswirkungen des grundgesetzlich bestimmten Selbstverwaltungsrechts von Religionsgemeinschaften auf das BDSG sind entsprechend richtlinienkonform auszulegen.

257 Siehe Dammann in Simitis, BDSG, 8. Auflage, Rn. 109 zu § 2

258 Siehe Simitis und Dammann in Simitis, BDSG, 8. Auflage, Rn. 136, 88 f. zu § 2

259 Siehe Simitis in Simitis, BDSG, 8. Auflage, Rn. 137 bis 139 zu § 2

260 Siehe Gola/Schomerus, BDSG, 12. Auflage, Rn. 14a zu § 2; Schreiber in Plath, BDSG, Rn. 11 zu § 2; Eßer in Auernhammer, 4. Auflage, Rn. 12 zu § 2 BDSG; Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, 4. Auflage, Rn. 9 zu § 2

261 Richtlinie 95/46/EG

262 EuGH, Urteil vom 6. November 2003 – C-101/01, Rn. 37-45

Aufgrund dieser Rechtslage haben wir den Pflegedienst mit einem Heranziehungsbescheid zur Auskunft uns gegenüber verpflichtet. Hiergegen hat der Pflegedienst Klage eingereicht, über die nun das Verwaltungsgericht zu entscheiden hat.

Auch Religionsgemeinschaften müssen das Recht auf informationelle Selbstbestimmung beachten und unterliegen unserer Aufsicht, soweit sie hierdurch nicht in ihrer Religionsfreiheit eingeschränkt werden.

10.2 Datenschutz gilt auch für uns – zur Beweisverwertung von Daten aus TKÜ-Maßnahmen

Vermehrt werden uns von der Staatsanwaltschaft Ermittlungsakten zur Prüfung übersandt, weil im Rahmen strafrechtlicher Ermittlungen wegen anderer Straftaten zufällig Verstöße gegen das Bundesdatenschutzgesetz (BDSG) aufgedeckt wurden.

In einem solchen Fall war das Telefon einer des schweren Raubes verdächtigten Person überwacht worden. Aus den Telefongesprächen war bekannt geworden, dass die überwachte Person einen privaten Kontakt zu einer Mitarbeiterin eines Mobilfunkshops dafür genutzt hatte, für nicht bekannte Zwecke Adressdaten aus der dortigen Kundendatenbank zu erfragen.

In einem weiteren Fall war durch eine Telefonüberwachung der dringende Verdacht aufgekommen, dass ein Beamter seine dienstlichen Zugänge zu Informationssystemen dafür genutzt hatte, Fahrzeughalterauskünfte für private Zwecke an Dritte zu übermitteln.

Zu den in Deutschland üblichen Telekommunikationsüberwachungsmaßnahmen (TKÜ-Maßnahmen) zählen das Abhören von Telefongesprächen und das Mitlesen von E-Mails und Kurzmitteilungen (SMS) sowie die Funkzellenabfrage oder der Einsatz von Stillen SMS.[263] Die Telekommunikationsüberwachung ist ein Eingriff

263 Siehe 1.5

in das verfassungsrechtlich geschützte Fernmeldegeheimnis und das Grundrecht auf informationelle Selbstbestimmung. Eine der wichtigsten Rechtsgrundlagen für solche schwerwiegenden Grundrechtseingriffe ist § 100a Strafprozessordnung (StPO). Danach darf ohne Wissen der Betroffenen die Telekommunikation nur unter strengen Voraussetzungen überwacht und aufgezeichnet werden. Grundsätzlich ist es erforderlich, dass die von der Maßnahme betroffene Person der Begehung einer im Gesetz konkret festgelegten Straftat[264] verdächtigt wird.

Für die im Zuge einer Überwachung und Aufzeichnung von Telefongesprächen erhobenen personenbezogenen Daten gilt, dass sie zu Beweiszwecken in anderen Strafverfahren nur dann verwendet werden dürfen, wenn die TKÜ-Maßnahme auch zur Aufklärung dieser Straftat hätte angeordnet werden dürfen.[265] Von diesem Grundsatz darf nur innerhalb enger Grenzen abgewichen werden, so z. B. wenn dies dazu dient, eine erhebliche Gefahr für die öffentliche Sicherheit abzuwehren.[266]

Die Aufklärung von Ordnungswidrigkeiten[267] und Straftaten[268] nach dem BDSG rechtfertigt nicht den Einsatz von TKÜ-Maßnahmen. In den uns vorgelegten Fällen können wir Beweismaterial daher nur dann zur Ahndung von Verstößen verwerten, wenn eine Einzelfallprüfung ergibt, dass eine schwerwiegende Gefahr für die Grundrechte anderer oder die Rechtsordnung allgemein vorliegt. Im Ergebnis dieser Einzelfallprüfungen waren die Voraussetzungen für eine Verwertung der Beweise in den genannten Fällen nicht gegeben. Zwar umfasst der Schutz der öffentlichen Sicherheit auch den Schutz von Individualgütern wie dem grundrechtlich geschützten informationellen Selbstbestimmungsrecht. Da jedoch keine konkreten Anhaltspunkte für drohende erhebliche Gefahren vorlagen, mussten wir mit Blick auf den schwerwiegenden Grundrechtseingriff durch die Telefonüberwachung zugunsten der Beschuldigten von einer Verwendungsbeschränkung der Daten ausgehen und von aufsichtsrechtlichen Maßnahmen absehen.

264 § 100a Abs. 2 StPO
265 § 477 Abs. 2 Satz 2 StPO
266 § 477 Abs. 2 Satz 3 Nr. 1 StPO
267 § 43 BDSG
268 §§ 43 Abs. 2 i. V. m. 44 BDSG

Auch wir müssen uns bei der Erfüllung unserer gesetzmäßigen Aufgaben immer an Rechtsvorschriften zum Schutz der informationellen Selbstbestimmung halten.

10.3 Das Liegenschaftskataster ist keine Werbekartei!

Wieder waren wir mit einer Reihe von Unternehmen aus der Immobilienbranche befasst, die unbefugt Daten von Immobilieneigentümern für Werbezwecke nutzten. So hatte ein Maklerunternehmen bei einem bezirklichen Vermessungsamt einen Antrag auf Übermittlung von Eigentümerdaten gestellt,[269] weil einer seiner Kunden vorgeblich ein konkretes Interesse daran besaß, die Immobilie zu kaufen. Tatsächlich nutzte das Unternehmen die Daten jedoch, um bei den Eigentümern der Immobilie allgemein mit seinen Makler- und Verwalterleistungen zu werben.

Die Vermessungsämter dürfen Eigentümerdaten nur an Personen oder Unternehmen herausgeben, die ein berechtigtes Interesse an dem Erhalt der Daten dargelegt haben. Während das konkrete Kaufinteresse an einer Immobilie ein solches berechtigtes Interesse darstellt, ist dies bei allgemeinen Werbezwecken zu verneinen. Darauf weisen die Vermessungsämter bei Antragstellung explizit hin.

Gegen unseren Bußgeldbescheid, mit dem wir ein dreistelliges Bußgeld festgesetzt haben, legte das Unternehmen Einspruch ein. Das Verfahren liegt nun dem Amtsgericht Tiergarten zur Entscheidung vor.

Das Liegenschaftskataster ist keine Werbekartei für die Immobilienbranche. Den Missbrauch von Eigentümerdaten zu Werbezwecken verfolgen wir mit hohen Geldbußen.

269 § 17 Abs. 1 Satz 2 Nr. 2 Vermessungsgesetz Berlin

10.4 Spielhalle is watching you

Gegen einen Spielhallenbetreiber setzten wir ein vierstelliges Bußgeld fest, weil er mit der Überwachung einer seiner Spielstätten zu weit ging. Bei einer Vor-Ort-Prüfung hatte das Ordnungsamt Neukölln festgestellt und dokumentiert, dass mit einer Außenkamera am Gebäude der gesamte Gehweg sowie die anliegende Fahrbahn über Monitore im Inneren der Spielhalle einzusehen waren.

Zwar kann die Überwachung per Videokamera zum Schutz vor Vandalismus und Einbrüchen sowie zur Einlasskontrolle unter bestimmten Voraussetzungen erlaubt sein.[270] Eine großflächige Videoüberwachung des öffentlichen Straßenlandes ist jedoch regelmäßig unzulässig. Das Amtsgericht Mitte entschied in einem ähnlichen Fall, dass der Erfassungsbereich von Kameras bis auf maximal einen Meter von der Hausfassade reduziert sein sollte, wenn diese unmittelbar an den öffentlich zugänglichen Bürgersteig grenzt. Passanten sollten bereits an der Ausrichtung der Videoüberwachung erkennen können, dass diese tatsächlich nur die Fassade erfasst.[271]

Da wir den Spielhallenbetreiber bereits in einem vorangegangenen Verfahren über die Voraussetzungen für den Betrieb einer Videoüberwachungsanlage beraten hatten, mussten wir in diesem Wiederholungsfall davon ausgehen, dass die Daten vorsätzlich unbefugt erhoben wurden. Der Beschuldigte legte Rechtsmittel gegen unseren Bescheid ein.

Der private Einsatz von Videoüberwachungstechnik im öffentlichen Raum ist nur begrenzt und für konkret festgelegte Zwecke gestattet. Eine großflächige Überwachung öffentlichen Straßenlandes durch private Stellen ist unzulässig.

270 § 6b Abs. 1 Nr. 2 und 3 BDSG

271 Siehe Urteil des Amtsgerichts Mitte vom 18. Dezember 2003 – 16 C 427/02

10.5 Privatvollstreckung mit GPS-Tracker?

Gegen eine Person, die am Fahrzeug der Anzeigenden einen GPS-Tracker befestigt hatte, stellten wir Strafantrag wegen unbefugter Datenerhebung mit Bereicherungsabsicht.[272] Mit den Ortungsdaten hatte die Person die Wohnanschrift der Anzeigenden in Erfahrung bringen wollen, um so berechtigte Geldforderungen eintreiben zu können.

Nur wenige Wochen, nachdem wir Strafantrag gegen den Beschuldigten gestellt hatten, teilte uns die Staatsanwaltschaft mit, das Ermittlungsverfahren eingestellt zu haben, da in der Handlung des Täters keine Bereicherungsabsicht zu erkennen gewesen sei. Dies wurde damit begründet, dass der Täter nachweislich einen zivilrechtlichen – und somit berechtigten – Anspruch gegen die Anzeigende hatte. Eine Bereicherungsabsicht setze hingegen voraus, dass der Täter einen Vermögensvorteil durch eine unberechtigte Vermögensverschiebung erreichen wolle.

Dieser Bewertung lag der fehlerhafte Vergleich mit anderen im deutschen Strafrecht verankerten Tatbeständen zugrunde. Bei Vermögensdelikten wie Erpressung (§ 253 StGB) und Betrug (§ 263 StGB) fordert das Gesetz, dass der durch die Tat bezweckte Vermögensvorteil rechtswidrig ist. Bei datenschutzrechtlichen Straftaten muss der beabsichtigte Vermögensvorteil hingegen nicht rechtswidrig sein. Dies ergibt sich aus dem Sinn und Zweck der Norm, das Grundrecht auf informationelle Selbstbestimmung (und nicht das Vermögen) zu schützen. Wer personenbezogene Daten unbefugt erhebt, um damit vermögensrechtliche Ansprüche durchzusetzen, beeinträchtigt das informationelle Selbstbestimmungsrecht des Opfers gleichermaßen wie jemand, der mit seiner Handlung einen rechtswidrigen Vermögensvorteil erstrebt. Der unbefugte Umgang mit personenbezogenen Daten kann also nicht durch zivilrechtliche Ansprüche gerechtfertigt sein. Wir haben die Staatsanwaltschaft auf diesen Umstand hingewiesen, woraufhin sie die strafrechtlichen Ermittlungen wieder aufgenommen hat.

Zivilrechtliche Ansprüche legitimieren den rechtswidrigen Umgang mit personenbezogenen Daten nicht.

272 § 43 Abs. 2 Nr. 1 i. V. m. § 44 BDSG

11 Datendiebstahl digital und analog

11.1 Informationspflicht bei Datenlecks

Es sind bei uns insgesamt 39 Mitteilungen zu Datenlecks[273] eingegangen. In 33 Fällen handelte es sich um Meldungen aus dem nicht-öffentlichen Bereich, während uns in den übrigen sechs Fällen öffentliche Stellen über einen Datenvorfall informiert haben.

11.1.1 Probleme in der Reisebranche

Aus der Praxis

Ein Unternehmen aus der Reisebranche unterrichtete uns über ein Datenleck, das durch eines seiner Internetportale entstanden war. Über die Webseite können Kundinnen und Kunden, die bei einem Reisebüro oder einem Flugbuchungsportal einen Flug gebucht haben, unter Eingabe der Buchungsnummer sowie des Nachnamens eines der Mitreisenden ihre Flugtickets sowie Rechnungsinformationen abrufen. Durch eine IT-Sicherheitslücke konnten die Datensätze von Millionen Flugreisenden, teilweise einschließlich der Kontodaten, ausgelesen werden.

Wir haben unverzüglich eine Betriebsprüfung vor Ort durchgeführt und dabei insbesondere die von dem Unternehmen in Anbetracht des Datenlecks ergriffenen Sicherheitsmaßnahmen kontrolliert. Nach Bekanntwerden der Sicherheitslücke hat es seine IT-Prozesse getestet und verbessert, um einen derartigen Vorfall in Zukunft zu verhindern.

Das Unternehmen hat uns gegenüber erklärt, als Auftragsdatenverarbeiter[274] für die Reisebüros und Flugbuchungsportale tätig zu sein. Aus diesem Grund obliege

273 § 42a BDSG, § 18a BlnDSG
274 § 11 BDSG

es nicht ihm, die Betroffenen zu informieren, sondern den jeweils verantwortlichen Stellen.[275] Unsere Prüfung dauert noch an.

Internetportale sind von ihren Betreibern regelmäßig hinsichtlich Datenschutz und IT-Sicherheit zu testen und abzusichern.

11.1.2 Datenleck bei einer Partei

Im Mai hat uns eine politische Partei gemeldet, dass personenbezogene Daten von aktuellen und ehemaligen Parteimitgliedern auf bestimmten parteifremden Webseiten veröffentlicht worden sind. Die Datensätze umfassten Angaben zu Namen, Anschriften, Geburtsdaten, Telefonnummern und E-Mail-Adressen. Es handelte sich dabei offenbar um personenbezogene Daten von Teilnehmerinnen und Teilnehmern an Parteitagen in den Jahren 2015 und 2016. Zu dem Datenleck haben uns zahlreiche Petenteneingaben erreicht.

Es ließ sich bisher nicht zweifelsfrei aufklären, auf welche Weise die sensitiven Daten[276] Dritten unrechtmäßig zur Kenntnis gelangt sind. Anlässlich des Datenlecks hat der Bundesverband der Partei umfangreiche IT-forensische Untersuchungen durchführen lassen. Die dabei gefundenen Schwachstellen hat die Partei beseitigt und einen Mitarbeiter als IT-Koordinator mit Schwerpunkt IT-Sicherheit eingestellt. Die Betroffenen wurden durch individuelle Anschreiben über den Vorfall informiert und haben zudem Empfehlungen für verstärkten Datenschutz und IT-Sicherheit erhalten.

Datenlecks müssen der Aufsichtsbehörde bei Vorliegen der gesetzlichen Voraussetzungen gemeldet und die Betroffenen in der Regel individuell über den Vorfall informiert werden.

275 Zu den Voraussetzungen der Meldepflicht siehe § 42 a BDSG
276 § 3 Abs. 9 BDSG

11.1.3 Datenleck bei einem Internetportal

Wir wurden über ein Datenleck bei einem Internetportal informiert, das bundesweit Reinigungskräfte vermittelt. Durch eine IT-Sicherheitslücke war es möglich, personenbezogene Daten der registrierten Kundinnen und Kunden einzusehen. Das Unternehmen hat sich vorsorglich mit Informationen zu dem Vorfall bei uns gemeldet und vorgetragen, nicht der gesetzlichen Meldepflicht[277] zu unterliegen, da von dem Datenleck nur Rechnungen betroffen waren, die die Adressdaten der Personen, aber keine Bankverbindungen enthielten.

Wir haben das Unternehmen aufgefordert, die Sicherheitslücke zu schließen. Es hat daraufhin technisch-organisatorische Maßnahmen vorgenommen, um ein Datenleck in Zukunft zu vermeiden. Zu diesen Maßnahmen gehörten Sicherheitstests aller Systeme, eine Überarbeitung des Sicherheitskonzepts in Bezug auf neue Entwicklungen sowie die Durchführung einer externen Sicherheitsüberprüfung. Da das Unternehmen zudem die Betroffenen individuell über das Datenleck informiert hat, haben wir den Vorgang abgeschlossen.

Datenlecks sollten auch bei Zweifeln am Vorliegen der gesetzlichen Voraussetzungen der Aufsichtsbehörde vorsorglich gemeldet und die Betroffenen über den Vorfall informiert werden.

11.1.4 Einbruch im Bürgeramt

Allerdings ist nicht nur im Internet der Schutz personenbezogener Daten gefährdet, sondern auch im analogen Leben. So wurden in einem Bürgeramt zweimal hintereinander mehrere hundert Ausweisdokumente gestohlen. Sie enthielten Passnummern, Namen, Vornamen und Geburtsdaten der Betroffenen und waren zur Zeit der Einbrüche in verschlossenen Metall- und Stahlschränken aufbewahrt. Über den Diebstahl wurden die Polizei, das Facility Management des Bezirksamts, die Betroffenen und wir in Kenntnis gesetzt. Im Anschluss an die Einbrüche wur-

277 Zu den Voraussetzungen der Meldepflicht siehe § 42 a BDSG

den Sicherungsmaßnahmen an den Fenstern und Zugängen zur Vermeidung weiterer Einbrüche vorgenommen und neue Metall- und Stahlschränke beschafft.

Personenbezogene Daten müssen auch in Papierform immer gegen Diebstahl geschützt sein.

11.2 Ransomware – die nicht zu unterschätzende Gefahr kann jeden treffen

Die Meldungen zu aktuellen Bedrohungen durch Angriffe auf die Informationstechnologie nehmen nicht ab. Anfang des Jahres gab es massive Angriffe von sog. Trojanern, die Speicherinhalte verschlüsselten. Meldungen wie „Ransomware-Virus legt Krankenhaus lahm" erschienen fast täglich in den Tageszeitungen. Auch in der Berliner Verwaltung soll es erfolgreiche Angriffe gegeben haben.

Unter all den Schadprogrammen gehört insbesondere die sog. Ransomware zu den sehr aktiven Schädlingen. Hierbei verbreitet sich eine Erpressungssoftware meist über E-Mails mit infizierten Anhängen, Programmen aus sog. nicht vertrauenswürdigen Quellen oder manipulierten Webseiten. Am gefährlichsten sind die Kryptotrojaner,[278] welche Festplatten oder Dateien auf den infizierten Systemen verschlüsseln. Gegen Zahlung einer „Gebühr" werden die Daten dann wieder entschlüsselt – so wird es zumindest in Aussicht gestellt. Ist der Rechner mit einem Netzwerk verbunden, kann eine Verbreitung auf weitere im Netzwerk integrierte Computer erfolgen.

Wenn man zurückblickt, geht die Idee auf das Jahr 1989 zurück. Der Schädling „Aids Trojan Disk" verschlüsselte Daten mit Hilfe einer infizierten Diskette.[279] Wurde damals noch aufgefordert, Geld an ein Postschließfach in Panama zu schicken, werden heute Bitcoins[280] verlangt. Die Beträge können je nach Größe und Bedeutung der Unternehmen leicht vier- bis fünfstellige Summen erreichen.

278 Dazu gehören u. a. Cryptowall, CryptoFence, TeslaCrypt, Locky und Maktub.
279 Siehe Wikipedia zum Thema „Ransomware"
280 Digitale Währung (Geldeinheit)

Anfang Februar 2016 explodierten die Angriffszahlen insbesondere in Deutschland durch „Locky". Der Trojaner verschlüsselte Dateien, die durch die Dateiendung „.locky" leicht erkennbar waren. Oft war das Öffnen einer vermeintlichen Rechnung, die in Form eines Microsoft-Office-Dokuments als Anhang einer E-Mail verschickt wurde, der Auslöser für die Verschlüsselung. Gegen Zahlung von Bitcoins konnte eine entsprechende Entschlüsselungssoftware erworben werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) riet grundsätzlich von einer Zahlung ab, da nicht auszuschließen war, dass trotz Zahlung eine Entschlüsselung nicht erfolgen würde; stattdessen solle man Anzeige erstatten. In der Presse war allein in Deutschland von 5000 infizierten Rechnern pro Stunde die Rede.[281]

Welche Vorkehrungen sollten getroffen werden, um sich vor solchen Angriffen wirksam zu schützen?

Das sinnvollste und einfachste Mittel ist eine regelmäßig durchgeführte Datensicherung. Sie kann sowohl durch eine Datensicherungssoftware unterstützt erfolgen als auch durch einfaches Kopieren der Dateien auf einen externen Datenträger. Dadurch stehen die unverschlüsselten Dateien nach einem Angriff wieder zur Verfügung. Da sich die Schadsoftware über Netzwerkfreigaben verbreiten kann, ist es jedoch wichtig, dass sich die Sicherung auf einem externen Speicherlaufwerk befindet, welches nicht permanent mit dem Computer verbunden ist. Hierfür eignen sich externe Festplatten, die ausschließlich für die Datensicherung angeschlossen werden, oder optische Speichermedien wie CDs oder DVDs. Die gesicherten Daten befinden sich dann außerhalb der Zugriffsmöglichkeit der Schadsoftware.

Bei „Locky" hätte es ausgereicht, die automatische Ausführung von Makros in den Einstellungen der Microsoft-Office-Programme zu deaktivieren. Hierzu sind nur wenige Änderungen in den Optionen der Software notwendig. Auch das Ansehen von Dateien mit reinen Leseprogrammen (sog. Viewer), die kostenfrei im Inter-

281 Handelsblatt vom 29. Februar 2016, S. 22 f.

net zur Verfügung stehen, hätte das Ausführen von Makros verhindert.[282] Zum Betrachten der Dateien reichen diese Programme vollkommen aus.

Auch ein vorsichtiger Umgang mit E-Mail-Anhängen kann vor solchen Bedrohungen schützen. Nicht jede E-Mail und jeder Anhang muss sofort geöffnet werden. E-Mails und insbesondere E-Mail-Anhänge von unbekannten Absendern sollten immer mit besonderer Vorsicht behandelt werden. Eine Nachfrage bei bekannten Absendern kann helfen, die Sicherheit zu erhöhen. Hier sollten Unternehmen und Behörden mehr Zeit in die Aufklärung und Unterweisung der Anwender investieren. Für alle zu empfehlen sind die hilfreichen Informationen des BSI, wie z. B. die Internetseite „BSI für Bürger".[283]

Offenbar hatten bei den aufgeführten Attacken weder der Virenschutz noch die Firewall einen Alarm ausgelöst. Das kommt daher, dass ein neuer Schädling meist erst nach ein paar Stunden durch das eingesetzte Virenschutzprogramm erkannt wird. Um das Risiko zu minimieren, sollten diese Schutzmechanismen immer aktuell gehalten werden, damit zumindest bekannte Schadsoftware abgewehrt werden kann. Natürlich werden auch Virenschutzprogramme weiterentwickelt. So wird gezielt nach neuen Schadsoftware-Verbreitungstechniken gesucht und versucht, diesen in geeigneter Weise zu begegnen. Die meisten Virenschutzprogramme bieten die Möglichkeit, das System auf anomales Verhalten zu untersuchen. Dieser Schutzmechanismus ist jedoch häufig zu schwach eingestellt oder deaktiviert, da sonst häufig Fehlalarme auch bei nicht infizierten Programmen ausgelöst werden.

Doch nicht nur die Virenschutzsoftware muss auf einem aktuellen Stand gehalten werden. Angriffe erfolgen auch über Lücken im Betriebssystem, in Browsern und Software wie Java oder Flash. Bezüglich der Meldung solcher Lücken sind Dienste wie das Bürger-CERT[284] hilfreich, die über aktuelle Bedrohungen informieren. Der

282 Viewer sind eigenständige Dateibetrachter, die Dateien im reinen Lesezugriff öffnen. Bei Microsoft-Office-Dokumenten wird dazu das eigentliche Microsoft-Office dann gar nicht verwendet. Die Dateien werden nur dargestellt. Ein Ändern der Dateiinhalte ist nicht möglich, und evtl. vorhandene Makros werden nicht ausgeführt.

283 www.bsi-fuer-buerger.de

284 www.buerger-cert.de

Dienst ist kostenfrei und die Informationen werden in der Regel durch Newsletter zugesandt.

Betroffene, die keine Datensicherung durchgeführt haben, können ihre Daten möglicherweise dadurch zurückerhalten, dass sie sog. Forensik-Tools[285] anwenden oder ein Entschlüsselungswerkzeug von einem Antivirenprogramm-Hersteller zur Verfügung gestellt bekommen. Da die Verschlüsselungs-Trojaner meist die Dateien verschlüsseln und die Originale löschen, kann u. U. ein Datenrettungsprogramm helfen, gelöschte Dateien wiederherzustellen. Über spezielle Internetseiten[286] können befallene Dateien hochgeladen werden. Dort wird versucht, die Ransomware zu identifizieren und dem Nutzenden Hinweise zum weiteren Vorgehen zu geben. Je nach eingesetztem Trojaner erhält man eventuell einen Link zu einem Programm, das die Dateien entschlüsseln kann.

Einfache Maßnahmen wie eine regelmäßige Datensicherung oder der vorsichtige Umgang mit E-Mail-Anhängen können helfen, sich vor Ransomware zu schützen.

285 Werkzeuge für die Analyse von Datenbeständen

286 z. B. https:\\id-ransomware.malwarehunterteam.com

12 Telekommunikation und Medien

12.1 Novellierung der Datenschutzrichtlinie für elektronische Kommunikation

Die Europäische Kommission hat mit der Überarbeitung der Richtlinie über den Schutz der Privatsphäre in der elektronischen Kommunikation[287] begonnen. Die Reform dient einerseits der Umsetzung der Strategie zum digitalen Binnenmarkt. Andererseits sollen Anpassungen vorgenommen werden, die durch die Verabschiedung des EU-Datenschutz-Reformpakets[288] sowie durch veränderte technische Rahmenbedingungen erforderlich geworden sind.

Im Zuge der Überarbeitung der Richtlinie steht vor allem zur Diskussion, ob und inwieweit der Anwendungsbereich der Richtlinie vergrößert werden soll, d. h. welche elektronischen Dienste unter die Regelungen der Richtlinie und welche unter die Regelungen der EU-Datenschutz-Grundverordnung (DS-GVO) fallen sollen. Sowohl der Europäische Datenschutzbeauftragte als auch die Art. 29-Datenschutzgruppe[289] haben sich dafür ausgesprochen, dass die insoweit strengeren Vorgaben der E-Privacy-Richtlinie zukünftig auch für sog. Over-The-Top-Dienste gelten sollen.[290] Hintergrund dieser Forderung ist, dass die Kommunikation über diese

287 Richtlinie 2002/58/EG, auch bekannt als Datenschutzrichtlinie für elektronische Kommunikation oder E-Privacy-Richtlinie

288 Siehe bereits JB 2015, 2.1

289 Sie besteht aus Vertretern sämtlicher europäischer Datenschutzbehörden und hat beratende Funktion.

290 Im Zusammenhang mit der Novellierung der Datenschutzrichtlinie wird der Begriff „Over-The-Top-Dienste" in Abgrenzung zu traditionellen Telekommunikationsdiensten, die von Telekommunikationsanbietern erbracht werden, verwendet. Während Telekommunikationsanbieter den Zugang zum Internet erbringen, setzen die Dienste der Over-The-Top-Anbieter voraus, dass die Nutzenden schon einen Internetzugang haben. Ihre Kommunikationsangebote bauen auf dem Angebot der klassischen Telekommunikationsanbieter auf. Zu diesen Diensten zählen Services wie z. B. WhatsApp oder Skype.

Dienste den gleichen strengen Anforderungen unterliegen muss wie die klassische Kommunikation über Telefon oder die Versendung von SMS. Der Europäische Datenschutzbeauftragte forderte darüber hinaus, dass die E-Privacy-Richtlinie im Zusammenhang mit dem sog. Internet der Dinge[291] auch auf die Kommunikation zwischen Maschinen anwendbar sein sollte, um auch in diesem Bereich ein hohes Maß an Vertraulichkeit zu gewährleisten. Weitere wichtige Punkte der Reformvorschläge beziehen sich auf die Erhebung von Verkehrs- oder Standortdaten durch andere Anbieter als klassische Telefonunternehmen, die Voraussetzungen für eine wirksame elektronische Einwilligung, das Verbot der Überwachung verschlüsselter Kommunikation und den besseren Schutz vor unerwünschter elektronischer Kommunikation. Die Kommission plant, im Frühjahr 2017 einen entsprechenden Entwurf zu veröffentlichen.

Auch sog. Over-The-Top-Dienste könnten zukünftig dem Anwendungsbereich der E-Privacy-Richtlinie unterfallen. Die Kommunikation über diese Dienste wäre dann ebenso vertraulich zu behandeln wie die Kommunikation über klassische Telefondienste.

12.2 Bewegungsprofile aus Standortdaten der Telekommunikationsanbieter

Aus der Praxis

Wir berieten ein Unternehmen, das Daten über den Aufenthaltsort von Mobilfunknutzenden ohne deren Einwilligung für die Analyse von Verkehrsströmen aufbereiten möchte.

Bei jeder Verbindung eines Smartphones mit dem Mobilfunknetz erhält das netzbetreibende Unternehmen eine Information darüber, wo sich die Besitzerin oder der Besitzer des Geräts gerade aufhält. Damit Mobilfunkverbindungen zustande kommen, ist es für das netzbetreibende Unternehmen erforderlich, diese Daten zu verarbeiten und wenigstens zeitweise zu speichern. Die Ortsangaben sind nicht präzise, sondern beschreiben (in Berlin) eine Umgebung von durchschnittlich 150

291 Die zunehmende informationelle Vernetzung von Gegenständen des alltäglichen Lebens

bis 300 Metern. In einigen Ortsteilen sind die Abstände zu den Mobilfunkmasten größer. Es gibt jedoch auch Antennen, die nur sehr kleine Bereiche abdecken.

Die Ortsangaben fallen regelmäßig an. Wird mit dem Smartphone nicht nur telefoniert, sondern werden auch Datendienste genutzt, verbindet sich das Gerät häufig mit dem Netz. So verfügen die Netzanbieter durchschnittlich über Ortsangaben im Fünf-Minuten-Takt.

Es liegt auf der Hand, dass die Beschreibung des Weges einer Person durch die Stadt trotz der örtlichen Unschärfe viel über sie aussagt. So ist zu sehen, wo die Person wohnt, wo sie arbeitet, vielleicht auch zu welcher Schule sie ihre Kinder bringt. Es können auch Orte dabei sein, die intimerer Natur sind und aus Sicht der betroffenen Person nicht offenbart werden sollten. Sicher ist: Es gibt keine zweite Person mit den gleichen täglichen Fixpunkten. Eine Person kann anhand dieser Bewegungsprofile erkannt werden. Damit handelt es sich um datenschutzrechtlich relevante Daten.

Das zu beratende Unternehmen bezieht die beschriebenen Standortdaten von einem großen deutschen Netzanbieter. Inwieweit das Zusammenstellen der Daten durch ihn rechtmäßig ist, wird von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beurteilt. Wir bewerten, ob die übergebenen Daten noch etwas über einzelne Personen aussagen. Wäre dies der Fall, würde das betreffende Unternehmen die Einwilligung der identifizierbaren Mobilfunkkunden für die Verarbeitung benötigen. Da es die Einwilligungen nicht selbst einholen kann, müssten dies die Mobilfunkanbieter tun. Diesen Weg möchte das Unternehmen nicht gehen.

Nun gibt es statistische Angaben, die zweifellos nichts über einzelne Personen aussagen: Wie viele Personen nutzen innerhalb einer Stunde das Mobilfunknetz in einem bestimmten Abschnitt der Berliner U-Bahn? – Das Unternehmen hat hierzu mit dem Netzbetreiber vereinbart, dass es diese Informationen erhält, wenn eine bestimmte Mindestzahl nicht unterschritten wird. Das ist nicht zu beanstanden. Wie viele Personen halten sich längere Zeit in Gegend A auf und bewegen sich dann zwischen zehn und elf Uhr nach Gegend B, um dort für eine Weile zu bleiben? – Hier muss der Blick sorgfältiger sein: Mindestzahlen sind einzuhalten und ggf. die Zahlen leicht zu verfälschen, um keine Schlüsse auf einzelne Personen

zuzulassen. Von derartigen Abweichungen wird eine Analyse des Verkehrsstroms nicht negativ beeinflusst.

Der Wunsch ist jedoch groß, weitergehende Einblicke in die Daten zu erhalten. Wäre es nicht möglich, die Bewegungsprofile ganzer Tage individuell zu betrachten? Wie lassen sich diese ggf. derart verfremden, dass die gleichen Schlüsse aus den Daten gezogen werden können, aber das Profil einzelner Personen nicht wiedererkannt werden kann? Kann eine Verknüpfung mit weiteren Daten erfolgen, wenn dies nicht anhand eines Namens oder der Nummer des Geräts bzw. der SIM-Karte geschieht? Ist eine Aufgliederung der Statistiken auf Kundinnen und Kunden und auf bestimmte Altersgruppen möglich? – Da das netzbetreibende Unternehmen selbst Mobilfunkanbieter ist, kann es diese Angaben zumindest bezogen auf die eigenen Kundinnen und Kunden zur Verfügung stellen.

Noch haben wir keinen schlüssigen Nachweis erhalten, dass der gewünschte Datenkatalog keine Schlüsse auf einzelne Personen zulässt. Die Anforderungen sind hoch: Die Schlüsse dürfen auch nicht durch geschickte mathematische Auswertungsverfahren zu erzielen sein. Selbst wenn sich nur ein geringer Prozentsatz der erhobenen Daten mit leicht zu erwerbendem Zusatzwissen einzelnen Personen zuordnen lässt, ist das Vorgehen nicht rechtmäßig.

Zudem mangelt es an Transparenz. Die Mobilfunkkundinnen und -kunden sollten von der Aufbereitung ihrer Daten durch netzbetreibende Unternehmen und sonstige Dritte wissen, auch wenn an ihrem Ende eine anonyme Statistik steht. Dies umso mehr, als Restrisiken fortbestehen und ihre Größe ungewiss bleibt, solange sie nicht mit wissenschaftlich anerkannten Methoden eingegrenzt wurden.

Diese Forderung richtet sich auch an andere Betreiber von Telekommunikationsdiensten, insbesondere die großen Betriebssystemhersteller Apple und Google, bei denen weit präzisere Standortdaten eingehen. Auch wenn sie mit der Einwilligung der Nutzenden operieren, ist das nur dann rechtlich wirksam, wenn diese Einwilligung freiwillig und informiert erteilt wurde, also bei Bestehen einer echten Wahl, ausreichender Information und ohne sachfremde Kopplung mit der Erbringung von Dienstleistungen, für die es keine Alternativen gibt.

Standort- und Bestandsdaten aus dem Mobilfunk sind nur schwer zu anonymisieren. Die Tragfähigkeit ihrer Verarbeitung ohne Einwilligung der Nutzenden ist zweifelhaft.

12.3 Konsequenzen aus der Entscheidung des Bundesgerichtshofs zur Facebook-Funktion „Freunde finden" für Anbieter von Telemedien

Der Bundesgerichtshof (BGH) hat entschieden, dass sog. Einladungs-E-Mails, die Facebook an Kontakte seiner Nutzerinnen und Nutzer verschickte, eine unzumutbare Belästigung im Sinne des Wettbewerbsrechts darstellen, wenn die Betroffenen nicht vorher eingewilligt haben.[292] Das Urteil bezieht sich auf E-Mail-Nachrichten, die Facebook versandte, nachdem die Nutzenden des Dienstes bei der Anmeldung die zusätzlich verfügbare Option „Freunde-finden" betätigt hatten. Die Nachrichten wurden an Nicht-Mitglieder von Facebook verschickt, deren Daten in den E-Mail-Accounts der Nutzerinnen und Nutzer hinterlegt waren.

Der BGH hat nun klargestellt, dass derartige Einladungs-E-Mails Werbemaßnahmen des sozialen Netzwerks darstellen. Denn sie zielen u. a. darauf ab, neue Mitglieder für die eigene Plattform zu gewinnen. Das Unternehmen könne sich nicht darauf berufen, dass der Versand der E-Mails privaten Charakter habe. Für den Werbe-Charakter reiche es bereits aus, dass die Einladungen zumindest auch dazu dienten, die Leistungen des Unternehmens anzupreisen. Für die Betroffenen sei außerdem erkennbar gewesen, dass die E-Mails keine persönlichen Botschaften ihrer Bekannten enthielten, sondern vielmehr von Facebook selbst erstellt und versandt wurden. Die Nutzerinnen und Nutzer, die Facebook den Zugriff auf ihre E-Mail-Konten erlaubten, seien darüber hinaus nicht hinreichend darüber informiert worden, dass auch Nicht-Mitglieder kontaktiert würden.

Der BGH hat damit deutlich gemacht, dass jede Person für sich selbst entscheiden können muss, ob sie Teil eines sozialen Netzwerks sein und diesem ihre personenbezogenen Daten zur Verfügung stellen möchte. Insofern gelten

292 BGH, Urteil vom 14. Januar 2016 – I ZR 65/14, in: ZD 2016, S. 484 ff.

für diese Unternehmen in Bezug auf die Verwendung personenbezogener Daten keine anderen Vorschriften als für Unternehmen anderer Branchen. Vor der Ansprache von Personen, die man für das eigene Netzwerk werben möchte, muss daher deren Einwilligung[293] eingeholt werden.

12.4 Neue Datenschutzrichtlinie von WhatsApp – mehr Daten an Facebook, weniger Selbstbestimmung?

Im August gab die Facebook-Unternehmensgruppe bekannt, in Zukunft auch Daten mit ihrem Tochterunternehmen WhatsApp auszutauschen. So wird seitdem u. a. die Telefonnummer der jeweiligen WhatsApp-Nutzenden zusammen mit einzelnen Nutzungsstatistiken an Facebook übermittelt. Bei der Übernahme von WhatsApp im Februar 2014 durch Facebook wurde dies noch ausgeschlossen.

Darüber hinaus gibt WhatsApp in seinen Antworten auf Fragen zu den aktualisierten Nutzungsbedingungen und der eigenen Datenschutzrichtlinie an, dass man neben der Verbesserung des Services u. a. auch anstrebt, die mögliche Kommunikation zwischen den Anwenderinnen und Anwendern und den Firmen über WhatsApp zu verbessern.[294] Des Weiteren sollen auch andere Dienste der Facebook-Familie wie Instagram zukünftig einzelne Daten von WhatsApp-Nutzenden erhalten, um z. B. passende Vorschläge für andere Nutzerinnen und Nutzer zu erarbeiten, denen man bei Instagram folgen könnte. Viele Teilnehmende sind seitdem besorgt, dass in Zukunft noch weitere Daten an die Facebook-Unternehmensgruppe übermittelt werden könnten. Auch die unklaren Beschreibungen der Datennutzung tragen nicht zur Beruhigung der Anwendenden bei. So gibt WhatsApp recht pauschal an: „Als Teil der Facebook-Unternehmensgruppe erhält WhatsApp Informationen von den Unternehmen dieser Unternehmensgruppe und teilt Informationen mit ihnen."[295] Der Inhalt von WhatsApp-Mitteilungen soll jedoch nach

293 Sog. Opt-In

294 https://www.whatsapp.com/faq/de/general/28030012

295 Rechtliche Hinweise / Verbundene Unternehmen unter https://www.whatsapp.com/legal

Angaben des Unternehmens vertraulich bleiben. Auch optionale Account-Informationen wie Profilnamen, Profilfotos oder Statusmeldungen sollen „im Moment" nicht mit Facebook geteilt werden.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ging aufgrund seiner Zuständigkeit für die deutsche Facebook-Niederlassung gegen die Weitergabe der Daten vor und hat diese per Verwaltungsanordnung Ende September untersagt. Noch ist unklar, wie Facebook und WhatsApp darauf im Einzelnen reagieren werden. Seit Anfang November wurde die Datenübermittlung laut eigenen Angaben von Facebook vorläufig gestoppt. Die Mutterfirma gab bekannt, dass man die Bedenken der Nutzerinnen und Nutzer sowie die Kritik von Daten- und Verbraucherschutz prüfen wolle, um danach zu entscheiden, wie man zukünftig damit umgehe.

Der Austausch von Daten zwischen WhatsApp, Facebook und weiteren Teilen der Unternehmensgruppe widerspricht den Versprechungen, die man 2014 gegenüber den Nutzenden und der Öffentlichkeit bei der Übernahme von WhatsApp abgegeben hat. Die weitere Entwicklung bleibt daher aufmerksam zu beobachten. Im persönlichen Bereich sollte auch die Anwendung alternativer, datenschutzfreundlicherer Alternativen in Betracht gezogen werden.

12.5 Zuständigkeit für Wikimedia e. V.

Häufig erreichen uns Anfragen, die die Veröffentlichung von personenbezogenen Daten bei der Online-Enzyklopädie „Wikipedia" betreffen. Die Webseite unter www.wikipedia.org wird von der Wikimedia Foundation Inc. mit Sitz in San Francisco/USA betrieben, d. h. von einer Stelle außerhalb unseres Zuständigkeitsbereichs. Gleichwohl wenden sich die Betroffenen an uns, weil die deutsche Länderorganisation der Wikimedia-„Bewegung",[296] die Wikimedia Deutschland Gesellschaft zur Förderung freien Wissens e. V., in Berlin niedergelassen ist.

296 So die Bezeichnung unter https://www.wikimedia.de/wiki/%C3%9Cber_uns

Nach unseren Erkenntnissen erhebt, verarbeitet oder nutzt der Wikimedia Deutschland e. V. keine personenbezogenen Daten in Deutschland. Der Verein unterhält zwar die Internetadresse www.wikipedia.de, nicht aber die Internetadresse www.wikipedia.org. Im Impressum von www.wikipedia.de wird darauf hingewiesen, dass Wikimedia Deutschland nicht Betreiber der Enzyklopädie Wikipedia (wikipedia.org) sei. Es gibt keine Anhaltspunkte dafür, an diesen Angaben zu zweifeln, da bei einer Suche über www.wikipedia.de immer ein Wechsel auf www.wikipedia.org erfolgt und sämtliche Inhalte nur über www.wikipedia.org abrufbar sind. Auf der Webseite www.wikipedia.de heißt es dazu: „Sämtliche Verweise auf Artikel werden automatisch aus dem Artikelbestand der Wikipedia gespeist und von Wikimedia Deutschland nicht ausgewählt oder beeinflusst. Die Verlinkung von Artikeln stellt keine Zueigenmachung des verlinkten Inhaltes dar. Eine Überprüfung der verlinkten Inhalte findet nicht statt."[297]

Gleichwohl haben wir uns die Frage gestellt, ob die neuere Rechtsprechung des Europäischen Gerichtshofs (EuGH) zur Anwendbarkeit des Datenschutzrechts eine andere Bewertung erforderlich macht. In der Entscheidung des EuGH zu Google Spain[298] ging es u. a. darum, ob das spanische Datenschutzrecht auch auf Datenverarbeitungen der Suchmaschine „Google" angewendet werden kann. Als Anknüpfungspunkt dafür diente u. a. die Tatsache, dass die US-amerikanische Google Inc. eine Tochtergesellschaft hat, die in Spanien niedergelassen ist.[299]

Übertragen auf Wikipedia lässt sich festhalten, dass keine gesellschaftsrechtliche Verbindung zwischen dem Wikimedia Deutschland e. V. und der Wikimedia Foundation Inc. besteht. Zudem handelt es sich bei Wikimedia Deutschland e. V. um einen unabhängigen Verein, sodass ein Abhängigkeitsverhältnis wie bei einer Niederlassung, Zweigstelle oder Agentur zweifelhaft ist.

Darüber hinaus ist zu berücksichtigen, dass der Wikimedia Deutschland e. V. die Ziele der Wikimedia Foundation Inc. zwar teilt und diese auch regional unterstützt, indem Spenden gesammelt und lokale Veranstaltungen durchgeführt werden sowie die „Bewegung" bekannt gemacht wird. Gleichwohl haben diese Aufgaben an-

297 Siehe www.wikipedia.de/imprint

298 EuGH, Urteil vom 13. Mai 2014, Rechtssache C-131/12

299 Zu den Einzelheiten im Übrigen siehe JB 2014, 11.3

ders als die Tätigkeiten der spanischen Google-Niederlassung keine unmittelbaren Bezüge bzw. Einflüsse auf die Veröffentlichungen unter www.wikipedia.org. Der EuGH hatte im o. g. Urteil die „Zurechnung“ der Datenverarbeitungen zu den Tätigkeiten der spanischen Google-Niederlassung u. a. darauf gestützt, dass die Niederlassung Werbeflächen auf der Webseite der Google-Suchmaschine, d. h. auf der Webseite der Google Inc., verkauft. Auf der Webseite www.wikipedia.de heißt es hingegen: „Auf die dort [unter wikipedia.org] von Freiwilligen erstellten Inhalte hat Wikimedia Deutschland keinen redaktionellen oder technischen Einfluss.“[300] Es werden auch keine Flächen auf der www.wikipedia.org-Webseite durch den deutschen Verein vermarktet.

Darüber hinaus gibt es eine gerichtliche Entscheidung, nach der sich die Wikipedia Foundation Inc. auf die Pressefreiheit berufen kann.[301] Vor diesem Hintergrund könnten die Veröffentlichungen auf www.wikipedia.org dem sog. Medienprivileg unterfallen. Dieses nimmt die journalistisch-redaktionelle und literarische Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu eigenen Zwecken weitgehend von den ansonsten einzuhaltenden Datenschutzbestimmungen nach dem BDSG aus, um die verfassungsrechtlich garantierte Presse- und Medienfreiheit zu schützen. Die für die Datenschutzaufsichtsbehörden vorgesehenen Kontrollkompetenzen nach dem BDSG sind daher in diesen Fällen nicht anwendbar.

Eine Zuständigkeit unserer Behörde für Veröffentlichungen auf wikipedia.org ist nicht gegeben.

12.6 Aus der Arbeit der „Berlin Group“

Die internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. Berlin Group) hat unter unserem Vorsitz in ihren Sitzungen am 24./25. April in Oslo (Norwegen) und am 22./23. November in Berlin zwei Arbeitspapiere verabschiedet.

300 Siehe www.wikipedia.de/imprint

301 Landgericht Tübingen, Urteil vom 18. Juli 2012 – 7 O 525/10

Bei dem **Arbeitspapier zu Datenschutz und Datensicherheit in der Internettelefonie (Voice over IP – VoIP) und verwandten Kommunikationstechnologien**[302] handelt es sich um eine Aktualisierung eines Arbeitspapiers, das die Berlin Group im Jahr 2006 verabschiedet hatte.[303] Das aktuelle Papier berücksichtigt die Entwicklungen der letzten zehn Jahre und passt die Empfehlungen an. Diese gelten nunmehr für alle Arten von Multimedia-Diensten, einschließlich Instant Messaging,[304] Real-Time Text[305] und Videodienste. Darüber hinaus unterscheidet das Arbeitspapier nicht zwischen einem VoIP-Dienst, der von einem Telekommunikationsdiensteanbieter angeboten wird, und dem Angebot eines „Over-The-Top"-Anbieters, da die Datenschutz- und Datensicherheitsrisiken trotz der Verwendung unterschiedlicher Technologien gleich bleiben. Das Papier erläutert den technischen Hintergrund und formuliert Empfehlungen für Gesetzgeber und Regulierungsbehörden sowie für VoIP-Anbieter, Software-Entwickler und Hardware-Hersteller. Den Nutzerinnen und Nutzern wird nahegelegt, sich über Sicherheits- und Datenschutzeigenschaften der verschiedenen Dienste zu informieren und diese danach auszuwählen. Zudem sollten sie sicherstellen, dass existierende Sicherheits- und Datenschutzmechanismen eines Dienstes vor dessen Nutzung aktiviert werden.

In dem **Arbeitspapier zu Biometrie in der Online-Authentifizierung**[306] werden Datenschutzrisiken erläutert, die beim Einsatz von biometrischen Verfahren entstehen können. Das Papier schließt mit Empfehlungen für Gesetzgeber, Regulierungs- und Aufsichtsbehörden, für Anbieter biometrischer Authentifizierungsverfahren, für Software-Entwickler und Hardware-Hersteller und für Nutzerinnen und Nutzer zum Umgang mit den aufgezeigten Risiken. Dabei wird den Anbietern solcher Verfahren dringend nahegelegt, immer ein nicht-biometrisches Authentifizierungsverfahren, das den Sicherheitsanforderungen genügt, als Alternative vorzusehen.

302 Dokumentenband 2016, S. 69

303 Dokumentenband 2006, S. 118

304 Dienste zur Echtzeitkommunikation von Nachrichten über das Internet, z. B. WhatsApp, Skype

305 Das ist ein Text, der von den Empfängern bereits gelesen werden kann, während er geschrieben wird.

306 Dokumentenband 2016, S. 77

13 Informationsfreiheit

13.1 Informationsfreiheit in Deutschland

Nach einer Entscheidung des Bundesverwaltungsgerichts vom letzten Jahr muss die Bundestagsverwaltung auf Antrag Zugang zu den Ausarbeitungen der Wissenschaftlichen Dienste des Deutschen Bundestags gewähren.[307] Inzwischen sind solche Anträge nicht mehr notwendig, da die Bundestagsverwaltung die Ausarbeitungen nunmehr vier Wochen nach Auslieferung an die Auftraggeber von sich aus im Internet veröffentlicht.[308] Vor diesem Hintergrund hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) die Verwaltungen der Landesparlamente aufgefordert, dem Beispiel der Bundestagsverwaltung in Sachen Transparenz und Open Data zu folgen und die Ausarbeitungen der jeweiligen Wissenschaftlichen Dienste bzw. der Gesetzgebungs- und Beratungsdienste unabhängig von individuellen Zugangsanträgen im Internet zu veröffentlichen.[309] Das Abgeordnetenhaus hat uns hierzu mitgeteilt, dass ohnehin geplant sei, die Ausarbeitungen des Wissenschaftlichen Parlamentsdienstes aktiv im Internet zu veröffentlichen, und lediglich noch Fragen der technischen Umsetzung zu klären seien. Die geplante Veröffentlichung wurde jedoch bisher noch nicht realisiert.

GovData[310] bietet einen einheitlichen zentralen Zugang zu offenen Verwaltungsdaten aus Bund, Ländern und Kommunen, die diese in ihren jeweiligen sog. Open Data-Portalen zugänglich gemacht haben. Das Portal wird auf der Grundlage einer Verwaltungsvereinbarung zwischen Bund und Ländern betrieben, der jedoch noch nicht alle Länder beigetreten sind. Viele Daten, an deren Veröffentlichung ein großes öffentliches Interesse besteht, sind daher zum jetzigen Zeitpunkt noch nicht abrufbar. Auch bewegt sich der Umfang und die Qualität der bereitgestellten

307 JB 2015, 16.1.1

308 www.bundestag.de/ausarbeitungen

309 Entschließung vom 28. April 2016: Auch die Verwaltungen der Landesparlamente sollen Gutachten der Wissenschaftlichen Dienste proaktiv veröffentlichen!, Dokumentenband 2016, S. 89

310 „GovData – das Datenportal für Deutschland", www.govdata.de

Daten auf unterschiedlichem Niveau. Die IFK hat daher an die noch verbleibenden Länder appelliert, der Verwaltungsvereinbarung beizutreten, und alle Beteiligten zur verstärkten Bereitstellung von Daten aufgefordert.[311]

Die Konferenz der Regierungschefinnen und Regierungschefs von Bund und Ländern hat im Oktober in Berlin beschlossen, in Bund und Ländern Open Data-Gesetze zu erlassen und dabei das Ziel zu verfolgen, bundesweit vergleichbare Standards für den Zugang zu öffentlichen Daten zu erreichen. Dieser Beschluss greift jedoch zu kurz, da die Bereitstellung von Rohdaten in standardisierten und offenen Formaten für sich genommen nicht genügt. Die Transparenz öffentlichen Handelns gebietet es vielmehr, zusammenhängende, aus sich heraus verständliche und nachvollziehbare Unterlagen zur Verfügung zu stellen. Vor diesem Hintergrund hat die IFK gefordert, die Behörden des Bundes und der Länder zu einer grundsätzlichen Veröffentlichung entsprechender Dokumente im Internet zu verpflichten. Derartige Regelungen sollen demnach nicht in Open Data- oder E-Government-Gesetze,[312] sondern vielmehr in Transparenzgesetze aufgenommen werden, die auch aus bestehenden Informationsfreiheitsgesetzen fortentwickelt werden können.[313]

13.2 Änderungen des Berliner Informationsfreiheitsgesetzes

Mit dem neuen Berliner E-Government-Gesetz[314] ist das Antragserfordernis nach dem Berliner Informationsfreiheitsgesetz (IFG) dahingehend erweitert worden, dass ein Antrag nicht nur mündlich oder schriftlich, sondern auch elektronisch gestellt werden kann,[315] und zwar auch mit einfacher und nicht qualifiziert elektronisch signierter E-Mail.

311 Entschließung vom 15. Juni 2016: GovData: Alle Länder sollen der Verwaltungsvereinbarung beitreten und Daten auf dem Portal bereitstellen!, Dokumentenband 2016, S. 90

312 Siehe 2.1

313 Entschließung vom 2. Dezember 2016: Nicht bei Open Data stehenbleiben: Jetzt auch Transparenzgesetze in Bund und Ländern schaffen!, Dokumentenband 2016, S. 91

314 Siehe 2.1

315 § 13 Abs. 1 IFG

Die öffentlichen Stellen des Landes Berlin sind bereits seit dem Inkrafttreten des IFG im Oktober 1999 verpflichtet, Verzeichnisse zu führen, die geeignet sind, die Aktenordnung und den Aktenbestand sowie den Zweck der geführten Akten erkennen zu lassen.[316] Darüber hinaus waren die öffentlichen Stellen auch bislang schon verpflichtet, diese Verzeichnisse sowie Register, Aktenpläne, Aktenordnungen, Aktenverzeichnisse, Einsendeverzeichnisse und Tagebücher allgemein zugänglich zu machen.[317] Dieser Verpflichtung wurde häufig dadurch nachgekommen, dass interessierte Bürgerinnen und Bürger die Verzeichnisse in den jeweiligen Diensträumen einsehen konnten. Wir veröffentlichen unsere Aktenordnung demgegenüber bereits seit August 2000 im Internet.[318] Seit Juli 2016[319] sind die öffentlichen Stellen nunmehr verpflichtet, die genannten Verzeichnisse nicht nur allgemein zugänglich zu machen, sondern auch im Internet zu veröffentlichen.[320] Wir werden zu gegebener Zeit überprüfen, inwieweit die öffentlichen Stellen dieser Verpflichtung nachkommen.

13.3 Einzelfälle

13.3.1 Beschwerliche Auskunft zu zwei Stiftungen

Eine Petentin begehrte von der Senatsverwaltung für Justiz und Verbraucherschutz bereits im Oktober 2015 Auskunft zu zwei Stiftungen, die beide Gesellschafterinnen eines als GmbH organisierten Diakoniewerks sind. Dabei interessierte sie sich insbesondere für die Satzungen sowie die Identität der Stifter und der Stiftungsratsmitglieder. Daraufhin erhielt sie zwar Kopien der Satzungen, die Auskunft zu den Identitäten wurde jedoch mit der Begründung abgelehnt, dass es sich um personenbezogene Daten handele, die nicht zu veröffentlichen seien.

316 § 17 Abs. 5 Satz 1 IFG
317 § 17 Abs. 5 Satz 2 IFG a. F.
318 datenschutz-berlin.de/content/berlin/berliner-beauftragter/aktenordnung
319 Viertes Gesetz zur Änderung des Berliner Informationsfreiheitsgesetzes vom 7. Juli 2016, GVBl. S. 434
320 § 17 Abs. 5 Satz 2 IFG n. F.

Der Offenbarung personenbezogener Daten stehen schutzwürdige Belange der Betroffenen in der Regel nicht entgegen, soweit sich aus einer Akte ergibt, dass die Betroffenen an einem Verwaltungsverfahren oder an einem sonstigen Verfahren beteiligt sind, eine gesetzlich oder behördlich vorgeschriebene Erklärung abgegeben haben, eine Anmeldung oder vergleichbare Mitteilung durch die Betroffenen gegenüber einer Behörde erfolgt ist und durch diese Angaben mit Ausnahme bestimmter Kerndaten (wie Namen und Anschrift) nicht zugleich weitere personenbezogene Daten offenbart werden.[321] Wir wiesen die Senatsverwaltung darauf hin, dass diese Regelbeispiele im Hinblick auf die Stifter und Stiftungsratsmitglieder erfüllt sein dürften. Auch bei einer Interessenabwägung dürfte das Informationsinteresse an der Identität der Stifter und Stiftungsratsmitglieder deren Interesse an der Geheimhaltung überwiegen. Wir baten deshalb um eine Überprüfung der ablehnenden Entscheidung.

Die Senatsverwaltung teilte uns daraufhin mit, dass die Petentin als Mitglied einer als Körperschaft des öffentlichen Rechts organisierten Kirchengemeinde einen eigenen Auskunftsanspruch aus der Verfassung dieser Gemeinde gegenüber dem Diakoniewerk habe, der nicht durch das IFG umgangen werden dürfe. Selbst bei Anwendbarkeit des IFG könne die begehrte Auskunft nicht erteilt werden, da die gewünschten Informationen einerseits nicht dem Zweck dienten, über die bestehenden Informationsmöglichkeiten hinaus die demokratische Meinungs- und Willensbildung zu fördern und eine Kontrolle des staatlichen Handelns zu ermöglichen,[322] andererseits die Petentin überwiegend Privatinteressen verfolge.[323] Deshalb dürften die begehrten personenbezogenen Daten nicht veröffentlicht werden.

Die Auffassung, dass der Auskunftsanspruch nach dem IFG durch die Verfassung der Kirchengemeinde verdrängt werden kann, findet im Gesetz keine Stütze. Zwar können spezialgesetzliche Ansprüche auf Informationszugang dem IFG vorgehen bzw. dessen Anwendbarkeit ausschließen, nicht jedoch die „untergesetzliche" Verfassung der Kirchengemeinde. Auch kommt es nicht darauf an, ob die Petentin Mitglied dieser Kirchengemeinde ist, da es bei der Entscheidung über den Aus-

321 § 6 Abs. 2 Satz 1 Nr. 1 a) und b) IFG
322 § 1 IFG
323 § 6 Abs. 1 IFG

kunftsanspruch nicht auf die Person der Antragstellerin ankommt. Im Übrigen ist der Informationszugang in dem beantragten Umfang zu gewähren, wenn keine der im zweiten Abschnitt des IFG geregelten Ausnahmen Anwendung findet,[324] sodass eine Einschränkung des Anspruchs auf Informationszugang unter Heranziehung des Gesetzeszwecks ausscheidet. Bei dem Merkmal der überwiegenden Verfolgung von Privatinteressen[325] handelt es sich um einen bloßen Auffangtatbestand für Fälle offensichtlichen Missbrauchs wie etwa Rache, Schikane oder Ähnliches. Jede antragstellende Person verfolgt mit ihrem Informationszugangsbegehren in der Regel jedenfalls auch private Interessen. Dies ist nach ständiger Rechtsprechung des Verwaltungsgerichts Berlin jedoch unschädlich, da diese Person in der Regel als Sachwalter der Allgemeinheit zugleich auch deren Informationsinteresse wahrnimmt. Wir regten daher eine erneute Überprüfung der ablehnenden Entscheidung an.

Die Senatsverwaltung schloss sich daraufhin unserer Rechtsauffassung an und gab den Stiftern sowie den Stiftungsratsmitgliedern Gelegenheit, zur beabsichtigten Gewährung der Aktenauskunft Stellung zu nehmen.[326] Nach Eingang der Stellungnahmen entschied die Senatsverwaltung, der Petentin die gewährte Aktenauskunft zu gewähren, und gab diese Entscheidung auch den Stiftern sowie den Stiftungsratsmitgliedern bekannt.[327] Diese legten hiergegen Widerspruch ein.[328] Nach Zurückweisung der Widersprüche durch die Senatsverwaltung erhoben die Stifter und Stiftungsratsmitglieder Ende des Jahres Klage vor dem Verwaltungsgericht. Der Ausgang des gerichtlichen Verfahrens bleibt abzuwarten.

Wird Informationszugang zu personenbezogenen Daten begehrt, hat die öffentliche Stelle eine Abwägung zwischen dem schutzwürdigen Interesse der Betroffenen an der Geheimhaltung und dem Informationsinteresse der Allgemeinheit vorzunehmen. Die Betroffenen haben das Recht, sich zu den entscheidungserheblichen Tatsachen zu äußern und Rechtsmittel gegen die Entschei-

324 § 4 Abs. 1 IFG
325 § 6 Abs. 1 IFG
326 § 14 Abs. 2 Satz 1 IFG
327 § 14 Abs. 2 Satz 2 IFG
328 § 14 Abs. 2 Satz 5 IFG

dung einzulegen. Der Informationszugang darf erst nach Bestandskraft dieser Entscheidung[329] gewährt werden.

13.3.2 Unzumutbarer Umgang mit dem IFG beim Landesamt für Bürger- und Ordnungsangelegenheiten

Im Februar 2012 begehrte ein Petent beim Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) Akteneinsicht in verschiedene Unterlagen zur Handhabung ausländerrechtlicher Verfahren. Dies lehnte das LABO im Juni 2012 ab. Zur Begründung wurde ausgeführt, dass der Petent sein Informationsinteresse nicht dargelegt habe, überwiegend Privatinteressen verfolge,[330] die Informationen beruflich nutzen wolle und diese einen wirtschaftlichen Nutzen für ihn hätten. Außerdem sei der Willensbildungsprozess innerhalb von Behörden[331] tangiert. Im Übrigen stünden Gründe der Verhältnismäßigkeit entgegen, da eine Abwägung zwischen dem Informationsinteresse des Antragstellers bzw. der Allgemeinheit mit dem Arbeitsaufwand der öffentlichen Stelle zu erfolgen habe und deren Funktionsfähigkeit insoweit nicht mehr gewährleistet werden könne. Hiergegen legte der Petent im Juli 2012 Widerspruch ein, den er im Januar 2013 sowie ergänzend im Dezember 2014 begründete. Auf seine wiederholten Nachfragen zum Sachstand im Dezember 2014 sowie im Februar und Juni 2015 wurde er jeweils um Geduld gebeten, da ältere Widerspruchsverfahren vorrangig behandelt würden. Eine Bescheidung des Widerspruchs erfolgte nicht.

Die Argumentation des LABO findet im Gesetz keine Stütze. Weder ist ein Antragsteller dazu verpflichtet, seinen Antrag auf Akteneinsicht zu begründen bzw. sein Informationsinteresse darzulegen, noch ist die öffentliche Stelle dazu befugt, vom Antragsteller eine entsprechende Begründung bzw. Darlegung zu verlangen. Zudem waren keinerlei Anhaltspunkte dafür erkennbar, dass der Petent überwie-

329 Oder zwei Wochen nach Anordnung der sofortigen Vollziehung, siehe § 14 Abs. 2 Satz 4
330 § 6 Abs. 1 IFG
331 § 10 Abs. 4 IFG

gend Privatinteressen verfolgen könnte.[332] Ferner ist nicht von Belang, ob der Antragsteller mit der Akteneinsicht berufliche Interessen verfolgt und die begehrten Informationen für ihn einen wirtschaftlichen Nutzen haben, da im IFG kein entsprechender Ausschlussgrund normiert ist. Vom Willensbildungsprozess innerhalb von Behörden sind im Übrigen nur der eigentliche Vorgang der behördlichen Entscheidungsfindung (also die Besprechungen, Überlegungen und Abwägungen) geschützt, nicht jedoch die Grundlagen und das Ergebnis der Willensbildung. Auch enthält das IFG weder einen Ausschlussgrund, um die Akteneinsicht wegen eines unverhältnismäßigen Verwaltungsaufwands abzulehnen, noch sieht es eine Abwägung zwischen dem zu erwartenden Verwaltungsaufwand und dem Informationsinteresse der antragstellenden Person bzw. der Allgemeinheit vor.

Dessen ungeachtet verstieß aber auch der Umgang mit dem Informationszugangsbegehren des Petenten gegen den Zweck des IFG, durch ein umfassendes Informationsrecht das in Akten festgehaltene Wissen und Handeln öffentlicher Stellen unmittelbar der Allgemeinheit zugänglich zu machen, um über die bestehenden Informationsmöglichkeiten hinaus die demokratische Meinungs- und Willensbildung zu fördern und eine Kontrolle des staatlichen Handelns zu ermöglichen.[333] Dieses Informationsrecht kann nur dann wirksam in Anspruch genommen werden, wenn die öffentlichen Stellen auch in angemessener Zeit über Anträge und Widersprüche entscheiden und die Bearbeitung nicht um Monate oder sogar Jahre verzögern. Über Anträge auf Informationszugang ist unverzüglich, also ohne schuldhaftes Zögern, zu entscheiden.[334] Auch über hiermit im Zusammenhang stehende Widersprüche ist unverzüglich zu entscheiden, wenn nicht im Einzelfall stichhaltige Gründe für diese Verzögerung bestehen. Die Nichtbescheidung eines Widerspruchs über einen Zeitraum von nahezu dreieinhalb Jahren ist jedoch unter keinem Gesichtspunkt hinnehmbar.

Wir wiesen das LABO auf diese Rechtslage hin und baten darum, nunmehr unverzüglich über den Widerspruch des Petenten zu entscheiden. Rund acht Wochen später, insgesamt knapp vier Jahre nach der ursprünglichen Antragstellung, gab

332 Zur überwiegenden Verfolgung von Privatinteressen siehe auch 13.3.1

333 § 1 IFG

334 § 14 Abs. 1 Satz 1 IFG

das LABO dem Widerspruch statt und gewährte dem Petenten die Akteneinsicht ohne Einschränkung.

Über Anträge auf Informationszugang ist ebenso wie über Widersprüche gegen ablehnende Entscheidungen unverzüglich zu entscheiden. Der Informationszugang darf nur dann verweigert werden, wenn und soweit eine der im IFG abschließend geregelten Ausnahmen Anwendung findet,[335] keinesfalls jedoch wegen des zu erwartenden Verwaltungsaufwands.

13.3.3 (Keine) Akteneinsicht nach dem IFG beim Bezirksamt Charlottenburg-Wilmersdorf?

Eine Petentin bat das Bezirksamt Charlottenburg-Wilmersdorf im Oktober 2015 um Auskunft zu den Verfahrensbeteiligten sowie zum Stand bzw. Ausgang eines Zweckentfremdungsverfahrens. Da sie hierauf keine Antwort erhielt, bat sie im November 2015 sowie erneut im Januar 2016 um Bescheidung ihres Antrags. Im Februar wurde ihr Antrag mit der Begründung abgelehnt, dass sie keinen Anspruch auf die begehrte Auskunft habe, da sie keine Verfahrensbeteiligte[336] sei.

Diese Verweigerung der Akteneinsicht ist rechtlich nicht haltbar. Zwar hat die Behörde den Beteiligten an einem Verwaltungsverfahren nach dem VwVfG Berlin Einsicht in die das Verfahren betreffenden Akten zu gestatten.[337] Auf die Frage, ob die Petentin Beteiligte an dem Zweckentfremdungsverfahren ist, kam es jedoch nicht an. Denn jeder Mensch hat nach Maßgabe des IFG ein eigenständiges Recht auf Einsicht in oder Auskunft über den Inhalt der von der öffentlichen Stelle geführten Akten.[338] Zur Klarstellung enthält das VwVfG Berlin sogar eine Regelung, wonach für Nichtbeteiligte das IFG gilt;[339] dies hatte das Bezirksamt wohl übersehen. Wir forderten es daher auf, erneut auf der Grundlage des IFG über den Antrag der Petentin zu entscheiden.

335 § 4 Abs. 1 IFG
336 § 1 Abs. 1 Verwaltungsverfahrensgesetz (VwVfG) Berlin i. V. m. § 13 VwVfG Bund
337 § 6 Abs. 1 Satz 1 VwVfG Berlin
338 § 3 Abs. 1 Satz 1 IFG
339 § 6 Abs. 4 VwVfG Berlin

Als wir weder auf dieses Schreiben noch auf eine Erinnerung eine Antwort erhielten, forderten wir zunächst die Leitung des Amts für Bürgerdienste unter ausdrücklichem Hinweis auf die Unterstützungspflicht[340] erneut zu abschließender Beantwortung auf. Nachdem das Bezirksamt auch die hier gesetzte Frist verstreichen ließ, wandten wir uns an den Bezirksbürgermeister und drohten für den Fall der fortdauernden Nichtbeantwortung eine Beanstandung[341] an.

Das Bezirksamt sagte uns daraufhin zu, der Petentin den begehrten Informationszugang nunmehr nach dem IFG zu gewähren.

Öffentliche Stellen müssen von sich aus alle Rechtsgrundlagen prüfen, die für die Gewährung von Informationszugang in Betracht kommen. Insbesondere wenn spezialgesetzlich normierte Ansprüche auf Informationszugang daran scheitern, dass deren Voraussetzungen nicht erfüllt sind, ist zwingend zu prüfen, ob der begehrte Informationszugang stattdessen nach dem IFG gewährt werden kann.

13.3.4 Schleppende Auskunft zur Sanierung der Yorckbrücke 5

Ein Petent bat das Bezirksamt Tempelhof-Schöneberg im Mai 2015 um Auskunft zu den Kosten der Sanierung der Yorckbrücke 5, insgesamt und aufgeschlüsselt nach Gewerken. Das Bezirksamt reagierte weder auf diesen Antrag noch auf mehrfache Erinnerungen im Juni, Juli und September 2015. Erst auf eine Erinnerung des Petenten im Januar 2016 wurde ihm mitgeteilt, dass aus Gründen des absehbar hohen Rechercheaufwands und der begrenzten Arbeitskapazitäten eine Beantwortung der Frage zurzeit nicht leistbar sei. Auf seine weiteren Erinnerungen im Februar, März und April 2016 erfolgte keine Reaktion mehr.

340 § 28 BlnDSG
341 § 26 BlnDSG

Dieser Umgang mit dem Informationszugangsbegehren des Petenten verstieß gegen den Zweck des IFG.[342] Wir wiesen das Bezirksamt darauf hin, dass eine Bearbeitungsdauer von mehr als 13 Monaten unter keinen Umständen mit der Pflicht vereinbar ist, unverzüglich über Anträge auf Informationszugang zu entscheiden.[343] Wir forderten das Bezirksamt daher auf, unverzüglich über den Antrag zu entscheiden, und stellten in Aussicht, eine fortdauernde Nichtbescheidung des Antrags zu beanstanden.[344]

Erst nach unserer Erinnerung übersandte das Bezirksamt uns schließlich die überraschende Antwort an den Petenten, dass die Daten zur Sanierung der Yorckbrücke 5 bei ihnen nicht in der gewünschten Differenziertheit vorlägen und er sich daher direkt an die DB Netz AG wenden möge.

Der Petent bat das Bezirksamt daraufhin um Einsicht in alle dort zur Sanierung der Yorckbrücke 5 vorhandenen Unterlagen.

Wir wiesen das Bezirksamt darauf hin, dass die DB Netz AG nicht dem IFG unterliegt[345] und der Petent daher lediglich einen Anspruch auf Informationszugang gegenüber dem Bezirksamt, nicht jedoch gegenüber der DB Netz AG hat. Dessen ungeachtet machten wir das Bezirksamt für zukünftige Fälle darauf aufmerksam, dass ein Antrag, der schriftlich bei einer unzuständigen öffentlichen Stelle gestellt wurde, unverzüglich an die zuständige Stelle weiterzuleiten und die antragstellende Person entsprechend zu unterrichten ist,[346] sie also gerade nicht darauf verwiesen werden darf, selbst einen Antrag bei der zuständigen Stelle zu stellen.

Das Bezirksamt gewährte dem Petenten die begehrte Akteneinsicht schließlich nach mehr als 14 Monaten seit seiner ursprünglichen Antragstellung.

Über Anträge auf Informationszugang ist unverzüglich, also ohne schuldhaftes Zögern zu entscheiden. Dabei ist insbesondere unverzüglich zu prüfen, ob die

342 Zu den Einzelheiten siehe 13.3.2
343 § 14 Abs. 1 Satz 1 IFG
344 § 26 BlnDSG
345 § 2 Abs. 1 Satz 1 IFG
346 § 13 Abs. 1 Satz 4 IFG

begehrten Informationen überhaupt vorhanden sind. Ist dies nicht der Fall, der öffentlichen Stelle jedoch bekannt, bei welcher informationspflichtigen Stelle die Informationen zu finden sind, ist der Antrag unverzüglich dorthin weiterzuleiten und der Antragsteller entsprechend zu unterrichten.[347]

347 § 13 Abs. 1 Satz 4 IFG

14 Aus der Dienststelle

14.1 Entwicklungen

Nach dem Umzug in die Friedrichstraße im Jahr 2015 gab es erneut einige grundlegende Veränderungen und Herausforderungen.

Mit der Wahl der neuen Berliner Beauftragten für Datenschutz und Informationsfreiheit am 28. Januar 2016 erfolgte auch ein Wechsel der Dienststellenleitung. Die Übergabe der Amtsgeschäfte verlief reibungslos, unterstützt durch das vorhandene sehr kompetente und hoch motivierte Team von Dienstkräften auf allen Ebenen.

Natürlich führte der Wechsel in der Dienststellenleitung auch zu neuen Schwerpunktsetzungen. Definiert wurden vor allem drei Bereiche: Die Förderung der Medienkompetenz von Kindern und Jugendlichen im Bereich des Datenschutzes, die Beratung von Start-up-Unternehmen sowie der große Bereich der Gesundheitsverwaltung, die im Zuge der Digitalisierung sämtlicher Lebens- und Arbeitsbereiche auch vor riesigen datenschutzrechtlichen Herausforderungen steht.

Die Förderung von Schlüsselkompetenzen bei Kindern und Jugendlichen zum sicheren Umgang mit sozialen Medien wird zunehmend als Teil des Bildungsauftrages gesehen. Dabei werden jedoch datenschutzrechtliche Aspekte nur untergeordnet berücksichtigt. Trotz der begrenzten Personalressourcen in der Dienststelle haben wir in Anbetracht der Bedeutung des Themas eine Medienpädagogin (zunächst befristet für zwei Jahre) für die Entwicklung von kind- und jugendgerechten Angeboten zum Medienschutz unter Einbeziehung datenschutzrechtlicher Fragestellungen eingestellt. Angesichts der Wichtigkeit dieser Aufgabe für die Zukunft wird angestrebt, im Haushalt 2018/2019 eine feste Stelle für die dauerhafte Beschäftigung dieser Fachkraft zu schaffen.

In den vergangenen Jahren war die ständig wachsende Zahl von Eingaben, Beratungsersuchen von Behörden und Unternehmen, Prüfungen von Amts wegen

und sonstigen Aufgaben von der Dienststelle kaum zu bewältigen. Mit Inkrafttreten der EU-Datenschutz-Grundverordnung im Mai 2016[348] hat sich die Situation dramatisch verschärft. Durch die kurze Umsetzungsfrist von nur zwei Jahren bis zu ihrer unmittelbaren Anwendbarkeit ab Mai 2018 sind die Mitarbeiterinnen und Mitarbeiter der Dienststelle bereits jetzt mit äußerst arbeitsintensiven Vorbereitungen auf die neue Rechtslage befasst. In den Arbeitskreisen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) und den Arbeitsgruppen des Düsseldorfer Kreises sind sie damit beschäftigt, Orientierungshilfen zu überarbeiten und Rechtsfragen zu klären, die durch die Datenschutz-Grundverordnung entstanden sind. Parallel dazu werden die Umsetzungsmaßnahmen in den Gremien auf Bundes-, Landes- und europäischer Ebene aktiv begleitet. Hinzu kommt eine steigende Anzahl von Beratungsersuchen zur Grundverordnung durch Berliner Behörden und Unternehmen. Auch auf Leitungsebene ist eine erhebliche Zunahme des Abstimmungsbedarfs zwischen den Aufsichtsbehörden von Bund und Ländern zur politisch-fachlichen Vorbereitung der neuen rechtlichen Lage zu verzeichnen. Im Gegensatz zur bisherigen Rechtslage wird es mit der unmittelbaren Anwendbarkeit nach Ablauf der zweijährigen Übergangsfrist der Datenschutz-Grundverordnung zu einer wesentlich engeren Zusammenarbeit zwischen den deutschen Aufsichtsbehörden untereinander kommen müssen, um europäische Abstimmungsprozesse innerhalb der vorgegebenen sehr kurzen Zeiträume auf nationaler Ebene vorzubereiten. Zusätzlich wird es erforderlich werden, sich auch zwischen den EU-Mitgliedstaaten abzustimmen. All dies erfordert neue Strukturen, die bereits jetzt vorbereitet werden müssen – ohne dass es für eine derart enge Zusammenarbeit in einem Fachgebiet auf europäischer Ebene schon Beispiele gäbe. Die Aufsichtsbehörden befinden sich dementsprechend schon heute in engster Abstimmung, um im Mai 2018 über ein möglichst funktionsfähiges Verfahren zu verfügen.

In Reaktion auf die Zunahme an Aufgaben und die damit verbundene Arbeit wurde die bisherige Organisationsstruktur der Dienststelle grundlegend geändert. Durch die Einrichtung von Referaten wurden Verantwortungs- und Entscheidungsbefugnisse dezentral auf entsprechend qualifizierte Mitarbeiterinnen und Mitarbeiter übertragen. Interne Arbeitsabläufe konnten dadurch optimiert und zeitlich reduziert werden. Um die Fachdezernate von Routinearbeiten zu befreien, wurde

348 Siehe 1.2

die Erledigung von zentralen Verwaltungsaufgaben (z. B. bei der Bearbeitung von Bürgereingaben oder im Sanktionsbereich) sog. Servicestellen zugeordnet.

Bereits jetzt zeichnet sich ab, dass diese Maßnahmen nicht ausreichen werden, um die zukünftigen Aufgaben, die mit der Umsetzung und Anwendung der Datenschutz-Grundverordnung verbunden sind, angemessen zu erfüllen. Dies wird nur mit einem erheblichen Zuwachs an Personal im Doppelhaushalt 2018/19 zu schaffen sein. Dabei ist leider festzustellen, dass es zunehmend schwieriger wird, sowohl in den juristischen Bereichen als auch im Bereich der Informatik hochqualifizierte Referentinnen und Referenten langfristig an die Dienststelle zu binden. Hier macht sich die unmittelbare Konkurrenz zu den in Berlin ansässigen Bundesbehörden bemerkbar. Auch im Berichtszeitraum mussten wir erneut den Wechsel von zwei erfahrenen Dienstkräften in die Bundesverwaltung durch die Einstellung von Berufseinsteigern kompensieren.

14.2 Zusammenarbeit mit dem Abgeordnetenhaus von Berlin

Der Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit tagte in zehn Sitzungen, in denen die Berliner Beauftragte für Datenschutz und Informationsfreiheit Empfehlungen zu verschiedenen Themen geben konnte. Dazu gehörten das neue Anliegenmanagement (AMS),[349] die Ermöglichung des freien WLAN nach Änderung des Telemediengesetzes,[350] vor allem aber die Diskussion um das Berliner E-Government-Gesetz,[351] das nach jahrelangen Beratungen kurz vor Ende der 17. Legislaturperiode verabschiedet wurde.[352] In die Ausschussarbeit eingebracht haben wir auch unsere Anmerkungen zum Gesetzentwurf zur Ausführung des Bundesmeldegesetzes.[353]

349 Siehe 2.2 und Inhaltsprotokoll ITDat 17/67 vom 15. Februar 2016, S. 9 ff.

350 Inhaltsprotokoll ITDat 17/69 vom 14. März 2016, S. 1 ff.

351 Wortprotokoll ITDat 17/70 vom 11. April 2016, S. 1 ff. und Inhaltsprotokoll ITDat 17/72 vom 9. Mai 2016, S. 2 ff.

352 Siehe 2.1

353 Siehe 3.1 und Inhaltsprotokoll ITDat 17/73 vom 23. Mai 2016, S. 6 ff.

Das Abgeordnetenhaus hat nach den Wahlen von Mitte September beschlossen, die inhaltlichen Fragestellungen unserer Behörde wieder in einem eigenen, dem Innenausschuss zugeordneten Unterausschuss zu behandeln. Dieser neue „Unterausschuss für Datenschutz, Informationsfreiheit und zur Umsetzung von Artikel 13 Abs. 6 GG sowie § 25 Abs. 10 ASOG" (kurz: UA Dat/G13) wird mit zwölf Mitgliedern besetzt werden.

14.3 Zusammenarbeit mit anderen Stellen

Die **Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)** tagte am 6./7. April in Schwerin und am 9./10. November in Kühlungsborn unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern und fasste zahlreiche Entschließungen zu aktuellen Fragen des Datenschutzes.[354] Aufgrund der Beratungen zur neuen EU-Datenschutz-Grundverordnung und der Vorbereitung eines darauf abgestimmten neuen Bundesdatenschutzgesetzes fanden darüber hinaus am 27. Januar in Frankfurt am Main sowie am 21. März, 31. Mai, 28. Juli, 22. September und 11. Oktober in Berlin insgesamt sechs Sondersitzungen der DSK statt, ebenfalls unter dem Vorsitz Mecklenburg-Vorpommerns. Für 2017 hat die Landesbeauftragte für den Datenschutz Niedersachsen den Vorsitz in der Konferenz übernommen. Neben diesen Sitzungen der gesamten DSK fanden noch eine Reihe weiterer Beratungsrunden teilweise auf Einladung oder unter Beteiligung der jeweils zuständigen Bundesministerien zur Vorbereitung des neuen Bundesdatenschutzgesetzes statt, an denen jeweils nur die Leitungen einzelner Datenschutzaufsichtsbehörden teilnahmen.

Der **Düsseldorfer Kreis**, in dem unter dem Vorsitz der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich zusammenarbeiten, fasste einen Beschluss zur Fortgeltung bisher erteilter Einwilligungen unter der EU-Da-

354 Dokumentenband 2016, S. 12 ff.

tenschutz-Grundverordnung und verabschiedete eine Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen.[355]

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland** tagte am 15. Juni und am 2. Dezember in Düsseldorf unter dem Vorsitz der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und fasste Entschließungen zugunsten von mehr Transparenz durch aktives Bereitstellen von Informationen durch die Landesparlamente und Verwaltungen.[356] 2017 wird der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz den Vorsitz in dieser Konferenz übernehmen.

Auf Einladung der Nationalen Behörde für Datenschutz und Informationsfreiheit Ungarns fand am 26./27. Mai die **Europäische Konferenz der Datenschutzbeauftragten** in Budapest statt. Es wurden Entschließungen zu einer noch stärkeren Zusammenarbeit der Aufsichtsbehörden in Europa nicht nur vor dem Hintergrund der EU-Datenschutz-Grundverordnung gefasst, sondern auch im Hinblick auf grenzüberschreitende Datenflüsse, bei denen die Aufrechterhaltung der Rechte der Betroffenen und die Stärkung des öffentlichen Bewusstseins für diese Rechte von besonderer Bedeutung sind.[357] Wir nahmen an dieser Konferenz nicht persönlich teil, sondern erstatteten nur schriftlich Bericht über die Arbeitsergebnisse der sog. Berlin Group.

Auf Einladung der Datenschutzbehörde Marokkos fand die **38. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre** vom 17. bis zum 20. Oktober in Marrakesch statt. Es wurden Entschließungen gefasst zur Datenschutzerziehung in Schulen, zur Entwicklung neuer Messgrößen für die Datenschutzregulierung, zum Schutz von Menschenrechtsverteidigern und zur Weiterentwicklung der internationalen Zusammenarbeit der Datenschutzaufsichtsbehörden.[358] Unser dort vorgetragener Bericht über die Arbeitsergebnisse der sog. Berlin Group stieß auf große Aufmerksamkeit.

355 Dokumentenband 2016, S. 41 ff.
356 Dokumentenband 2016, S. 89 ff.
357 Dokumentenband 2016, S. 53 ff.
358 Dokumentenband 2016, S. 58 ff.

Die **„Berlin Group“** tagte unter unserem Vorsitz am 24./25. April im norwegischen Oslo und verabschiedete dort ein Arbeitspapier, mit dem ein früheres[359] zum Thema Datenschutz und Datensicherheit bei der Internet-Telefonie aktualisiert wurde.[360] Bei ihrer Sitzung am 22./23. November in Berlin beschloss die Gruppe ein Arbeitspapier zu Biometrie in der Online-Authentifizierung.[361]

Erneut erhielten wir Besuch von mehreren ausländischen Delegationen, die sich in unserer Dienststelle über praktische Fragen der Datenschutzkontrolle informierten. Dazu gehörten Vertreter aus der Volksrepublik China sowie aus den USA.

14.4 Öffentlichkeitsarbeit

Am 28. Januar fand auf Einladung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eine zentrale Veranstaltung im Dominikanerkloster in Frankfurt am Main aus Anlass des 10. Europäischen Datenschutztages statt. Das Thema lautete „Europäisches Datenschutzrecht – Vielfalt in der Kohärenz“.

Neben der umfangreichen Prüf- und Beratungstätigkeit, der zeitnahen Kommentierung von Gesetzen und Verordnungen, dem fachlichen Austausch mit Kolleginnen und Kollegen auf nationaler und internationaler Ebene leisten sowohl die Berliner Beauftragte für Datenschutz und Informationsfreiheit als auch ihre Mitarbeiterinnen und Mitarbeiter eine vielfältige Vortragstätigkeit im Rahmen unterschiedlichster Veranstaltungen und Schulungen. Dazu einige Beispiele:

Am 4. Mai nahmen wir an einer **Podiumsdiskussion der Bundesstiftung zur Aufarbeitung der SED-Diktatur im Rahmen der Reihe „Deutschland 2.0“ mit dem Titel „Deutschland 2.0: Stasi reloaded – Leben wir in einem neuen Überwachungsstaat?“** teil, in der versucht wurde, die aktuelle Debatte in einen geschichtlichen Kontext zu setzen und danach zu fragen, wo die Unterschiede liegen zwischen der

359 Dokumentenband 2006, S. 118
360 Dokumentenband 2016, S. 69
361 Dokumentenband 2016, S. 77

„Stasi“ der DDR und der aktuellen Arbeit von Geheimdiensten oder der massiven Datennutzung von gewinnorientierten Wirtschaftsunternehmen.

Am 23. Juni beteiligten wir uns am **Workshop „Chancen und Risiken von Smart Cams im öffentlichen Raum“**, einer Veranstaltung des Datenschutzbeirats der Deutschen Bahn AG. Am Beispiel der Smart Cams wurde die Problematik der Videoüberwachung im öffentlichen Raum durch Private aus der Sicht einer Aufsichtsbehörde beleuchtet und auf die vielen Eingaben hingewiesen, die sich auf Bildaufnahmen beziehen.

In einem **Vortrag auf der Betriebs- und Personalrätekonferenz** am 5. Oktober wurden die Funktion und die Aufgaben unserer Behörde vorgestellt und Einzelfragen zum Beschäftigtendatenschutz wie Umgang mit Outlook-Kalendern, Personalakten und Gesundheitsdaten näher behandelt.

Die Teilnahme an Expertengesprächen zu den Themen **„Datenschutzerklärungen bei Internetanbietern“** und **„Datenschutz in der Arztpraxis“** fand in zwei ausführlichen Artikeln in der März-Ausgabe der Zeitschrift Stiftung Warentest ihren Ausdruck.

Zahlreiche Vorträge zum Thema Datenschutz in der Medizin befassten sich mit dem Erfordernis besonderer Umsicht im Umgang mit sensitiven medizinischen Daten. So wurde z. B. auf der **Fachtagung „Datenschutz in der Medizin – Update 2016“** am 10. November auf kritische Datenschutzdefizite im Gesundheitssektor hingewiesen, die durch Erfahrungen aus unserer Prüfpraxis als Aufsichtsbehörde belegt werden können.

Auch für eine Spezialschulung für Beschäftigtenvertretungen der Berliner Justiz, die die Deutsche Justizgewerkschaft angeboten hatte, standen wir zur Verfügung. Die aktuelle Sachlage erfordert es, die Beschäftigtenvertretungen zu informieren, auf welche datenschutzrechtlichen Bestimmungen sie in Verfahren der **„Einbestellung zur amtsärztlichen Untersuchung von Beschäftigten“** zu achten haben. Die Schulung fand am 8. Juni statt.

Das Sozialpädagogische Fortbildungsinstitut Berlin-Brandenburg (SFBB) bietet in seinem **Schulungsangebot** Veranstaltungen **für pädagogische Fachkräfte in der**

Jugendhilfe im Strafverfahren an. Da im Bereich der Kinder- und Jugenddelinquenz auch das Thema Datenschutz eine wichtige Rolle spielt, hat eine Mitarbeiterin dort als Dozentin mitgewirkt. In diesem Jahr fand die Veranstaltung am 27. September statt.

Häufig werden wir im Bereich der Kinder- und Jugendhilfe gebeten, Vorträge zum Datenschutz für die in diesem Tätigkeitsfeld beschäftigten Fachkräfte zu halten. In diesem Jahr haben wir am 16. November eine Fortbildung zum Thema **„Datenschutz und Kinderschutz"** durchgeführt.

Jedes Jahr im November startet die Vorlesungssaison der KinderUni Lichtenberg (KUL). Es gibt Vorträge aus verschiedenen Fachgebieten der Hochschule für Technik und Wirtschaft und der Hochschule für Wirtschaft und Recht für Kinder ab acht Jahren. Parallel finden Veranstaltungen für Eltern statt. Am 19. November konnten sie einen Vortrag zum Thema „Check: WhatsApp – Worauf Eltern und Kinder achten sollten" besuchen und sich umfassend über Risiken und Gefahren bei der Verwendung von WhatsApp informieren. Im Rahmen der mobilen Vorlesungsreihe „KUL unterwegs" bieten wir außerdem regelmäßige Veranstaltungen zum Thema **„Soziale Netzwerke und Datenschutz – Facebook, Twitter, WhatsApp & Co."** für Kinder an. Die Vorträge können jedoch auch für Jugendliche gebucht werden.[362]

Außerdem sind einige Mitarbeiter immer wieder nebenberuflich als Dozenten an der Verwaltungsakademie Berlin und der Hochschule für Wirtschaft vor allem im Bereich der **IT-Sicherheit** und der **Informationsfreiheit** tätig, um auch auf diese Weise ihr Wissen an möglichst große Bevölkerungskreise weiterzugeben.

Schließlich sind wir im Bereich der Öffentlichkeitsarbeit dabei, die Umgestaltung und Modernisierung der **Außendarstellung** der Dienststelle der Berliner Beauftragten für Datenschutz und Informationsfreiheit in Angriff zu nehmen. Wir haben mit der Neugestaltung des bisherigen Corporate Designs bereits begonnen. Das neue Logo und der vorliegende Tätigkeitsbericht sind Teile dieses Konzepts und wurden in diesem Jahr realisiert. Die komplette Überarbeitung unserer veralteten Webseite, die heutigen Ansprüchen in keiner Weise mehr genügt, wird der nächste Schritt sein.

362 Nähere Informationen unter http://kul-unterwegs.de/angebot/neue-medien

Anhang

Rede der Berliner Beauftragten für Datenschutz und Informationsfreiheit am 12. Januar 2017 im Abgeordnetenhaus von Berlin zum Jahresbericht 2015

Sehr geehrte Frau Präsidentin,
sehr geehrte Damen und Herren,

ich freue mich sehr, dass ich Ihnen hier einige Aspekte meines Jahresberichts 2015 vorstellen kann, mit dem Sie sich heute befassen wollen.

Vielleicht aus aktuellem Anlass kurz vorweg: Auch 2015 gab es bereits eine Diskussion über eine Ausweitung der Videoüberwachung aus Gründen der inneren Sicherheit. Diese Diskussion hat in diesen Tagen durch den Anschlag hier in Berlin neue Aktualität erhalten. Natürlich stellt sich nach diesem schlimmen Ereignis die Frage nach einer neuen Abwägung zwischen den Aspekten der Sicherheit und den Freiheitsgrundrechten, aus denen sich das Grundrecht auf informationelle Selbstbestimmung und letztlich auch der Datenschutz herleiten. Ich begrüße es dabei sehr, dass die Koalition nicht in einer Kurzschlussreaktion eine massive Ausweitung der Videoüberwachung beschlossen hat, sondern einen am Einzelfall orientierten Kameraeinsatz als Baustein eines größeren Sicherheitskonzeptes. Denn eine Videoüberwachung ist kein Allheilmittel – das müssen wir uns immer wieder bewusst machen. Auf den ersten Blick scheint mir das Ergebnis der Senatsklausur daher tatsächlich ein Ergebnis mit Augenmaß zu sein. Wir alle werden uns in der kommenden Zeit noch vertiefter mit diesem Thema beschäftigen müssen, und ich gehe davon aus, dass ich noch Gelegenheit zur Stellungnahme zu dem Konzept bekommen werde.

Schwerpunkte des Jahresberichts 2015 waren neben dem neuen Rechtsrahmen für Europa aktuelle Entwicklungen rund um Big Data und vernetzte Fahrzeuge. Insgesamt zeigt der Bericht, dass die Digitalisierung inzwischen in die verschiedensten Lebensbereiche vorgedrungen ist und der Datenschutz damit in allen gesellschaftlichen Bereichen immer wichtiger wird. Man mag diese technische Entwicklung begrüßen oder auch nicht, jedenfalls muss man sie zur Kenntnis nehmen. Und als Datenschutzbeauftragte muss ich in jedem Fall auch vor den Risiken warnen, die damit verbunden sind. Denn viele dieser vernetzten Gegenstände des so genannten Internets der Dinge erheben eine große Menge personenbezogener Daten und übermitteln diese unter Umständen auch an Dritte. Mittlerweile umgeben uns in unserem Alltag eine Vielzahl vernetzter Gegenstände – vom smarten Fernseher, der Sehgewohnheiten aufzeichnet, über das vernetzte Auto bis hin zu Kühlschränken und ganzen smarten Wohngebäuden, die das Wohnverhalten der Bewohner aufzeichnen.

Es geht hier nicht darum, diese Techniken pauschal zu verteufeln. Das Internet der Dinge kann vielen Menschen den Alltag erleichtern und uns helfen, zu einer modernen Metropole zu werden. Smarte Gebäude zum Beispiel können dazu beitragen, im hohen Alter ein selbstbestimmtes Leben zu Hause zu ermöglichen. Doch gerade deshalb ist es unbedingt erforderlich, dass die so erhobenen Daten angemessen vor Missbrauch und kriminellen Angriffen von außen geschützt werden. Und es ist unerlässlich, dass wir alle uns immer wieder ins Bewusstsein rufen, dass bei dieser technischen Entwicklung zunehmend persönliche Daten von uns aufgezeichnet werden. Nur so können wir souverän damit umgehen und Sicherungsmaßnahmen ergreifen.

Personenbezogene Daten gelten als das Öl des 21. Jahrhunderts und wecken dementsprechende Begehrlichkeiten. Umso wichtiger ist die Kontrolle dieser Datenflüsse geworden – insbesondere auch im internationalen Kontext. Das betrifft nicht nur große Konzerne, sondern auch viele mittelständische Unternehmen, die z. B. Cloud-Computing-Lösungen ausländischer Anbieter nutzen.

Momentan beschränkt sich meine Kontrollkompetenz als Landesdatenschutzbeauftragte noch auf in Berlin ansässige Unternehmen und öffentliche Landeseinrichtungen, nicht auf international agierende Konzerne. Das wird sich aber mit der europäischen Datenschutz-Grundverordnung ab Mai 2018 grundlegend ändern.

Damit wird sich meine Zuständigkeit auch auf ausländische Unternehmen erstrecken, wenn Daten von Berliner Bürgerinnen und Bürgern verarbeitet werden, wie es z. B. bei Facebook oder Google der Fall ist. Hier kommen riesige und äußerst zeit- und personalintensive Herausforderungen auf meine Behörde zu, weil die Grundverordnung die Datenschutzbehörden der EU-Mitgliedstaaten verpflichtet, gemeinsam und innerhalb sehr enger Zeitfenster in abgestimmten Verfahren zu handeln. Aber ich freue mich auf diese neue Aufgabe, da sich meine Handlungsmöglichkeiten zum Schutz der Daten der Menschen in Berlin ganz wesentlich erweitern werden.

Im Bereich der Informationsfreiheit möchte ich an dieser Stelle nur auf einen übergeordneten Punkt eingehen. Das Land Berlin war mit dem Informationsfreiheitsgesetz von 1999 Vorreiter für andere Gesetze in der Bundesrepublik. Mittlerweile hat sich allerdings die Gesellschaft nicht zuletzt aufgrund der umfassenden Digitalisierung des Lebens deutlich verändert. Die Erwartungen der Menschen an eine transparente Verwaltung gehen inzwischen dahin, Informationen vom Staat zu erhalten, ohne Anträge stellen zu müssen. Das Abgeordnetenhaus hat diese Entwicklung im vergangenen Jahr bei der Verabschiedung des E-Government-Gesetzes aufgegriffen, ebenso wie die neue Koalition in ihrem Koalitionsvertrag, der eine Weiterentwicklung des Informationsfreiheitsgesetzes hin zu einem Transparenzgesetz vorsieht. Das begrüße ich sehr. Aus meiner Sicht kann es dabei jedoch nicht darum gehen, unbesehen sämtliche Rohdaten, die es gibt, zu veröffentlichen, da das kaum zu einer verbesserten Transparenz und Kontrolle öffentlichen Handelns führen würde. Es bestünde eher die Gefahr, dass die tatsächlich relevanten Informationen in dieser Informationsflut untergehen. Vielmehr sollte die Verwaltung verpflichtet werden, zusammenhängende und aus sich heraus nachvollziehbare Unterlagen bereitzustellen. Ich werde dieses Vorhaben sehr gern beratend begleiten und möchte damit schließen.

Ich danke für Ihre Aufmerksamkeit!

Stichwortverzeichnis

A

B

C / D

E

F

G

H / I

J

K

L

M

N / O

P

R

S

T

U

V

W

Z

Veröffentlichungen 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.

Dokumente zu Datenschutz und Informationsfreiheit: Diese Schriftenreihe erscheint jährlich als Anlage zu unserem Tätigkeitsbericht. Sie enthält die bedeutsamen Dokumente der nationalen und internationalen Arbeitsgruppen und Konferenzen des genannten Jahres.

Berliner Informationsgesetzbuch (BlnInfGB): In dieser Textsammlung werden von uns die wichtigsten Regelungen zum Datenschutz und zur Informationsfreiheit für das Land Berlin herausgegeben.

Ratgeber und Faltblätter zum Datenschutz: In diesen Publikationen haben wir praktische Informationen zu einzelnen Fragen im Alltag zusammengestellt. Damit wollen wir die Menschen in die Lage versetzen, ihre Datenschutzrechte bzw. ihr Recht auf Informationszugang eigenständig wahrzunehmen.

Welche Broschüren wir im Einzelnen veröffentlicht haben, können Sie einer Übersicht auf unserer Website www.datenschutz-berlin.de entnehmen. Den überwiegenden Teil unserer Broschüren haben wir dort für Sie auch zum Download bereitgestellt. Eine Bestellung per Post ist gegen Einsendung eines an Sie selbst adressierten und mit 1,00 Euro frankierten DIN-A5-Umschlages möglich.

Der Jahresbericht 2016 umfasst folgende Schwerpunkte:

Post-Safe-Harbor: Das neue EU-US Privacy Shield, Datenschutz-Grundverordnung, Gesundheitsdatenschutz in der öffentlichen Verwaltung, Rechtliche Grenzen des Outsourcings von Patientendaten, Einsatz von Stillen SMS in strafrechtlichen Ermittlungsverfahren.

www.datenschutz-berlin.de

be Berlin