

Berliner Beauftragter für
Datenschutz und Informationsfreiheit



Datenschutz und Informationsfreiheit

Bericht 2012

Impressum

Herausgeber: Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4 – 10, 10787 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/>

Disclaimer: Bei den im Text enthaltenen Verweisen auf Internet-Seiten (Links) handelt es sich stets um „lebende“ (dynamische) Verweisungen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat vor Drucklegung zwar den fremden Inhalt daraufhin überprüft, ob durch ihn eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Für spätere Veränderungen dieses fremden Inhalts ist er jedoch nicht verantwortlich.

Satz: LayoutManufaktur.de

Druck: Druckerei Dienstleistungen

BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2012

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§§ 29 Berliner Datenschutzgesetz, 18 Abs. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den am **28. März 2012** vorgelegten Jahresbericht 2011 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2012 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band („Dokumente 2012“) veröffentlicht.

Dieser Jahresbericht ist über das Internet (<http://www.datenschutz-berlin.de/>) abrufbar.

Inhalt

Einleitung	9
-------------------------	----------

1 Digitale Verwaltung

1.1 E-Government	13
1.2 Open Data.....	16
1.3 Weitere Berliner IT-Projekte	18

2 Schwerpunkte

2.1 Funkzellenabfragen – von der Ausnahme zur Regel?	23
2.2 Zehn Vorschläge zur Verbesserung der EU-Datenschutz-Grundverordnung...28	
2.3 BYOD – „Bring your own device“: Arbeiten mit privaten Endgeräten	32
2.4 Wann dürfen Apothekenrechenzentren Verordnungsdaten weitergeben?	38
2.5 Wenn die Aufsichtsbehörde klingelt – vermeidbare Fehler von Unternehmen bei Prüfungen.....	42

3 Öffentliche Sicherheit

3.1 Antiterrordatei auf dem Prüfstand	48
3.2 Rechtsextremismus-Datei: Ideenlose Imitation der Antiterrordatei	49
3.3 Akkreditierung für den Papstbesuch	51
3.4 Stille SMS.....	51
3.5 Protokollierung des Abfragegrundes	52
3.6 Unbefugter Abruf aus INPOL.....	53
3.7 Unzulässige Datenspeicherung – Führerschein weg.....	54
3.8 Wiedereinführung der taktischen Hinweise?.....	55

4 Melde- und Ausländerwesen

4.1 Bundesmeldegesetz	57
4.2 Zugriff auf das Melderegister für private Zwecke	58
4.3 Löschung oder Archivierung von Meldedaten	59
4.4 Dauerhafte Aufbewahrung von Einbürgerungsanträgen?	61

5 Verkehr

5.1 Videoüberwachung im Straßenverkehr.....	62
5.2 Verkehrserhebung:Verschlüsselung der Kfz-Kennzeichen auf der Tangential- Verbindung Ost	64
5.3 Fahrkarten und Parktickets übers Handy	65

6 Justiz

6.1 Zentrale Auskunftsstelle Justizvollzug.....	70
6.2 Einsichtnahme in frühere Examensklausuren	71
6.3 Auslagerungen gerichtlicher Archivakten.....	72

7 Finanzen

7.1 Einsichtnahme in Steuerakten – Neubewertung von Gebäudeteilen	74
7.2 Steuerfahndung in der Fahrschule	75

8 Jugend und Soziales

8.1 WIMES – ein neues Verfahren für die Jugendhilfe	78
8.2 Kinderschutz und Datenschutz.....	79
8.3 Bezirksamt lädt Vermieter zur Schnüffelei ein	80
8.4 Überschießende Datenerhebung im Sozialamt	83
8.5 Fremde Daten in der Schwerbehindertenakte.....	85

9 Gesundheitswesen

9.1 Neue Hygieneverordnung.....	87
9.2 Ungesicherte Datenbaustellen in der Zentralen Stelle nach Kinderschutzgesetz	88
9.3 Termin versäumt – Kinderärztin informiert das Gesundheitsamt.....	89
9.4 Pseudonymisierung in der klinischen Krebsregistrierung	91
9.5 Das Endoprothesenregister Deutschland	92
9.6 Was kann eine Protokollierung der Datenzugriffe in Krankenhäusern leisten?	93

9.7 Tablet-Computer in der medizinischen Behandlung durch die Charité.....	95
9.8 Laxer Umgang mit sensitiven Schreiben im Gesundheitsamt Steglitz-Zehlendorf.....	96

10 Beschäftigtendatenschutz

10.1 Private Nutzung von Internet und E-Mail	98
10.2 Dienstvereinbarung zur Telearbeit im Land Berlin.....	99
10.3 Datenerhebung im Rahmen von Präqualifikationsverfahren.....	100
10.4 Erhebung und Speicherung von Beschäftigtendaten zum Schutz des Urheberrechts?	101

11 Wohnen und Umwelt

11.1 Orientierungshilfe Smart Metering – Datenschutz bei intelligenten Stromzählern	103
11.2 Berliner Mietspiegel	104
11.3 Automatisierte Datenübermittlungen – Bodenschutz ohne Datenschutz ...	105
11.4 Wer darf in die Bauakte schauen?	106

12 Wissen und Bildung

12.1 Forschung	108
12.1.1 Wenn Lehrkräfte beforscht werden	108
12.1.2 Können Partner sich gegenseitig für Elterninterviews bevollmächtigen?	109
12.1.3 Zusammenarbeit mit der Ethik-Kommission des Landes Berlin	111
12.1.4 RFID-Technik in öffentlichen Bibliotheken	112
12.2 Schule	113
12.2.1 Schultrojaner	113
12.2.2 Einsatz von privaten Smartphones durch Lehrkräfte zu dienstlichen Zwecken	115
12.2.3 Veröffentlichungen von Abiturientendaten in der Tagespresse	116
12.2.4 Das Abiturzeugnis des Regierenden Bürgermeisters	118
12.2.5 Werbefilm aus der Basketball-AG.....	120
12.2.6 Die Hausaufgabenliste und ein Datenaustausch „unter Brüdern“!...122	
12.2.7 Videoüberwachung an Schulen.....	124

13 Wirtschaft

13.1 Banken und Versicherungen.....	127
13.1.1 Bankrecht ersetzt nicht Datenschutzrecht.....	127
13.1.2 Ist das ec-cash-Verfahren sicher?.....	129
13.1.3 Kuvertierungsprobleme in einer Bank.....	130
13.1.4 Vorsicht bei Online-Bonitätsprüfungen!.....	131
13.2 Industrie- und Handelskammer	132
13.2.1 IHK als Adresshändler	132
13.2.2 Überprüfung der Wahlvorschläge für die IHK-Vollversammlung	133
13.3 „fragenstaat.de“ – jetzt datenschutzgerecht.....	135
13.4 Festplatten-Crash – Was passiert mit den Daten bei der Reparatur?	136
13.5 Video- und Kameraeinsatz zu künstlerischen und werbewirksamen Zwecken	137
13.6 Aus der Arbeit der Sanktionsstelle	139

14 Europäischer und internationaler Datenschutz

14.1 Neuer europäischer Rechtsrahmen.....	141
14.2 Weitere Ergebnisse aus Brüssel.....	143

15 Datenschutzmanagement

15.1 Bundesweite Premiere: Anerkennung von Verhaltensregeln nach dem BDSG	147
15.2 Informationspflicht bei Datenlecks in Wirtschaft und Verwaltung	149
15.2.1 Datenpannen in der Wirtschaft	151
15.2.2 Datenpannen in der Verwaltung	156
15.3 Datenschutzfreundliche Verfahrensgestaltung: Behandlungsleitlinien für Schmerzpatienten	160
15.4 Stiftung Datenschutz	161

16 Telekommunikation und Medien

16.1 Die neue Google-Datenschutzerklärung – ein Rückschritt für den Datenschutz.....	163
---	-----

16.2 Soziale Netzwerke.....	165
16.2.1 Social Plugins	165
16.2.2 Anschluss- und Benutzungszwang bei Facebook?.....	166
16.2.3 Leitfäden für den Einsatz von sozialen Medien in der Berliner Verwaltung	168
16.3 Liquid Feedback mit Klarnamen?	168
16.4 Selbsthilfe im Internet	171
16.4.1 Selbstschutz gegen Tracking	171
16.4.2 Wie kann ich eigene Daten löschen?.....	175
16.5 Smartphones und Apps	177
16.6 Intelligente Werbeflächen.....	180
16.7 Aus der Arbeit der „Berlin Group“	181

17 Technik und Organisation

17.1 Kontrolle bei den Bäder-Betrieben.....	183
17.2 Organisation des Datenschutzes in den Bezirken.....	184

18 Informationsfreiheit

18.1 Informationsfreiheit in Deutschland.....	187
18.2 Informationsfreiheit in Berlin	188
18.3 Einzelfälle.....	191

19 Was die Menschen sonst noch von unserer Tätigkeit haben ...

20 Aus der Dienststelle

20.1 Entwicklungen.....	208
20.2 Zusammenarbeit mit dem Abgeordnetenhaus, dem Deutschen Bundestag und dem Europäischen Parlament	208
20.3 Zusammenarbeit mit anderen Stellen	209
20.4 Öffentlichkeitsarbeit	211

Stichwortverzeichnis

213



Einleitung

Wer beim größten Internetbuchhändler Amazon das Angebot durchsucht oder Bücher bestellt, dessen Interessen werden dafür genutzt, um dem Käufer Vorschläge zu machen, was ihn noch interessieren könnte. Der eine mag das nützlich finden, während andere dies als aufdringlich ansehen. Noch weiter geht Amazon bei seinem eBook-Reader Kindle, mit dem man elektronische Bücher platzsparend lesen und transportieren kann. Hier wird das Nutzungsverhalten der Leserin oder des Lesers bis hin zu der Seite, die sie oder er gerade liest oder bei der die Lektüre unterbrochen wird, überwacht und Amazon mitgeteilt. Der Buchhändler schaut den Leserinnen und Lesern ständig über die Schulter. Auch die dabei gewonnenen Daten können für Werbezwecke nützlich sein. Viele Leserinnen und Leser würden dies allerdings – wüssten sie davon – als inakzeptablen Einbruch in ihre Privatsphäre empfinden. In den USA hat der kalifornische Gesetzgeber bereits im Sommer 2011 hierauf reagiert und ein Gesetz zum Schutz der Privatsphäre des Lesers (Reader Privacy Act) verabschiedet. Darin wird Anbietern von elektronischen Büchern zwar nicht die Erhebung entsprechender Daten, wohl aber ihre Weitergabe an Dritte (z. B. Werbetreibende) verboten, solange die Betroffenen nicht ausdrücklich eingewilligt haben oder ein Gericht dies angeordnet hat.

Im Gegensatz zu den Vereinigten Staaten haben die Gesetzgeber in Deutschland und in Europa seit jeher nicht versucht, auf technische Bedrohungen der informationellen Selbstbestimmung des Einzelnen punktuell mit speziellen Gesetzen zu reagieren, sondern sie haben in allgemeinen Datenschutzgesetzen der Verarbeitung personenbezogener Daten Grenzen gesetzt. Dies zeigt sich im Bundesdatenschutzgesetz, im Berliner Datenschutzgesetz und auch in der Europäischen Datenschutzrichtlinie von 1995. Technologienahe Regelungen wie der kalifornische Reader Privacy Act haben den Vorteil der größeren Präzision, aber zugleich den erheblichen Nachteil der zu großen Abhängigkeit von einer sich immer schneller entwickelnden Technik. Aber auch der allgemeiner formulierte, in Europa geltende Rechtsrahmen bedarf dringend der Erneuerung und Anpassung an die vollkommen veränderte Informationsumgebung des 21. Jahrhunderts.

Es ist das Verdienst der Europäischen Kommission, dass sie diesen dringenden Modernisierungsbedarf mit ihrem im Januar vorgelegten **Reformpaket für einen neuen europäischen Rechtsrahmen** entsprochen hat.¹ Das gilt insbesondere für den Entwurf einer Datenschutz-Grundverordnung, die den Datenschutz in der Wirtschaft und in großen Teilen der öffentlichen Verwaltung europaweit vereinheitlichen soll.² Der Kommissionsentwurf für eine Richtlinie zum Datenschutz im Bereich der Strafverfolgungsbehörden und der Polizei leistet dagegen keinen wesentlichen Beitrag zur Weiterentwicklung des Datenschutzes und droht zudem am Widerstand der europäischen Regierungen zu scheitern. Auch der Entwurf der Datenschutz-Grundverordnung stößt auf Widerstände, die aber nicht dazu führen dürfen, dass dieses Vorhaben bis zur Neuwahl des Europäischen Parlaments 2014 verzögert oder gar ganz verhindert wird. Insbesondere ist es zu begrüßen, dass die vom Bundesrat – mit der Stimme Berlins – erhobene Subsidiaritätsrüge nicht genügend Unterstützung aus anderen europäischen Ländern erhalten hat. Denn es kann kein Zweifel daran bestehen, dass die wesentlichen Grundzüge des Datenschutzrechts europaweit einheitlich festgelegt werden sollten.

Dabei muss aber weiterhin der Grundsatz gelten, den bereits die Datenschutzrichtlinie von 1995 enthielt: Die Angleichung der nationalen Rechtsvorschriften darf nicht zu einer Verringerung des Datenschutzniveaus führen, sondern muss im Gegenteil darauf abzielen, in der Gemeinschaft ein **hohes Datenschutzniveau** sicherzustellen.³ Die europaweite Vereinheitlichung des Datenschutzes darf insbesondere nicht zu einer Absenkung des in Deutschland und in Berlin geltenden Datenschutzniveaus führen, wie es etwa das Berliner Datenschutzgesetz und das Sozialgesetzbuch des Bundes vorsehen. Diese Gefahr besteht durchaus. Denn in den gegenwärtig laufenden dreiseitigen Verhandlungen zwischen Europäischem Parlament, Rat und Kommission (Trilog) wird eine **Absenkung des Datenschutzniveaus** zu Lasten der Bürgerinnen und Bürger vor allem von Unternehmen der Internetwirtschaft und der Werbebranche, aber auch von mehreren Regierungen betrieben. Dabei wird zu Unrecht davon ausgegangen, dass der Datenschutz per se innovationshem-

1 Siehe 14.1

2 Siehe 2.2

3 Erwägungsgrund (10) zur Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

mend sei und es zu den gegenwärtig vorherrschenden datenschutzunfreundlichen Geschäftsmodellen im Internet keine Alternative gebe. Stattdessen wird es in den nächsten Monaten darauf ankommen, den Vorschlag der Kommission durch eine Stärkung der Betroffenenrechte und durch mehr Flexibilität für die nationalen Gesetzgeber und Datenschutzbeauftragten vor allem im öffentlichen Bereich zu verbessern. Eine völlige Ausklammerung des öffentlichen Bereichs vom Anwendungsbereich der Verordnung wäre allerdings ein verhängnisvoller Rückschritt gegenüber der Rechtslage nach der geltenden Richtlinie von 1995.

Auch wenn das Datenschutzrecht europaweit vereinheitlicht wird, so sollte doch am bewährten **Prinzip der dezentralen Datenschutzkontrolle** festgehalten werden. Das gilt sowohl innerhalb Deutschlands als auch auf europäischer Ebene. Der ursprüngliche Kommissionsvorschlag sah weitreichende Befugnisse für die Europäische Kommission vor, die die Unabhängigkeit der nationalen Datenschutzbehörden gefährdet hätten. Es zeichnet sich aber ab, dass stattdessen der künftige Europäische Datenschutzausschuss, in dem alle Datenschutzbehörden der Mitgliedstaaten vertreten sein werden, anstelle der Kommission auch weiterhin die Datenschutzkontrolle in Europa koordinieren wird. Zu der erfolgreichen Zusammenarbeit der Datenschutzbehörden in Deutschland und in Europa hat Berlin stets einen wichtigen Beitrag geleistet und wird dies auch in Zukunft tun.

Im November wurde erstmals der Verhaltenskodex eines Wirtschaftsverbandes, des Gesamtverbandes der Deutschen Versicherungswirtschaft, nach dem Bundesdatenschutzgesetz anerkannt.⁴ Dies könnte der Auftakt für weitere erfolgreiche **Projekte der regulierten Selbstregulierung** sein. Selbstregulierung kann jedoch niemals rechtliche Regeln ersetzen, sondern nur ergänzen und präzisieren. Denjenigen, die nach amerikanischem Vorbild die Selbstregulierung auch auf europäischer Ebene als Ersatz für einen modernen Rechtsrahmen ansehen, ist entgegenzuhalten, dass dies die Rechte der von Datenverarbeitung Betroffenen empfindlich schwächen würde.

Die Entwicklung des Informationsfreiheitsrechts tritt mit dem neuen Hamburgischen Transparenzgesetz in eine neue Phase.⁵ Während es immer noch fünf

4 Siehe 15.1

5 Siehe 18.1, 18.2

Bundesländer⁶ gibt, die nicht einmal ein Informationsfreiheitsgesetz herkömmlicher Art haben, nehmen die politischen Bestrebungen auch in Berlin zu, mehr Informationen in der öffentlichen Verwaltung proaktiv zugänglich zu machen. Das Berliner Informationsfreiheitsgesetz sieht dies bisher nur für bestimmte Informationen wie Aktenpläne und Verträge mit Privaten über Infrastrukturleistungen vor. Einer Ausdehnung dieses Gedankens, **Informationen als Bringschuld** gegenüber den Menschen zu verstehen, steht der Datenschutz nicht prinzipiell entgegen, er muss aber angemessen berücksichtigt werden. Dies gilt auch für die vielfältigen Bestrebungen, Verwaltungsdienstleistungen elektronisch zu erbringen (eGovernment) und Verwaltungsinformationen online zum Abruf und zur Weiterverarbeitung (Open Data) bereitzustellen.

6 Baden-Württemberg, Bayern, Hessen, Niedersachsen, Sachsen

1 Digitale Verwaltung

Die Digitalisierung von Verwaltungsvorgängen und die Entwicklung elektronischer Dienstleistungsangebote der Verwaltung für Bürgerinnen und Bürger schreitet voran, allerdings erheblich langsamer als vor Jahren angekündigt. Digitales Verwalten und elektronisches Regieren lassen sich nicht auf Knopfdruck, sondern nur schrittweise einführen, zumal dafür erst vielfältige Voraussetzungen geschaffen werden müssen. Insbesondere fehlen noch rechtliche Rahmenbedingungen auf Bundes- und Landesebene, die sicherstellen, dass beim E-Government Datenschutz und Datensicherheit nicht auf der Strecke bleiben.

Zugleich muss „Digitale Verwaltung“ auch „Offene Verwaltung“ sein. E-Government und Open Government bzw. Open Data stehen in einem engen Zusammenhang. Deshalb ist es zu begrüßen, dass das Abgeordnetenhaus als Nachfolger für den bisherigen Unterausschuss „Datenschutz und Informationsfreiheit“ des Innenausschusses einen eigenen Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit eingesetzt hat.

1.1 E-Government

Das Bundesministerium des Innern veröffentlichte im März den Referentenentwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (**E-Government-Gesetz**). Ziel des Gesetzes ist es, durch den Abbau bundesrechtlicher Hindernisse die elektronische Kommunikation mit der Verwaltung zu erleichtern. Der Entwurf hatte zahlreiche datenschutzrechtliche Mängel. So wurden Schutzziele im Hinblick auf die Gewährleistung des Datenschutzes und der Datensicherheit formuliert, die unvollständig waren. Im Berliner Datenschutzgesetz⁷ sind die wesentlichen Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisions-

7 § 5 Abs. 2 Nr. 1 – 6 BlnDSG

fähigkeit und Transparenz definiert; sie sind bereits bei bestehenden Verfahren umzusetzen und sollten für die elektronische Verwaltung erst recht gelten.

Die Schaffung einer gesetzlichen Grundlage für die elektronische Aktenführung ist grundsätzlich positiv zu bewerten. Die Nachvollziehbarkeit und Vollständigkeit einer elektronischen Akte („e-Akte“) muss genauso gewährleistet sein wie bei einer Papierakte. Die elektronische Aktenführung sollte daher den gegenwärtigen Standard verbessern und nicht hinter diesem zurückbleiben.

Das Bundeskabinett hat im September einen auch aus Datenschutzsicht überarbeiteten Entwurf beschlossen. Allerdings hat der Bundesrat im November erhebliche Einwände erhoben, sodass angesichts der Zustimmungsbedürftigkeit des Gesetzes mit Änderungen im Vermittlungsausschuss zu rechnen ist. Wesentlicher Kritikpunkt des Bundesrates ist die verpflichtende Formulierung der Bestimmungen für die Behörden der Länder und Kommunen. In seiner Stellungnahme⁸ regt der Bundesrat die Umwandlung in Kann-Bestimmungen an. Begrüßenswert ist der Vorschlag, Bürgerinnen und Bürgern die verschlüsselte Übermittlung von elektronischen Dokumenten an Behörden anzubieten. Eine fehlende Möglichkeit der Verschlüsselung stellt ein wesentliches Hindernis für den Einsatz der elektronischen Verwaltung dar. Die Bundesregierung hat diesen Vorschlag bereits abgelehnt – allerdings in nicht nachvollziehbarer Weise, nämlich wegen des zu hohen Verwaltungsaufwands.⁹

Bereits 2011¹⁰ haben wir kurz über den im Frühjahr vorgelegten Referentenentwurf zu einem **Berliner E-Government-Gesetz** berichtet. Aufgrund der Verzögerung und der Auswirkungen des E-Government-Gesetzes des Bundes auf die Landesebene liegt noch keine neue Fassung eines Berliner Entwurfs vor. Die Landesregierung sollte aber den Mut haben, ein eigenes Gesetz ins Parlament einzubringen, wenn das Vermittlungsverfahren auf Bundesebene vor der Bundestagswahl nicht mehr abgeschlossen wird.

Im Rahmen der Kommunikation von Bürgerinnen und Bürgern mit öffentlichen Stellen des Bundes oder der Länder stellt **De-Mail** eine wichtige Kompo-

8 BR-Drs. 557/12(B)

9 BT-Drs. 17/11473, S. 93

10 JB 2011, 1.2.1

nente dar, soll sie doch die sichere, vertrauliche und nachweisbare Kommunikation über das Internet gewährleisten. Im Berichtszeitraum wurden die ersten De-Mail-Anbieter beim Bundesamt für Sicherheit in der Informationstechnik akkreditiert. Im Gegensatz zum **E-Postbrief** der Deutschen Post ermöglicht De-Mail auch die Verwendung der qualifizierten elektronischen Signatur und kann daher einen klassischen Brief ersetzen.

Problematisch ist jedoch die Zulässigkeit der Versendung besonders schutzbedürftiger Daten mittels De-Mail. Das De-Mail-Gesetz sieht keine Ende-zu-Ende-Verschlüsselung vor, sondern bestimmt lediglich, dass der akkreditierte Diensteanbieter (DMDA) eine Ende-zu-Ende-Verschlüsselung durch die Nutzenden zu unterstützen hat,¹¹ was die Datenschutzbeauftragten schon im Gesetzesverfahren kritisiert haben.¹² Die Nachrichten werden zwar auf dem Transportweg verschlüsselt, jedoch wird vor dem Versand und vor dem Ablegen im Postfach des Empfängers automatisch eine Kopie der Nachricht erstellt, um diese auf Schadsoftware zu überprüfen. Hierzu geben die Nutzenden bei Freischaltung eines De-Mail-Nutzerkontos ihre Einwilligung. Die Kopie wird anschließend gelöscht. Dieser Prüfprozess erfolgt automatisiert auf Servern des DMDA. Die Beschäftigten des DMDA haben zwar kein Recht, wohl aber die technische Möglichkeit des Zugriffs auf die Daten.

Ein solches Verfahren ist für die Versendung besonders schutzbedürftiger Daten wie Sozialdaten, Gesundheitsdaten und Daten, die dem Steuergeheimnis unterliegen, unzureichend. So fordert das Steuerrecht,¹³ dass die Finanzbehörde Daten, die dem Steuergeheimnis unterliegen, vor der elektronischen Übermittlung verschlüsseln muss. Es gibt zwar Maßnahmen, die die Sicherheit des Verfahrens gewährleisten sollen, wie die förmliche Akkreditierung des DMDA, die Erfüllung der Vorgaben des De-Mail-Gesetzes und dessen Konkretisierung durch die Technische Richtlinie des BSI¹⁴ und den Datenschutz-Kriterien-

11 § 5 Abs. 3 Satz 2 De-Mail-Gesetz

12 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. April 2009: Datenschutz beim vorgesehenen Bürgerportal unzureichend, siehe Dokumentenband 2009, S. 14 ff.

13 § 87a Abs. 1 Satz 3 Abgabenordnung

14 Technische Richtlinie 01201 De-Mail des Bundesamtes für Sicherheit in der Informationstechnik vom 23. März 2011

katalog¹⁵ des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Grundsätzlich muss aber an der Forderung nach einer Ende-zu-Ende-Verschlüsselung für personenbezogene Daten mit besonderem Schutzbedarf festgehalten werden. Ausnahmen sind nur unter bestimmten Bedingungen denkbar, die jeweils gesondert und detailliert betrachtet werden müssen.

1.2 Open Data

Berlin hat im September 2011 als erstes Bundesland ein eigenes Open Data-Portal als Pilot- und Testprojekt im Rahmen des E-Government-Programms „ServiceStadt Berlin“ gestartet.¹⁶ Inzwischen haben auch andere Bundesländer entsprechende Portale oder Prototypen vorgestellt, u.a. Baden-Württemberg, Bayern und Bremen. Dagegen wird der Bund erst zur CeBIT 2013 das Pilotprojekt für ein länderübergreifendes Portal starten. Darüber hinaus wurden vom Land Berlin auch Sonderpreise im Rahmen des bundesweiten Wettbewerbs „Apps4Deutschland“ für die Nutzung der Berliner Datensätze ausgelobt. Die Preisverleihung sowohl für den Gesamtwettbewerb als auch für die Berliner Sonderpreise erfolgte im März auf der CeBIT in Hannover.

Wie im Koalitionsvertrag vereinbart, hat Berlin die bereits 2010 begonnene Open Data-Initiative auch in diesem Jahr fortgesetzt und ausgebaut. Hierzu wurde im Januar von der federführenden Senatsverwaltung für Wirtschaft, Technologie und Forschung zusammen mit dem Fraunhofer-Institut für offene Kommunikationssysteme (FOKUS) die Berliner Open Data-Strategie veröffentlicht.¹⁷ Diese sieht einen Stufenplan zur Förderung von offenen Daten und zum Ausbau des bestehenden Open Data-Portals der Hauptstadt vor. Basierend auf den Empfehlungen des Strategiepapiers und den bisherigen Erfahrungen hat der Senat verschiedene Schritte beschlossen, um das Thema Open Data in der Hauptstadt weiter voranzubringen.

15 Gemäß § 18 Abs. 3 Nr. 4 De-Mail-Gesetz

16 JB 2011, 1.2.1 (S. 27 ff.)

17 Both/Schieferdecker (Hrsg.), Berliner Open Data-Strategie, Organisatorische, rechtliche und technische Aspekte offener Daten in Berlin – Konzept, Pilotsystem und Handlungsempfehlungen

Kurzfristig soll der Gedanke der offenen Daten in den Berliner Verwaltungsvorschriften verankert und das **Berliner Datenportal** („daten.berlin.de“) in den Regelbetrieb überführt werden.¹⁸ Dies ist für Anfang 2013 geplant. Innerhalb der nächsten zwei bis drei Jahre sollen ein nachhaltiger Ausbau der Datenangebote des Landes Berlin und eine Ergänzung um Werkzeuge, höherwertige Dienste und Schulungen für die Beschäftigten des öffentlichen Dienstes erfolgen. Dies beinhaltet auch, dass „alle Beschlüsse und Protokolle von Senats-, Stadtrats-, Parlaments- und Ausschusssitzungen in offenen Formaten wie z. B. Office Open XML (OOXML) oder OASIS Open Document Format (ODF) veröffentlicht werden.“¹⁹ Die Daten auf dem Portal sollen in einer maschinenlesbaren Form angeboten werden, und Datensätze sollen möglichst unter einer „Creative Commons“-Lizenz mit Pflicht zur Namensnennung (CC BY) bereitgestellt werden, um auch eine kommerzielle Nutzung zu ermöglichen. Langfristig ist die Abstimmung und Integration der Berliner Datenangebote mit anderen Angeboten in Deutschland, im deutschsprachigen Raum und in Europa geplant.²⁰

Sowohl inhaltlich als auch technisch wird der Ausbau des Berliner Open Data-Angebots durch die Mitglieder der Open Data-Arbeitsgruppe begleitet. Die Einsetzung der Arbeitsgruppe wurde im Juni vom Staatssekretärsausschuss zur Verwaltungsmodernisierung beschlossen, um sich den offenen Fragen der Harmonisierung rund um die Beschreibung und Bereitstellung der Daten zu widmen und ein entsprechendes Weiterbildungsangebot für die Beschäftigten Berlins zu entwickeln. In der Arbeitsgruppe sind Mitglieder verschiedener Verwaltungen, insbesondere aus den Bereichen Geodaten, Verkehr, Umwelt, Verbraucherschutz, Gesundheit und Soziales sowie des Amtes für Statistik Berlin-Brandenburg vertreten. Die Landesredaktion sowie das ITDZ wirken bei der Gestaltung des technischen Umfeldes ebenso mit wie wir, damit sowohl die Belange des Datenschutzes als auch der Informationsfreiheit gewahrt werden.

Aktuell stehen auf der Webseite 84 Datensätze aus 18 unterschiedlichen Kategorien bereit (u.a. Arbeitsmarkt, Stadtplanung, Tourismus, Wirtschaft, öffentliche Verwaltung, Verbraucherschutz, Protokolle und Beschlüsse, Demographie, Bil-

18 Siehe Kurzfassung der Studie „Berliner Open Data-Strategie“, S. 6

19 A. a. O., S. 17

20 A. a. O., S. 20

dung), die zur Informationsrecherche oder auch als Basis für die Entwicklung von Smartphone-Applikationen genutzt werden können.

Es bleibt zu hoffen, dass die Open Data-Strategie des Senats nicht nur propagiert, sondern auch in politisch brisanten Bereichen gelebt wird. Daran entstanden Zweifel, als der Finanzsenator kurz nach Veröffentlichung der Open Data-Strategie des Senats dem Sonderausschuss „Wasserverträge“ mitgeteilt hat, dass die gesetzlich vorgesehene Veröffentlichung des Konsortialvertrages (nebst Anlagen und Änderungsvereinbarungen) zur Teilprivatisierung der Berliner Wasserbetriebe in maschinenlesbarer Form derzeit nicht möglich sei.

1.3 Weitere Berliner IT-Projekte

Im Rahmen des Projektes **Anliegen-/ Beschwerdedatenbank** im Ordnungsamt überraschte die Aussage des Leiters eines Ordnungsamtes, dass unsere Behörde nicht zu beteiligen sei,²¹ sondern lediglich der behördliche Datenschutzbeauftragte informiert werden müsse. Er berief sich auf einen Vermerk der Senatsverwaltung für Inneres und Sport von 2011, in dem dargelegt wurde, dass die Anliengendatenbank zwar eine Form der automatisierten Datenverarbeitung im Bereich einer Behörde und die Änderung der Datenverarbeitung sogar wesentlich ist, eine Beteiligung des Berliner Beauftragten für Datenschutz und Informationsfreiheit jedoch unterbleiben kann, da es sich nicht um eine berlinweit einheitliche Lösung handelt, sondern nur in einzelnen Bezirken zum Einsatz kommen soll.

Möglicherweise beruht die rechtliche Fehleinschätzung in dem Vermerk auf der gesetzlichen Regelung,²² wonach der Berliner Beauftragte für Datenschutz und Informationsfreiheit bei der Vorabkontrolle zu beteiligen ist, wenn sie den beabsichtigten Einsatz verwaltungsübergreifender Verfahren betrifft. Aber auch dann ist die Auffassung nicht nachvollziehbar, da das betreffende Verfahren gerade

21 Nach § 24 Abs. 3 Satz 3 BlnDSG ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit über die Einführung neuer Automationsvorhaben und wesentliche Änderungen automatisierter Datenverarbeitungen im Bereich der Behörden und sonstigen öffentlichen Stellen zu informieren.

22 § 24 Abs. 1 Satz 4 BlnDSG

mehrere Bezirke betrifft. Wir haben die Senatsverwaltung für Inneres und Sport gebeten zu veranlassen, dass die irrtümliche Rechtsauffassung nicht weiterverbreitet wird, und die Verwaltungen auf die richtige Rechtslage hinzuweisen. Dieser Bitte wurde entsprochen. Auch wenn die datenschutzrechtliche Bewertung dieses Verfahrens ergeben hat, dass keine grundsätzlichen Bedenken gegen den Einsatz der Datenbank bestehen, entscheidet der Berliner Beauftragte für Datenschutz und Informationsfreiheit selbst darüber, wann eine Beteiligung nach § 24 Abs. 3 BlnDSG notwendig ist.

Der Rechnungshof stellte in seinem Jahresbericht 2011 fest, dass es aufgrund der technischen Entwicklungen wirtschaftlicher ist, von der dezentralen Datenverarbeitung zur zentralen Datenverarbeitung „zurückzukehren“, da eine **zentrale Serverinfrastruktur** den Behörden erhebliches Einsparpotential bietet. Der Senat griff die Empfehlung des Rechnungshofes auf und legte eine Strategie für einen einheitlichen Serverbetrieb vor. Vor diesem Hintergrund vereinbarten das Bezirksamt Mitte und das ITDZ Berlin, den dezentralen Serverbetrieb aus den Standorten des Bezirksamtes in das Rechenzentrum des ITDZ zu verlagern. Damit ist das Bezirksamt Mitte eine der ersten Verwaltungen, die sich der allgemein geplanten Serverkonsolidierung bedienen.

Nach dem BlnDSG²³ sind vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der Datenverarbeitung die zu treffenden technischen und organisatorischen Maßnahmen auf Grundlage einer Risikoanalyse und eines Sicherheitskonzeptes zu ermitteln. Da die Verlagerung von Betriebsleistungen zumindest eine wesentliche Änderung der Datenverarbeitung mit datenschutzrechtlicher Relevanz darstellt, sind die bisher erstellten Sicherheitskonzepte an die neuen Verhältnisse anzupassen. Sofern für ein Verfahren ein solches Sicherheitskonzept noch nicht existiert, muss das Verlagerungsprojekt der Anlass sein, das Versäumte nachzuholen.

Auch wird eine umfangreiche vertragliche Regelung der Auftragsdatenverarbeitung nach § 3 Abs. 1 und 2 BlnDSG durch das ITDZ notwendig, die alle verlagerten IT-Verfahren betrifft. Problematisch erscheint hier die gesetzliche Forderung,²⁴ dass die Angaben zu den verarbeiteten Datenarten hinreichend

23 § 5 Abs. 3 Satz 1 BlnDSG

24 § 3 Abs. 1 Satz 3 Nr. 2 BlnDSG

genau sein müssen und vor allem die besonderen Kategorien von personenbezogenen Daten²⁵ ausdrücklich zu bezeichnen sind, da es eine Vielzahl von Fachanwendungen betrifft. Dieses praktische Problem ist jedoch lösbar, da die von den behördlichen Datenschutzbeauftragten zu führenden und öffentlich einsehbaren Dateibeschreibungen²⁶ eine geeignete Quelle für die notwendigen Angaben sind. Wenn die Dateibeschreibungen dort aktuell und vollständig vorliegen, kann auf sie als Vertragsbestandteil verwiesen werden.

Derzeit führt die Senatsverwaltung für Bildung, Jugend und Wissenschaft neue und einheitliche Hard- und Software im Rahmen des Projekts **eGovernment@School** in allen Berliner Schulen ein. Zweck der Maßnahme ist eine Vereinheitlichung der bisher heterogenen Schul-IT mit dem erklärten Ziel, die IT-Sicherheit zu erhöhen. Zuerst erfolgt die sichere Anbindung der zur Verwaltung der Schulen dienenden Verwaltungsnetze, da hier personenbezogene Schülerdaten verarbeitet werden. Später soll hierüber auch die Internetanbindung der in den Klassenräumen zur Verfügung stehenden Unterrichtsnetzwerke erfolgen, wobei eine strikte Trennung vom Verwaltungsnetz notwendig ist.

Grundlage ist die Verbindung der Berliner Schulen über ein sog. **sicheres Berliner Schulintranet (sBSI)**. Dazu erhält jede Schule eine physisch geschützte Datacenterbox, die über eine dedizierte Leitung an zentrale Server des sBSI angeschlossen wird. Ebenso wird das schulinterne Datennetz jeder Schule aus Sicherheitssicht überprüft und wenn nötig erneuert. Auf der Datacenterbox sind die Serverkomponenten der einheitlichen Schulverwaltungssoftware – bestehend aus Schüler- und Klassenverwaltung sowie einer Stundenplanverwaltung – vorinstalliert. Als Modellprojekt wird zudem der Einsatz eines **elektronischen Klassenbuches** (eKlassenbuch) an einigen Schulen getestet. Dieses Projekt ermöglicht u. a., die **Erziehungsberechtigten unentschuldig fehlender Schülerinnen und Schüler zeitnah per SMS zu informieren**.

Obwohl keine Grundverschlüsselung der Datenverbindungen innerhalb des Verwaltungsnetzes der Schulen bzw. auf den dedizierten Leitungen im sBSI umgesetzt wird, kann die Realisierung wegen der einheitlichen und geprüften Hard- und Software als ausreichend sicher angesehen werden. Die Datenverar-

25 § 6 a BlnDSG

26 § 19 a Abs. 1 Satz 4 i. V. m. § 19 Abs. 2 BlnDSG

beitung erfolgt durch die Datacenterbox – mit Ausnahme des eKlassenbuchs – weiterhin in der einzelnen Schule. Durch die zentrale Bereitstellung wird dennoch ein hohes Sicherheitsniveau erreicht. Personenbezogene Daten werden für die Übertragung zusätzlich verschlüsselt: Sämtliche Schulen sind oder werden mit digitalen Zertifikaten ausgerüstet, die eine gesicherte E-Mail-Kommunikation ermöglichen. Auch die Meldungen für die automatisierte Schülerdatei erfolgen zusätzlich gesichert und in pseudonymisierter Form. Die verwendete Schulverwaltungssoftware wird fortlaufend weiterentwickelt. Dazu haben wir auf bisher nicht umgesetzte Maßnahmen, wie z. B. die fehlende verschlüsselte Datenübertragung zwischen Client und Server sowie nicht vorhandene Protokollierungsmöglichkeiten, hingewiesen.

Bei dem eKlassenbuch handelt es sich um eine webbasierte Anwendung, bei der die Klassenbücher der teilnehmenden Schulen auf zentralen Servern im Rahmen einer Auftragsdatenverarbeitung in Berlin geführt werden sollen. In der Testphase, die einige Klassen in zehn Schulen auf freiwilliger Basis umfasst, erfolgt die Datenhaltung sogar auf den Servern des Softwareanbieters in Österreich. Eine solche Lösung ist grundsätzlich durch vertragliche Regelungen zur Auftragsdatenverarbeitung umsetzbar, in denen u. a. hinreichende Sicherheitsmaßnahmen wie z. B. Verschlüsselung, sichere Zweifaktor-Authentifizierung der zugriffsberechtigten Lehrkräfte sowie Mandantentrennung festgelegt werden. Die Sicherheitsmaßnahmen werden gerade entwickelt und spätestens zum berlinweiten Einsatz vollständig umgesetzt sein. Ein wesentlicher Sicherheitsaspekt ist die Ausstattung der Schulen mit zentral vorkonfigurierten Laptops, um ein ausreichendes Sicherheitsniveau zu erreichen. Wir empfehlen hier, sensitive personenbezogene Daten so weit wie möglich lokal in der jeweiligen Schule zu verarbeiten. Dies ist insbesondere dann zu berücksichtigen, wenn das eKlassenbuch später zur Aufzeichnung von Leistungsdaten der Schülerinnen und Schüler eingesetzt werden sollte.

Die Benachrichtigung der Erziehungsberechtigten über unentschuldigtes Fehlen ihres Kindes mittels „Schulschwänzer-SMS“ ist ohnehin nur als Angebot an die Eltern denkbar, denn niemand ist zum Besitz eines Mobiltelefons verpflichtet. Auch wenn die Eltern sich auf diesem Weg informieren lassen wollen, darf eine von der Schule versandte SMS nur die Bitte um Rückruf enthalten. Eine Kurzmitteilung des Inhalts, dass eine bestimmte Schülerin oder ein bestimmter Schüler fehlt, wäre datenschutzwidrig, denn die Schule kann nicht

sicher davon ausgehen, dass diese personenbezogene Information beim berechtigten Empfänger ankommt (z. B. weil dieser seine Nummer geändert oder das Mobiltelefon weitergegeben hat).

Die derzeit eingeführte einheitliche Schul-IT ist ein begrüßenswerter Fortschritt im Hinblick auf Datenschutz und IT-Sicherheit. Es besteht jedoch noch Raum für Verbesserungen der IT-Sicherheit. Insbesondere beim eKlassenbuch wäre eine dezentrale Lösung wünschenswert. „Schulschwänzer-SMS“ dürfen nur an Eltern versandt werden, die dem zugestimmt haben, und sie müssen sich auf eine Bitte um Rückruf beschränken.

2 Schwerpunkte

2.1 Funkzellenabfragen – von der Ausnahme zur Regel?

Die Strafprozessordnung gibt den Strafverfolgungsbehörden die Möglichkeit, zur Aufklärung besonders schwerer Straftaten von den Telekommunikationsanbietern Auskunft über die Verbindungsdaten sämtlicher Mobilfunktelefonate, die in einer vorgegebenen Zeit in einem bestimmten Gebiet geführt worden sind, zu verlangen.²⁷ Eine solche Maßnahme hat weitreichende Folgen, da sie zum einen in das verfassungsrechtlich geschützte Fernmeldegeheimnis eingreift und zum anderen sehr viele Personen betroffen sein können, ohne dass diese Anlass für die Durchführung einer solchen Maßnahme gegeben haben. An die Zulässigkeit und Durchführung dieser Funkzellenabfragen sind daher hohe Anforderungen zu stellen.

Der Gesetzgeber hat die Maßnahme unter den Vorbehalt der richterlichen Anordnung gestellt. Diese darf erst dann von den Strafverfolgungsbehörden beantragt werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der oder des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Bei der Auswertung der durch eine Funkzellenabfrage erlangten personenbezogenen Daten müssen die Strafverfolgungsbehörden weitere Vorgaben beachten: Die erhobenen Verkehrsdaten sind besonders zu kennzeichnen. Sie sind unverzüglich zu löschen, sobald sie nicht mehr zum Zwecke der Strafverfolgung oder einer möglichen gerichtlichen Überprüfung erforderlich sind. Zudem sind die Betroffenen mit einigen Ausnahmen von der Durchführung einer Funkzellenfrage zu benachrichtigen (insbesondere bei der Abfrage von Bestandsdaten) und auf die Möglichkeit nachträglichen Rechtsschutzes und die hierfür vorgesehenen Fristen hinzuweisen.

Die gesetzlichen Regelungen zur Durchführung von **Funkzellenabfragen** und deren praktische Umsetzung durch die Strafverfolgungsbehörden stehen spätestens seit Bekanntwerden der im Zusammenhang mit Demonstrationen erfolgten Erhebung von über 800.000 Verkehrsdatensätzen durch das LKA Sachsen

²⁷ Siehe § 100g Abs. 1 i. V. m. Abs. 2 Satz 2 StPO

im Februar 2011 in **Dresden** im Fokus der öffentlichen Kritik.²⁸ Die dort durchgeführten Funkzellenabfragen, von denen einige zehntausend unbeteiligte Versammlungsteilnehmende betroffen waren, waren Anlass für die gemeinsame Forderung der Datenschutzbeauftragten des Bundes und der Länder an den Gesetzgeber, den Anwendungsbereich solcher Maßnahmen insbesondere im Hinblick auf deren Verhältnismäßigkeit einzuschränken.²⁹

Im parlamentarischen Bereich gab es in Folge der Dresdner Vorfälle ebenfalls Initiativen zur Überarbeitung der gesetzlichen Regelungen zu Funkzellenabfragen. Der Freistaat Sachsen legte im Bundesrat den Entwurf eines Gesetzes zur Neuregelung der nichtindividualisierten Verkehrsdatenerhebung vor.³⁰ Daneben brachte die Fraktion Bündnis 90/Die Grünen den Entwurf eines Gesetzes zur Neuregelung der nichtindividualisierten Verkehrsdatenerhebung in den Bundestag ein.³¹ Beide Initiativen wurden bislang jedoch nicht verabschiedet.

Anfang 2012 berichteten die Medien über die Durchführung einer **Funkzellenabfrage** im Zusammenhang mit einem Brandanschlag auf ein Kraftfahrzeug im **Berliner Bezirk Friedrichshain-Kreuzberg**. Dies führte erneut zu kontroversen politischen Diskussionen über den Einsatz solcher Maßnahmen. Im Abgeordnetenhaus wurde hierüber im Plenum sowie im Ausschuss für Inneres, Sicherheit und Ordnung und im Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit debattiert.³² Dies veranlasste uns zu einer stichprobenartigen Überprüfung der Umsetzung der gesetzlichen Vorgaben zu Funkzellenabfragen durch die Berliner Strafverfolgungsbehörden im Rahmen von 108 Ermittlungsverfahren in den Jahren 2009 bis 2011.

In unserem Abschlussbericht, der dem Abgeordnetenhaus und den Senatsverwaltungen für Justiz und Verbraucherschutz sowie für Inneres und Sport zugeleitet wurde, haben wir strukturelle Mängel bei der Durchführung der

28 Siehe Bericht des Sächsischen Datenschutzbeauftragten an den Sächsischen Landtag, Drs. 5/6787

29 Siehe Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011: Funkzellenabfrage muss eingeschränkt werden!, siehe Dokumentenband 2011, 16 ff.

30 BR-Drs. 532/11

31 BT-Drs. 17/7033

32 Siehe u. a. Plenarprotokoll 17/7 vom 26. Januar 2012

Maßnahmen feststellen müssen. Dies betrifft insbesondere die Prüfung der Verhältnismäßigkeit der Maßnahme sowie die Umsetzung der Betroffenenrechte. Es entstand oft der Eindruck, dass sich die Strafverfolgungsbehörden der Eingriffsintensität von Funkzellenabfragen entweder nicht bewusst waren oder diese missachtet haben müssen. So wurden sehr häufig Funkzellenabfragen beantragt und durchgeführt, obwohl nicht ersichtlich war, dass während der Tat ein Mobilfunktelefon genutzt wurde. Oft boten sich auch andere, weniger gravierende Ermittlungsansätze an, denen vor Durchführung der Funkzellenabfrage nicht oder nicht abschließend nachgegangen wurde. Eine über den Gesetzeswortlaut hinausgehende Begründung des Einsatzes einer solchen Maßnahme fand in der Regel nicht statt. In einigen Fällen wurden sogar Funkzellenabfragen durchgeführt, obwohl keine Straftat von auch im Einzelfall erheblicher Bedeutung vorlag.

Die fehlerhafte Durchführung von Funkzellenabfragen ist durch die unklaren gesetzlichen Vorgaben sowie durch die inkonsequente und uneinheitliche Umsetzung dieser Vorschriften bedingt. Insoweit sind Gesetzgeber und Verwaltung gefordert, Änderungen vorzunehmen.

In den zurückliegenden Ermittlungsverfahren sind die Betroffenen, soweit erforderlich und noch nicht erfolgt, von entsprechenden Maßnahmen zu informieren und über ihre Rechtsschutzmöglichkeiten aufzuklären. Darüber hinaus sind nicht mehr erforderliche Daten, die durch Funkzellenabfragen erlangt worden und noch gespeichert sind, unverzüglich zu löschen. Die Löschung bzw. die Entscheidung über eine weitere Speicherung der Daten sollte nebst Begründung dokumentiert werden. Die weiterhin gespeicherten Daten sind eindeutig als aus einer Funkzellenabfrage stammend zu kennzeichnen.

Zur praktischen Durchführung zukünftiger Funkzellenabfragen empfiehlt es sich, folgende Vorgaben in Dienstanweisungen festzuschreiben:

- Die Begründung des Einsatzes von Funkzellenabfragen sowie der Durchführung der Benachrichtigungs- und Löschpflichten sind einzelfallbezogen zu dokumentieren.
- Die Umsetzung der Kennzeichnungspflichten ist standardisiert durchzuführen.

- Internen und externen Kontrollinstanzen ist die Möglichkeit zu geben, regelmäßig und umstandslos die Umsetzung der gesetzlichen Vorgaben prüfen zu können.

Daneben sollte sich das Land Berlin für folgende Änderungen der Strafprozessordnung einsetzen:

- Die Bestimmungen zur Durchführung von Funkzellenabfragen sind insbesondere im Hinblick auf die Verhältnismäßigkeit der Maßnahme und den Zweckbindungsgrundsatz zu konkretisieren und enger zu fassen.
- Es ist eine Dokumentationspflicht für die Begründung des Einsatzes von Funkzellenabfragen sowie die Durchführung der Benachrichtigungs- und Löschpflichten einzuführen.
- Der Anwendungsbereich für Funkzellenabfragen ist zumindest auf konkret benannte Straftaten³³ zu beschränken.
- Es bedarf über den Verweis auf die Erforderlichkeit zur Strafverfolgung oder eine mögliche gerichtliche Maßnahmenüberprüfung hinaus genauer Vorgaben für die Löschung der aus Funkzellenabfragen erlangten Daten.
- Um eine unabhängige Evaluation zu ermöglichen, sollte eine Berichtspflicht der Strafverfolgungsbehörden gegenüber dem Parlament eingeführt werden.

Die Staatsanwaltschaft hat in einer ersten Stellungnahme die Auffassung vertreten, der Berliner Beauftragte für Datenschutz und Informationsfreiheit sei nicht befugt, das Vorgehen der Staatsanwaltschaft im Vorfeld einer richterlichen Anordnung zu überprüfen. Zudem sei es „praxisfern“, den Strafverfolgungsbehörden erst dann eine Funkzellenabfrage zu ermöglichen, wenn andere Spuren ausgewertet worden seien und nicht zum Ermittlungserfolg geführt hätten.

In beiden Punkten ist die Auffassung der Staatsanwaltschaft rechtsirrig. Das Berliner Datenschutzgesetz³⁴ nimmt die Gerichte von der Kontrolle durch den Datenschutzbeauftragten aus, soweit sie nicht in Verwaltungsangelegenheiten tätig werden. Die Staatsanwaltschaft unterliegt dagegen wie jede andere öffentliche Stelle der Datenschutzkontrolle.

³³ Siehe § 100a Abs. 2 StPO

³⁴ § 24 Abs. 2 BlnDSG

Zwar haben die Gerichte die Rechtmäßigkeit der von der Staatsanwaltschaft beantragten Maßnahme zu prüfen,³⁵ jedoch kann sich die Staatsanwaltschaft deshalb der Kontrolle durch den Datenschutzbeauftragten nicht entziehen. Gerade die durchgeführte Prüfung ausgewählter Ermittlungsverfahren mit Funkzellenabfragen hat gezeigt, wie wichtig die unabhängige Datenschutzkontrolle ist: Da vielfach die gesetzlich vorgeschriebene Benachrichtigung Betroffener unterblieb, konnten diese keinen Rechtsschutz erlangen.

Auch ist es nicht hinnehmbar, wenn eine Strafverfolgungsbehörde die Vorgabe des Gesetzgebers, eine so einschneidende Maßnahme wie die massenhafte Funkzellenabfrage erst als letztes Mittel (ultima ratio) einzusetzen, als „praxisfern“ bezeichnet und deshalb offenbar zu ignorieren bereit ist.

Immerhin soll in einer gemeinsamen Arbeitsgruppe mit Vertretern des Polizeipräsidenten, des Generalstaatsanwalts sowie der Staats- und Staatsanwaltschaft ein Konzept erarbeitet werden, das Versäumnisse bei der Kennzeichnung, Benachrichtigung und Löschung von Funkzellendaten künftig vermeiden soll. Dieses Konzept soll mit uns abgestimmt werden, was bislang noch nicht geschehen ist.

Der Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit hat dem Plenum des Abgeordnetenhauses empfohlen, den Senat aufzufordern, auch in den Fällen eine Information der Öffentlichkeit auf der Internetseite der Staatsanwaltschaft zu prüfen, in denen eine individuelle Benachrichtigung Betroffener zu Recht unterblieben ist.³⁶

Offensichtlich sind Funkzellenabfragen in vielen Deliktsbereichen entgegen der gesetzlichen Vorgabe zum alltäglichen Ermittlungsinstrument geworden. Aufgrund der Eingriffstiefe und Streubreite darf ihr Einsatz jedoch nicht zur Regel werden. Die stärkere Begrenzung der Durchführung solcher Maßnahmen ist durch den Gesetzgeber und die Strafverfolgungsbehörden sicherzustellen. Die Staatsanwaltschaft unterliegt auch dann der Kontrolle durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit, wenn die von ihr beantragten Maßnahmen unter Richtervorbehalt stehen.

35 Siehe § 162 Abs. 2 StPO

36 Protokoll der Ausschuss-Sitzung vom 22. Oktober 2012

2.2 Zehn Vorschläge zur Verbesserung der EU-Datenschutz-Grundverordnung

Die Initiative der Europäischen Kommission, mit einer Datenschutz-Grundverordnung das Datenschutzrecht in Europa zu harmonisieren und zu modernisieren,³⁷ ist zu begrüßen. Um dieses Ziel zu erreichen, muss zum einen verhindert werden, dass der Entwurf im weiteren europäischen Gesetzgebungsverfahren³⁸ verwässert wird. Das hohe deutsche Datenschutzniveau, das nach Angaben der Kommission maßgeblichen Einfluss auf die Formulierung des Verordnungsentwurfs gehabt hat, darf nicht im Interesse einer falsch verstandenen Rechtsangleichung abgesenkt werden.³⁹ Deshalb sollte der Verordnungsentwurf, der bei seiner Verabschiedung als europäisches Datenschutzgesetz an die Stelle des Bundesdatenschutzgesetzes (BDSG) treten wird, in mehreren Punkten noch verbessert werden. Unabhängig von den detaillierten Stellungnahmen, die sowohl die nationale Konferenz der Datenschutzbeauftragten des Bundes und der Länder als auch die Art. 29-Gruppe der europäischen Datenschutzbehörden abgegeben haben,⁴⁰ seien hier ohne Anspruch auf Vollständigkeit zehn Vorschläge genannt, die für die praktische Anwendung der Verordnung von besonderer Bedeutung sind:

Die Aufsichtsbehörde sollte das Recht auf anlasslosen Zugang zu Geschäfts- und Diensträumen behalten.

Anders als nach dem BDSG kann die Aufsichtsbehörde nach dem Entwurf nur bei einem Anlass (Verdacht eines Datenschutzverstoßes) Vor-Ort-Kontrollen durchführen.⁴¹ Verantwortliche Stellen würden die Möglichkeit erhalten, durch das Bestreiten eines Anlasses eine Überprüfung vor Ort zu verhindern. Eine Prüfung wäre dann in der Regel nur im Anschluss an eine richterliche Entscheidung möglich. Etwaige Beweise für Datenschutzverstöße könnten rechtzeitig vernichtet werden.

37 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 25. Januar 2012, KOM(2012) 11 endgültig

38 Hierzu und generell zum neuen europäischen Rechtsrahmen siehe 14.1

39 Siehe Einleitung

40 Siehe 14.1 sowie Dokumentenband 2012, S. 10, 19

41 Art. 53 Abs. 2b

Die Bestellpflicht der oder des betrieblichen Datenschutzbeauftragten sollte nicht zu einem Ausnahmetatbestand werden.

Die vorgesehene Bestellpflicht erst ab 250 Beschäftigten führt dazu, dass in Deutschland nur 0,3 % aller Unternehmen verpflichtet wären, eine mit dem betrieblichen Datenschutz beauftragte Person zu bestellen. Dies wäre ein Rückschritt, da sich die Rechtsfigur des betrieblichen Datenschutzbeauftragten in Deutschland bewährt hat. Das Fehlen betrieblicher Datenschutzbeauftragter führt dazu, dass für die Aufsichtsbehörden ein erhöhter Kontrollbedarf entsteht. Aus diesem Grund empfehlen wir, den Schwellenwert von 250 auf 50 zu senken. Unabhängig von der Beschäftigtenzahl sollte bei risikobehafteten Kerntätigkeiten (wie in Call-Centern oder Detekteien) und bei Sensitivität der verarbeiteten Daten (wie in Arztpraxen und Anwaltskanzleien) stets eine Bestellpflicht bestehen.

Die Rechte der betrieblichen und behördlichen Datenschutzbeauftragten sind zu stärken.

Verantwortliche Stellen haben die Möglichkeit, die Amtszeit der oder des Datenschutzbeauftragten auf zwei Jahre zu beschränken. Eine nur befristet tätige Person kann die Belange des Datenschutzes nicht voll wahrnehmen, ohne persönliche Nachteile befürchten zu müssen. Sie verliert hierdurch die Unabhängigkeit. Wenn sich die verantwortliche Stelle (der Arbeitgeber) dafür entscheidet, nach zwei Jahren eine neue Person zu bestellen, kann die vorherige evtl. betriebsbedingt gekündigt werden. Eine mit dem Datenschutz beauftragte angestellte Person wäre somit arbeitsrechtlich schlechter gestellt als andere Angestellte. Dies hätte zur Folge, dass es schwierig wäre, qualifizierte Datenschutzbeauftragte zu finden. Die oder der angestellte Datenschutzbeauftragte sollte deshalb grundsätzlich unbefristet bestellt werden und einen besonderen Kündigungsschutz genießen, wie es der gegenwärtigen Rechtslage in Deutschland entspricht.

Das Ungleichgewicht zwischen verantwortlicher Stelle und Betroffenen ist kein geeignetes Kriterium für die Freiwilligkeit der Einwilligung.

Nach dem BDSG ist nur die freiwillig erteilte Einwilligung wirksam. Der Entwurf will die Freiwilligkeit der Einwilligung dadurch sicherstellen, dass Einwilligungen bei einem „erheblichen Ungleichgewicht“ zwischen verarbeitender Stelle und betroffener Person keine Rechtsgrundlage für eine Verarbeitung

darstellen.⁴² Es sind aber auch Fälle denkbar, in denen zwar kein strukturelles Ungleichgewicht besteht, trotzdem aber keine freiwillige Einwilligung vorliegt. Auf der anderen Seite kann auch trotz eines Ungleichgewichts der Vertragspartner Freiwilligkeit gegeben sein. Falls etwa ein Monopolist beschließt, Werbung zukünftig nur noch bei Vorliegen einer Einwilligung des Betroffenen zu machen, bestände an der Freiwilligkeit kein Zweifel. Selbst im Beschäftigungsverhältnis gibt es Fälle von Freiwilligkeit, etwa wenn eine leitende Person in die Übermittlung ihrer personenbezogenen Daten zur Konzernmutter für ein Incentive-Programm oder andere Anreizsysteme bzw. die Aufnahme ihrer Daten in die konzernweit genutzte Karrieredatei für Managerinnen und Manager zustimmt.

Es sind Rechtsgrundlagen für Auskunfteien zu schaffen.

Die Verordnung enthält zwar 91 Artikel, aber nur wenige und deshalb sehr allgemein gehaltene Rechtsvorschriften, die eine Datenverarbeitung gestatten. Das BDSG regelt genau, unter welchen Voraussetzungen Daten an Auskunfteien übermittelt werden dürfen, welche Daten Auskunfteien speichern dürfen und unter welchen Bedingungen diese Daten an ihre Kunden übermittelt werden können. Durch die Regelung auch vieler Einzelfälle ist es dem Bundesgesetzgeber möglich, eine weitgehend praktische Konkordanz zwischen den Interessen der Auskunftei, der Kunden der Auskunftei (z. B. einer Bank) und der Betroffenen zu erreichen. Nach dem Vorschlag der Kommission müssten sämtliche Datenflüsse von und zu einer Auskunftei an Art. 6 Abs. 1 f) des Entwurfs gemessen werden. Diese Norm ist zu allgemein, um die Betroffenen vor einer rechtswidrigen Datenverarbeitung im Auskunfteibereich ausreichend zu schützen. Auch erwähnt Art. 6 Abs. 1 f) der Grundverordnung nicht berechnigte Interesse eines Dritten, die gerade im Auskunfteibereich Prüfungsmaßstab sind. Der Verordnungsgeber geht offenbar davon aus, dass bei der verantwortlichen Stelle berechnigte Interessen gegeben sind, wenn Dritte ein berechtigtes Interesse an den Daten haben. Zu größerer Rechtsklarheit trägt dies sicher nicht bei.

Es sollten strengere Regelungen für das Scoring eingeführt werden.

Die Verordnung schützt die von einem Scoring-Verfahren Betroffenen nicht ausreichend. Es sollte geregelt werden, dass

42 Art. 7 Abs. 4

- für das Scoring-Verfahren keine sensitiven Daten verwendet werden und
- die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit erheblich sind und
- für die Berechnung des Wahrscheinlichkeitswerts keine Anschriftendaten genutzt werden. Das Scoring von Anschriften führt dazu, dass ganze Stadtteile oder Gegenden stigmatisiert werden.

Werbung sollte nur mit Einwilligung der Betroffenen möglich sein.

Der Entwurf regelt nur, dass Betroffene gegen Direktwerbung Widerspruch einlegen können. Es gibt aber keine spezifischen werberechtlichen Erlaubnistatbestände. Es ist zu befürchten, dass die Anwendung der allgemeinen Datenverarbeitungsregeln (Abwägung der berechtigten Interessen des Werbetreibenden mit den Interessen der Beworbenen)⁴³ dazu führt, dass die Bürgerinnen und Bürger zukünftig mehr unerwünschte Werbung als bisher erhalten. Besser wäre es, wenn der Gesetzgeber – trotz des massiven Widerstands der Werbelobby – Werbung und Adresshandel für Werbezwecke nur noch bei Vorliegen einer Einwilligung gestattet.

Bei Videoüberwachungen sollte weiterhin eine Hinweispflicht vorgesehen sein.

Anders als im Auskunftsbereich erscheint es möglich, mit Hilfe von Art. 6 Abs. 1 f) der Grundverordnung eine Interessenabwägung vorzunehmen, die in etwa der des BDSG gleicht. Allerdings empfehlen wir, auch wenn dies eine gewisse Durchbrechung der Technikneutralität darstellen könnte, an der Hinweispflicht wie im BDSG festzuhalten.

Es fehlen Pflichten zu Anonymisierung und Pseudonymisierung.

Anders als das Telemediengesetz (TMG) oder das BDSG verwendet die Verordnung nicht die Begriffe Anonymisierung und Pseudonymisierung. Es sollte zumindest klargestellt werden, dass eine Verarbeitung von Daten nach dem Stand der Technik auch Anonymisierungs- und Pseudonymisierungsmöglichkeiten ausschöpfen muss. Betroffene sollten ein Recht auf Pseudonymisierung

43 Art. 6 Abs. 1 f)

ihrer Daten haben. Die Regeln des TMG zur Beschränkung von Nutzungsprofilen im Internet sollte der europäische Gesetzgeber übernehmen.

Kontrollrechte gegenüber Auftragsdatenverarbeitern sind zu stärken.

Eine wirksame Kontrolle des Auftragsdatenverarbeiters ist nur möglich, wenn der verantwortlichen Stelle ein Kontrollrecht vor Ort eingeräumt wird. Einige Datenskandale, an denen Auftragnehmer beteiligt waren, haben den deutschen Gesetzgeber veranlasst, die Kontrollrechte der Auftraggeber zu stärken. Da der Auftraggeber Herr der Daten bleibt, muss er auch die Möglichkeit erhalten, sich vor Ort davon zu überzeugen, dass der Auftragnehmer seine Weisungen beachtet.

Der Entwurf für eine europäische Datenschutz-Grundverordnung eröffnet die Chance für eine überfällige Modernisierung des Datenschutzrechts. Sie darf nicht vertan werden, indem der Entwurf verwässert wird. Er sollte vielmehr in einigen Punkten verbessert werden, um das gegenwärtige Datenschutzniveau zu sichern und weiterzuentwickeln.

2.3 BYOD – „Bring your own device“: Arbeiten mit privaten Endgeräten

„Bring your own device“ (BYOD) ist eine aktuelle Entwicklung, bei der Beschäftigte ihre privaten mobilen Geräte wie Smartphones, Notebooks oder Tablet-PCs am Arbeitsplatz verwenden und darauf die vom Arbeitgeber bereitgestellten Ressourcen wie E-Mail, Geschäftskontakte, Kalender und Datenbanken genauso nutzen wie ihre persönlichen Einstellungen und Daten. Das Phänomen ist in nahezu allen Unternehmen angekommen. Meist entziehen sich jedoch die Privatgeräte dem IT-Management, mit dem der Arbeitgeber die eigenen informationstechnischen Geräte – auch aus Gründen des Datenschutzes – verwaltet und kontrolliert. Ihr Einsatz birgt deshalb auch datenschutzrechtliche und technische Risiken. In der öffentlichen Verwaltung ist daher der Einsatz privater Datenverarbeitungsgeräte bisher prinzipiell untersagt.

Selten zuvor wurde ein Trend so vielseitig diskutiert wie das Thema BYOD. Die neuen „Spielzeuge“ – technisch sehr moderne und äußerst mobile Gerä-

te – sollen nicht daheim liegen, sondern in die vorhandene IT-Landschaft des Arbeitgebers integriert werden. Die Initiative kann dabei genauso gut vom Arbeitnehmer wie vom Arbeitgeber ausgehen. Mit der Vielfalt an Geräten sehen sich die mit der Betreuung der IT beauftragten Beschäftigten einer stetig steigenden Zahl zu verwaltender Betriebssysteme und Plattformen ausgesetzt. Doch wie kommt es zu diesem Trend? Als Grund wird angegeben, dass die IT in der öffentlichen Verwaltung und den Unternehmen veraltet und dadurch zu langsam sei. Dazu kommt, dass die notwendigen Sicherheitsmaßnahmen als Behinderungen wahrgenommen werden. Gerade bei der schnell fortschreitenden Entwicklung von mobilen Geräten (insbesondere Smartphones und Tablet-PCs) wollen die Beschäftigten ihre privaten Geräte einsetzen, da diese leistungsfähiger und nutzerfreundlicher sind. Die Mitarbeiterinnen und Mitarbeiter können berufliche und private Aufgaben kombinieren, was zu mehr Motivation und einer deutlichen Steigerung der Effizienz und Produktivität beitragen kann. Das Unternehmen erscheint als flexibler und attraktiver Arbeitgeber und spart Geld für die Hardware. Selbstverständlich birgt eine Durchmischung beruflicher und privater Aspekte auch Gefahren. Neben datenschutzrechtlichen Vorkehrungen müssen auch technische Rahmenbedingungen geschaffen werden. Soll BYOD in die geschäftliche Kommunikation eines Unternehmens integriert werden, ist daher die Entwicklung einer Gesamtstrategie sinnvoll.

Schriftliche Vereinbarung zur Regelung der rechtlichen und technischen Details

Ausgangspunkt der Überlegungen ist, dass auch bei der Verarbeitung personenbezogener Daten auf privaten Geräten das Unternehmen die verantwortliche Stelle im Sinne des Datenschutzrechts bleibt.⁴⁴ Sie ist für die ordnungsgemäße Datenverarbeitung verantwortlich. Es empfiehlt sich daher, schriftliche Festlegungen gegenüber den Beschäftigten in Form einer Betriebsvereinbarung, in bestimmten Fällen auch einer Individualvereinbarung zu treffen. BYOD ist als technische Einrichtung grundsätzlich dazu geeignet, Verhalten und Arbeitsweise der oder des Beschäftigten zu überwachen. Bei der Ausgestaltung der Vereinbarung und Nutzung hat daher der Betriebsrat ein Mitbestimmungsrecht.⁴⁵ Eine

44 § 3 Abs. 7 BDSG

45 § 87 Abs. 1 Nr. 6 BetrVG. Entsprechendes gilt für das Personalvertretungsrecht, falls der Einsatz privater Computer in der öffentlichen Verwaltung zugelassen werden sollte.

Regelung, wie die Beschäftigten das Gerät zu nutzen haben, löst ebenso das Mitbestimmungsrecht aus.⁴⁶

Wichtig ist, dass eine individuelle Vereinbarung auf der Freiwilligkeit beider Seiten basiert. Für die Beschäftigten ist dieser Punkt bedeutsam, um nicht zur Nutzung privater Geräte verpflichtet zu werden. Duldet der Arbeitgeber die Nutzung der Geräte ohne Vereinbarung, kann die Nutzung als betriebliche Übung zu werten sein, was zu Rechtsunsicherheit bei der einzelnen Ausgestaltung führt. Deshalb sind in jedem Fall schriftliche Vereinbarungen zu empfehlen.

Zugriff auf die Daten

Eine Vereinbarung sollte zunächst Vorgaben enthalten, wie zwischen privaten und geschäftlichen Daten getrennt werden soll, und wer wann und in welcher Form Zugriff auf die Daten hat. In der Vereinbarung sollte zudem festgehalten sein, dass die Beschäftigten am Endgerät bestimmte Sicherheitsvorkehrungen einzurichten haben oder diese nicht mehr verändern dürfen. Grundsätzlich darf niemand ohne Einwilligung des Eigentümers bzw. Besitzers auf dessen Geräte zugreifen. Will also das Unternehmen Dokumente, Daten oder Apps auf dem Gerät speichern, empfiehlt es sich, auch dies zu regeln und die erforderlichen Prozeduren schriftlich zu vereinbaren. Werden bereits gespeicherte Daten auf dem Gerät verändert, wäre eine solche Vereinbarung auch aus strafrechtlicher Sicht relevant.⁴⁷

Beim Zugriff auf Daten der Beschäftigten muss danach unterschieden werden, ob es sich trotz einer technischen Trennung von dienstlichen und privaten Daten tatsächlich um berufliche Daten handelt. Ein Zugriff auf private Daten ist nur zu dem Zweck erlaubt, um sie der einen oder anderen Kategorie zuzuordnen zu können. Abgesehen davon, dass es in Arbeitsverhältnissen häufig an der Freiwilligkeit fehlt, kommt hinzu, dass es sich überwiegend auch um Daten Dritter handeln wird. Deren Einwilligung ist in diesen Fällen kaum möglich. Gleiches gilt für den Zugriff auf E-Mails. Während Dienst-E-Mails vom Arbeitgeber gelesen werden können, ist der Zugriff auf die privaten E-Mails

46 § 87 Abs. 1 Nr. 1 BetrVG

47 Ein solches Vorgehen kann den Straftatbestand der Datenveränderung nach § 303a StGB erfüllen.

nicht zulässig, da hier schutzwürdige Interessen der Betroffenen, z. B. das Telekommunikationsgeheimnis, grundsätzlich überwiegen.

Weiterhin muss geklärt werden, wann und wie Daten gelöscht werden können. Nach dem Bundesdatenschutzgesetz besteht eine Pflicht zur Löschung, wenn die Speicherung personenbezogener Daten unzulässig ist oder Daten für geschäftliche Zwecke verarbeitet werden und ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.⁴⁸ Die Frage wird außerdem relevant, wenn das Endgerät verloren geht. Von einer möglichen Fernlöschung wären dann u. U. auch private Daten betroffen. Eine verantwortliche Stelle ist zudem verpflichtet, Betroffene und die Aufsichtsbehörden zu informieren, wenn Dritten personenbezogene Daten zur Kenntnis gelangt sind, beispielsweise bei Verlust.⁴⁹ Daher sollte auch diese Pflicht in eine Vereinbarung aufgenommen werden. Beschäftigte, die private Geräte mit dienstlichen Daten verlieren, müssen ihren Arbeitgeber informieren, um ihm die Erfüllung seiner Meldepflichten zu ermöglichen.

Die Nutzung des privaten Smartphones durch Dritte ist zu untersagen und es ist sicherzustellen, dass wirklich nur Berechtigte auf unternehmensinterne Daten Zugriff nehmen können. Anderenfalls könnte eine unzulässige Übermittlung personenbezogener Daten vorliegen. Bei notwendigen Reparaturen und Wartungsarbeiten muss das Gerät an die IT-Abteilung des Unternehmens übergeben werden. Eine Weitergabe an Dritte sollte ausgeschlossen werden. Wenn doch eine Übergabe an einen unternehmensexternen Experten notwendig wird, muss vereinbart werden, dass zuvor ggf. eine Datensicherung durchgeführt wird und sensible Daten gelöscht werden können.

Arbeitszeit, Kostenverteilung, Beendigung

Aus Arbeitnehmersicht ist es sinnvoll, Regelungen zur Arbeitszeit und zur Kostenverteilung zwischen Unternehmen und Arbeitnehmer für Gerät, Software und Nutzungsentgelte zu treffen. Grundsätzlich muss der Arbeitgeber der oder dem Beschäftigten Aufwendungsersatz für die durch die Nutzung entstandenen Kosten des privat bezahlten Dienstes leisten.⁵⁰ Es sollte geklärt werden, ob es

48 § 35 Abs. 2 BDSG

49 Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten bzw. von Dritten nach § 42a BDSG bzw. § 18 a BlnDSG, siehe 15.2

50 §§ 675, 670 BGB

einen pauschalen oder einzelnachweisbasierten Ersatz geben wird. Am einfachsten und datenschutzfreundlichsten klärt sich die Kostenfolge bei einer Flatrate. Sinnvoll ist es, gleich zu Beginn der Nutzung Maßnahmen für ein mögliches Ende des Gebrauchs zu treffen. So kann festgehalten werden, ob es sich um eine befristete Möglichkeit zur Nutzung handelt und in welcher Form die dienstlichen Daten nach Beendigung an den Arbeitgeber herauszugeben sind. Außerdem sollte bestätigt werden, dass die oder der Beschäftigte nach Auflösung des Arbeitsverhältnisses verpflichtet ist, dienstlich erlangte Daten an den Arbeitgeber herauszugeben.⁵¹

Technische Aspekte

Die Nutzung von privaten mobilen Geräten am Arbeitsplatz ist außerdem mit technischen Risiken verbunden. Grundsätzlich gibt es Maßnahmen, die eine sichere Nutzung von mobilen Geräten ermöglichen.

Mögliche Bedrohungen

Eine wesentliche Bedrohung ist der unberechtigte Zugriff auf das Gerät und damit auf die lokal gespeicherten Daten. Ein mögliches Szenario wäre ein Diebstahl oder der Einsatz einer Schadsoftware. Dabei kann z. B. ein Trojaner Tastatureingaben mitlesen und diese zu einem definierten Zeitpunkt zu einem vorher eingetragenen Ziel senden. Nach einem Diebstahl könnten u. a. Kontaktdaten, Anruflisten, Kennwörter, Fotos und SMS extrahiert werden. Auch könnten Unbefugte Kenntnis von wichtigen Unterlagen erlangen oder Schadsoftware Daten verfälschen oder zerstören.

Die Anbindung der Geräte an die Informationstechnik des Arbeitgebers kann insbesondere zur Gefährdung dieser Infrastruktur führen. Kommunikationseinrichtungen können durch „DoS“⁵²-Angriffe gestört werden. Auch können über diese Wege unerlaubte Zugriffe auf im Firmennetz gespeicherte Daten erfolgen sowie durch ein nicht ausreichend geschütztes Gerät Schadsoftware eingeschleust werden. Auf Smartphones und Tablet-PCs existieren zahlreiche Apps. Gefährdungen können nicht nur von systemeigenen Apps ausgehen, sondern auch von Cloud-Apps und -Services, auf die über das Gerät zugegriffen

51 Dies basiert auf § 667 BGB.

52 „Denial of Service“ als Folge einer Überlastung z. B. eines Mailservers durch Überflutung mit Nachrichten

wird. Apps können über weitreichende Rechte verfügen und führten schon zu so manchem Skandal, weil komplette Adressbücher an Unbefugte übertragen wurden.

Sicherheitsmaßnahmen

Neben den bekannten Risiken und Maßnahmen beim herkömmlichen PC-Einsatz sind die neuen Betriebssystemplattformen und der Einsatz von „Apps“ zu betrachten.

Besonders hervorzuheben ist die Authentifikation. Der Nutzer muss sich gegenüber dem System am sichersten per Zwei-Faktoren-Authentifizierung⁵³ anmelden. Beim Smartphone sollte nicht nur die Sim-Kartensperre, sondern auch die Bildschirmsperre aktiviert sein, damit z. B. ein Angreifer in einer Konferenzpause nicht „auf die Schnelle“ die im Handy gespeicherten Informationen zur Kenntnis nehmen kann. Die Integration in die Infrastruktur des Arbeitgebers sollte nur gesichert erfolgen. Dies kann z. B. verschlüsselt über VPN⁵⁴ realisiert werden. Aktuelle Virens Scanner auf den mobilen Geräten sind obligatorisch.

Als weitere Sicherheitsmaßnahme kann eine sinnvolle Protokollierung dienen, die eine Feststellung von Angriffen ermöglicht. Die Installation eines Patch-managements reduziert die Gefahr, dass Sicherheitslücken durch Angreifer genutzt werden. Auch kann ein mobiles Gerät durch Desktop-Virtualisierung in zwei Bereiche – Arbeit und Privat – unterteilt werden. Bei einem Anbieter werden hierbei zwei Betriebssysteme installiert. Dienstliche Daten können so z. B. grundsätzlich im Rechenzentrum gespeichert werden. Sollten doch Daten lokal auf dem Gerät gespeichert worden sein, kann die IT-Abteilung eine Löschung aus der Ferne einleiten. Beim „**Application Streaming**“ sind nicht nur die Daten, sondern auch die Anwendungen im gesicherten Rechenzentrum des Arbeitgebers gespeichert. Ausschließlich die Benutzeroberfläche wird auf dem mobilen Gerät zur Verfügung gestellt. Bei Bedarf werden dann Anwendungen auf das mobile Gerät per Knopfdruck übertragen.

53 Wie z. B. bei einer Smartcard durch Besitz und Wissen (Karte und PIN)

54 Virtual Private Network

Zur Wahrung der Vertraulichkeit und Integrität sollten Daten nur **verschlüsselt** gespeichert werden. Dabei kann entweder der komplette Speicher des Gerätes verschlüsselt werden oder es können verschlüsselte Bereiche (Container) erzeugt werden, in denen Daten abgelegt werden.

Der Arbeitgeber kann auch eine Software zum „Mobile Device Management (MDM)“ einsetzen. Diese erlaubt es, die eingesetzten Geräte zentral zu verwalten. Die Möglichkeiten dieser Werkzeuge sind sehr vielfältig. So kann die PIN-Eingabe erzwungen, Rechte verteilt und überwacht und Daten auf gestohlenen oder verlorenen Geräten ferngelöscht werden. Es ist jedoch zu berücksichtigen, dass meist nicht alle Betriebssystemplattformen gleichermaßen gut unterstützt werden.

Das BSI⁵⁵ hat ein Papier zu diesem Thema angekündigt. Es ist anzunehmen, dass auch Maßnahmenempfehlungen im Grundschatzkatalog des BSI folgen werden.

Das Phänomen BYOD ist weiter zu beobachten. Bestimmte Probleme, Bedrohungen und Sicherheitsmaßnahmen sind bekannt, Lösungen bereits diskutiert und verfügbar. Durch die Kombination verschiedener technischer und rechtlicher Maßnahmen müssen die Risiken beherrscht werden, die durch die Nutzung privater Datenverarbeitungsgeräte im beruflichen Umfeld entstehen. Deshalb sollte BYOD in der öffentlichen Verwaltung weiterhin die Ausnahme bleiben.

2.4 Wann dürfen Apothekenrechenzentren Verordnungsdaten weitergeben?

Bei einer Kontrolle eines in Bremen ansässigen Apothekenrechenzentrums stellte die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen unzulässige Datenflüsse fest. Wir nahmen dies zum Anlass, auch die Verarbeitung von Verordnungsdaten durch Berliner Rechenzentren zu prüfen.

55 Bundesamt für Sicherheit in der Informationstechnik

Die Versicherten der Gesetzlichen Krankenversicherung (GKV) reichen jedes Jahr Millionen von Rezepten bei Apotheken ein. Die Bezahlung (abzüglich der gesetzlichen Zuzahlung) übernehmen die Krankenkassen. Zu Zwecken der Abrechnung übermitteln die Apotheken Angaben über die abgegebenen Arzneimittel und die hierfür ausgestellten Rezepte an die Krankenkassen. Sie schalten hierfür Rechenzentren ein, die sowohl Apothekerverbänden als auch anderen Eigentümern gehören.

Der Gesetzgeber hat den Apothekenrechenzentren (ARZ) auferlegt, die von ihnen verarbeiteten Daten nur für die Zwecke der Abrechnung zu verarbeiten. Zwei Ausnahmen sind vorgesehen: Zum einen haben die ARZ die Verordnungsdaten an einige öffentliche Stellen zu übermitteln, die sie im Rahmen ihrer Aufgaben innerhalb der GKV weiterverarbeiten. In jedem dieser Fälle sind spezifische Regelungen getroffen, inwieweit die jeweilige Stelle erfahren darf, auf welche Versicherten und welche Ärzte sich die erhaltenen Daten beziehen. Als Dienstleister für die Übermittlungen an die Kassenärztlichen Vereinigungen schalten die ARZ die ebenfalls in Berlin ansässige **„Gesellschaft für zentrales Datenmanagement und Statistik im Gesundheitswesen“** ein. Eine eigenständige Verarbeitung der Verordnungsdaten ist dieser nicht gestattet. Diesbezügliche Werbung wurde von der Gesellschaft noch vor unserer Prüfung eingestellt. Zum anderen dürfen die ARZ die Verordnungsdaten auch für eigene oder fremde Zwecke nutzen und an andere Stellen übermitteln, dies jedoch nur, wenn die Daten zuvor so verändert wurden, dass ein Bezug zu den einzelnen Versicherten und verschreibenden Ärzten nicht mehr hergestellt werden kann. Eine solche Veränderung wird als **Anonymisierung** bezeichnet.

Es besteht ein großes wirtschaftliches Interesse an der Auswertung der Verordnungen. Solche Interessen gibt es nicht nur bei den Sozialleistungsträgern und anderen Beteiligten der GKV, sondern auch bei Apothekern und Pharmaunternehmen. Die ARZ sind daher bestrebt, eine vielfältige Auswertung der Daten zu ermöglichen. Wann überschreiten sie dabei die gesetzlichen Schranken? Dies ist offensichtlich dann der Fall, wenn Verordnungsdaten so an Dritte weitergegeben wurden, dass diese zu einem Rezept auch die Versicherungsnummer des Patienten oder die Arztnummer des verschreibenden Arztes bestimmen können. Presseberichten zufolge wurde dies teilweise von ARZ außerhalb Berlins praktiziert. Andererseits ist es sicher zulässig, wenn ein ARZ aus jedem Verordnungsdatensatz alle Hinweise auf Patienten und verschreibende Ärzte löscht

und die verbleibenden Daten selbst nutzt oder an Dritte weitergibt. Stattdessen wählt die Rezeptabrechnungsstelle Berliner Apotheker (RBA) einen Mittelweg: Teilweise wird die Versichertennummer durch einen Code ersetzt, der sich aus ihr errechnet. Teilweise wird der Arztbezug durch eine Angabe über die Zugehörigkeit des Arztes zu einer Gruppe von Ärzten ersetzt. Welche Ärzte welcher Gruppe angehören, wird dabei vom Informationsempfänger vorgegeben.

Der Versichertenbezug

Das Ersetzen der Versichertennummer mit einem Code ist eine Veränderung, die der Gesetzgeber als Pseudonymisierung bezeichnet, zumindest falls eine Rückrechnung nur schwer möglich ist.

Ist die Regel zur Berechnung des Codes öffentlich bekannt, so ist ein Rückrechnen durch Anwendung der Regel auf alle möglichen Versicherungsnummern möglich. Mit der entstehenden Tabelle kann jeder Code aufgelöst werden. In unserer Prüfung mussten wir in einem Verfahren die Anwendung einer so schwachen Methode feststellen. Derart codierte Daten darf ein ARZ weder nutzen noch weitergeben.

Ist die Regel nur dem ARZ (oder einer von ihr beauftragten Stelle) bekannt und wird sie geheim gehalten, besteht diese Gefahr nicht. Dennoch bleiben die Daten eines Patienten solange bestimmbar, wie die Regel angewandt wird. Einige Auswerter von Ordnungsdaten verknüpfen alle Rezepte, die den gleichen Versichertencode enthalten. Es ist für sie interessant nachzuvollziehen, wie sich das Ordnungsverhalten der Ärzte bezogen auf einzelne Patienten verändert. Unter welchen Bedingungen wird das eine durch das andere Medikament ersetzt?

Doch kann dieser Prozess auch illegitim ausgenutzt werden. Wer die Nummer auch nur eines Rezeptes kennt, das ein Patient eingelöst hat, kann in dem Datenbestand alle Angaben zu dem Patienten finden. Man beachte hierbei: Ein als anonym geltender Datenbestand unterliegt nicht dem Datenschutz, kann beliebig weitergegeben, ausgewertet, ja veröffentlicht werden. Hier werden die Anforderungen an eine Anonymisierung aber verletzt. Wollen die ARZ eine Versichertennummer einfach nur umcodieren, dürfen sie deshalb jeden Code nur einmal verwenden. Taucht der gleiche Patient in einer späteren Datenlieferung ein zweites Mal auf, muss ihm ein neuer Code zugeordnet werden.

Der Arztbezug

Ordnen die ARZ jeden Arzt einer hinreichend großen Gruppe zu und ersetzen die Arztnummern in den Rezepten durch eine Bezeichnung der Gruppe, so scheint der Arztbezug aufgehoben. Das ist jedoch nicht immer der Fall.

Bestände die Gruppe aus je einem Augenarzt, Neurologen, HNO-Arzt, Chirurgen und Gynäkologen, ließen sich die Verordnungen der einzelnen Ärzte recht eindeutig voneinander trennen. Ein anderer Fall tritt ein, wenn die Zusammensetzung der Gruppen je nach Auswerter oder dessen Auftraggeber variiert. Wer zunächst die Daten von vier Ärzten abfragt und danach die einer Fünfergruppe, der die ersten vier angehören, der hat die Verordnungen des neu hinzugekommenen Arztes isoliert. Schließlich ist auch klar: Wenn sich unter den Rezepten, die von einer Gruppe von Ärzten ausgestellt wurden, keine Verordnung eines neuen Medikaments findet, so hat auch der einzelne von einer besonderen Werbemaßnahme angesprochene Arzt in der Gruppe das Medikament nicht verschrieben.

Jede dieser Gruppenzusammensetzungen ist unzulässig. Ermöglichen Daten die Herleitung von Angaben über einzelne Personen, so sind sie nicht anonym. Das auch von der RBA verwendete Verfahren ist anfällig für illegitime Auswertungen zumindest der beiden letztgenannten Arten.

Zwei Möglichkeiten bleiben den ARZ: Eine wechselnde Codierung wie im Abschnitt zum Versichertenbezug beschrieben oder die Zuordnung der Ärzte zu Gruppen, deren Größe die vom Gesetzgeber angestrebte Schranke überschreitet, im Vorhinein und unabhängig von Anfragen interessierter Seiten. So können alle Ärzte einer Region zusammengefasst werden, wenn in dieser Region wie in jedem Berliner Bezirk mehr als 300.000 Menschen leben oder mehr als 1.300 Ärzte praktizieren. Wird dies umgesetzt, bleibt das Verschreibungsverhalten des einzelnen Arztes auch im Rahmen der weiteren Verarbeitung der dergestalt anonymisierten Verwaltungsdaten weitestgehend geschützt.

Die Datenverarbeitung der ARZ zeigt wie durch ein Brennglas, welcher Sorgfalt es bedarf, bevor sensitive Daten aus dem Schutzbereich von Datenschutz- und Sozialrecht entlassen werden dürfen. Der statische Ersatz eines Identitätskennzeichens durch ein anderes ist vielfach unzureichend. Je größer das wirtschaftliche Interesse an der Ableitung von Sachangaben über Einzelne aus

einem Datenbestand, desto nachhaltiger muss geprüft werden, welche Möglichkeiten zur Informationsgewinnung der Datenbestand und das Verfahren seiner Erstellung bieten. Auch ein Vorgehen, das bewusst gegen gesetzliche Vorgaben verstößt, darf nicht zum Ziel führen.

Wir werden aufmerksam verfolgen, wie die RBA ihre Verarbeitungsvorgänge an die gesetzlichen Vorgaben anpasst. Soweit nicht Daten aus anderen Quellen personenbezogen auf gesetzlicher Grundlage oder nach informierter Einwilligung der Betroffenen zur Verfügung stehen, müssen die wirtschaftlichen und Forschungsinteressen mit den tatsächlich anonymisierten Daten der ARZ befriedigt werden.

2.5 Wenn die Aufsichtsbehörde klingelt – vermeidbare Fehler von Unternehmen bei Prüfungen

Erhalten wir häufiger zu einem Unternehmen Beschwerden, enthalten die von uns angeforderten Stellungnahmen von Unternehmen oft Widersprüche oder Unklarheiten. Erfahren wir z. B. aus der Presse, dass im Unternehmen Datenschutzverstöße begangen wurden, kontrollieren wir die Datenverarbeitung in dem Unternehmen vor Ort.⁵⁶ Bei solchen Kontrollen stellen wir fast immer fest, dass die Unternehmen nicht alle datenschutzrechtlichen Anforderungen einhalten. Viele Fehler beruhen auf mangelnder Kenntnis der rechtlichen Regelungen oder einer nicht datenschutzgerechten Organisation. So setzen die Unternehmen z. B. die seit 2009 geltenden Regelungen für die Verarbeitung und Nutzung von personenbezogenen Daten zu Werbezwecken immer wieder fehlerhaft um.⁵⁷ Im Folgenden haben wir typische weitere Fehlerquellen und Abhilfemöglichkeiten aufgelistet:

56 § 38 Abs. 4 BDSG

57 Übersicht zur Rechtslage in JB 2010, 2.2

Fehlendes oder mangelhaftes Verfahrensverzeichnis

Jedes Unternehmen ist verpflichtet, ein sog. Verfahrensverzeichnis zu führen.⁵⁸ Dieses Verzeichnis enthält Angaben zur Organisation der verantwortlichen Stelle (Namen, Adresse, Leitungspersonen), eine allgemeine Beschreibung zu den Datenerhebungen, -verarbeitungen und -nutzungen (Angabe der betroffenen Personengruppen und der diesbezüglich verwendeten Datenarten, der Empfänger, der Regelfristen für die Löschung sowie Angaben zur Datenübermittlung in Drittstaaten) sowie ihrer Zwecke.⁵⁹ Das Verzeichnis ist auf Antrag jedermann in geeigneter Weise von der oder dem Unternehmensdatenschutzbeauftragten oder, soweit nicht vorhanden, von der Geschäftsleitung verfügbar zu machen.

In unseren Vor-Ort-Kontrollen stellen wir häufig gleich am Anfang fest, dass ein Verfahrensverzeichnis im Unternehmen nicht vorhanden ist. Da dieses Verzeichnis ein erster Orientierungspunkt ist, um die Rechtmäßigkeit der Erhebung und Verarbeitung von personenbezogenen Daten zu überprüfen und besondere Risiken innerhalb des Unternehmens zu erkennen, bedeutet das Fehlen des Verzeichnisses ein erhebliches Erschwernis der Kontrolltätigkeit der oder des betrieblichen Datenschutzbeauftragten und der Aufsichtsbehörde.

Aber auch wenn das geprüfte Unternehmen ein Verfahrensverzeichnis führt, enthalten die Verzeichnisse oft Mängel, weil z. B. nicht alle betroffenen Personengruppen und die darauf bezogenen Zwecke der Verarbeitung benannt werden (Arbeitnehmer- und Lieferantenangaben werden häufig vergessen) oder Angaben zu den Löschfristen nicht präzise genug in Bezug auf die betroffenen Personengruppen beschrieben werden (ein allgemeiner Verweis auf gesetzliche Löschfristen ist nicht ausreichend).⁶⁰

Fehlende oder mangelhafte Verträge über die Auftragsdatenverarbeitung

Soweit Unternehmen andere Stellen mit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten gemäß ihren Weisungen beauftragen (z. B.

58 § 4g Abs. 2 bzw. 2a, § 4e Satz 1 BDSG

59 § 4e Satz 1 BDSG

60 Ein Muster für ein Verfahrensverzeichnis sowie eine Ausfüllanleitung sind abrufbar unter https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Formulare/Formulare.php.

Call-Center-Leistungen, Datenträgervernichtung, IT-Systembetreuung), liegt keine Datenübermittlung vor, sondern eine bloße Datennutzung. Der Auftraggeber bleibt weiterhin im vollen Umfang für den Umgang mit den personenbezogenen Daten beim Dienstleister verantwortlich.⁶¹ Zwischen den Parteien eines solchen Auftrags ist in diesen Fällen ein sog. Auftragsdatenverarbeitungsvertrag zu schließen, der bestimmte Mindestvertragsbestandteile enthalten und schriftlich abgeschlossen werden muss.⁶² So muss der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen, die zu treffenden technischen und organisatorischen Maßnahmen, die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers geregelt werden.⁶³ Die Mindestvertragsbestandteile eines Auftragsdatenverarbeitungsvertrages sind regelmäßig nicht oder nur lückenhaft in dem zugrundeliegenden zivilrechtlichen Vertrag zur Beauftragung enthalten. „Auftrag“ ist in diesem Zusammenhang nicht gleich „Auftrag“.

Wenn wir in Kontrollen feststellen, dass der Auftraggeber einen Auftragsdatenverarbeitungsvertrag nicht abgeschlossen hat bzw. dieser Vertrag nicht die erforderlichen Mindestvertragsbestandteile enthält, können wir ein Bußgeld von bis zu 50.000 Euro verhängen.⁶⁴ Unternehmen sollten die von ihnen abgeschlossenen Verträge daher daraufhin prüfen, ob die gesetzlichen Mindestvertragsbestandteile für eine Auftragsdatenverarbeitung schriftlich festgelegt worden sind.

Fehlende Unabhängigkeit oder Fachkunde der oder des Datenschutzbeauftragten

Die oder der Datenschutzbeauftragte eines Unternehmens ist eine wichtige Kontrollinstanz innerhalb der verantwortlichen Stelle. Sie oder er wirkt auf die Einhaltung der Datenschutzregelungen im Unternehmen hin und ist an keine Weisungen gebunden. Die Aufgabe kann nur erfüllt werden, wenn die notwendige Fachkunde und Zuverlässigkeit vorhanden ist.⁶⁵ Dies bedeutet, dass insbesondere keine Interessenkonflikte bestehen dürfen. Die Bestel-

61 § 11 Abs. 1 Satz 1 BDSG

62 § 11 Abs. 2 Satz 2 BDSG

63 Weitere Hinweise auch unter http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/auftragsdatenverarbeitung.pdf

64 § 43 Abs. 1 Nr. 2b BDSG

65 § 4f Abs. 2 Satz 1 BDSG

lung von Personen aus der Geschäftsführung, der Leitung der EDV-Abteilung oder der Leitung der Personalabteilung zur oder zum Datenschutzbeauftragten des Unternehmens ist daher nicht zulässig. In diesen Fällen verlangen wir die Abberufung der bestellten Person.

In fachlicher Hinsicht muss die oder der Datenschutzbeauftragte technische Grundkenntnisse haben und die einschlägigen Datenschutzrechtsgrundlagen kennen, die in seinem Unternehmen von Bedeutung sind. Hier stellen wir häufig fest, dass die bestellten Datenschutzbeauftragten uns zwar die Teilnahme an Fortbildungen nachweisen können, der Wissensstand aber unzureichend ist. Als Antwort auf unsere Frage nach den einschlägigen Datenerhebungs- und Verarbeitungsnormen in dem Unternehmen „DIN-Normen“, „Grundgesetz“ oder „irgendwo im Bundesdatenschutzgesetz“ zu präsentieren, entspricht nicht den gesetzlichen Anforderungen an die Fachkunde von Datenschutzbeauftragten. Bei geringen Defiziten geben wir regelmäßig eine Nachschulung auf. Soweit größere Wissenslücken bestehen und die interne Kontrolle des Unternehmens z. B. aufgrund der Anzahl oder der Sensitivität der verarbeiteten personenbezogenen Daten nicht mehr sichergestellt werden kann, können wir auch die Abberufung der oder des Datenschutzbeauftragten verlangen.⁶⁶ Die Anforderungen, die an Beauftragte für den Datenschutz gestellt werden, hat der Düsseldorfer Kreis in einem Papier zusammengefasst.⁶⁷

Fehlendes Lösch- und Sperrkonzept

Personenbezogene Daten dürfen nicht unbegrenzt gespeichert werden. Sie müssen u. a. unverzüglich gelöscht werden, wenn die Verarbeitung für eigene Geschäftszwecke nicht mehr erforderlich ist.⁶⁸ Bestehen gesetzliche oder vertragliche Aufbewahrungspflichten, müssen die Daten gesperrt und aus dem operativen Geschäft entfernt werden.⁶⁹ Ein Zugriff auf diese Daten ist grundsätzlich nur noch für die zur Aufbewahrung vorgesehenen Zwecke erlaubt. Fehlen Regelungen im Unternehmen zur Löschung und Sperrung, stellt dies eine erhebliche Pflichtverletzung dar. Die unbefugte Speicherung von personenbezogenen Daten ist ein schwerer Datenschutzverstoß, der mit empfindli-

66 § 38 Abs. 5 Satz 3 BDSG

67 Siehe Dokumentenband 2010, S. 25 ff.

68 § 35 Abs. 2 Satz 2 Nr. 3 BDSG

69 § 35 Abs. 3 Nr. 1 BDSG

chen Bußgeldern von bis zu 300.000 Euro sanktioniert werden kann.⁷⁰ Regelungen zur Löschung und Sperrung im Unternehmen sind daher unabdingbar.

Missachtung der Auskunftsrechte von Betroffenen

Betroffene können von der verantwortlichen Stelle Auskunft darüber verlangen, welche Daten über sie zu welchem Zweck gespeichert sind und an welche Empfänger die Daten weitergegeben worden sind. Soweit die Herkunft der Daten gespeichert ist, kann auch darüber Auskunft verlangt werden.⁷¹ Der Auskunftsanspruch ist Voraussetzung für die Wahrnehmung weiterer Rechte der Betroffenen (z. B. Berichtigung, Löschung, Widerwiderspruch, Schadensersatz) und damit die „Magna Charta“ des Datenschutzrechts. Ein Verstoß hiergegen wiegt schwer und ist sanktionsbewehrt.⁷²

Teilweise haben wir bei unseren Vor-Ort-Kontrollen festgestellt, dass den Unternehmen dieser Auskunftsanspruch nicht bekannt war. Verfahrensvorkehrungen zur Auskunftserteilung an die Betroffenen haben die Unternehmen daher nicht ergriffen. Häufig wurde bei der Auskunftserteilung die oder der betriebliche Datenschutzbeauftragte nicht einbezogen, sodass es zu fehlerhaften Auskünften kam. Regelungen zur Auskunftserteilung an die Betroffenen sind im Unternehmen deshalb erforderlich.

Fehlende oder mangelhafte Verpflichtung auf das Datengeheimnis

Beschäftigten, die mit personenbezogenen Daten im Unternehmen zu tun haben, ist es verboten, unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Jede und jeder Beschäftigte trägt die persönliche Verantwortung, das gesetzliche Verbot der unbefugten Datenerhebung und -verarbeitung zu wahren (Datengeheimnis). Hierauf sind sie bei Aufnahme ihrer Tätigkeit zu verpflichten.⁷³ Die uns in den Unternehmenskontrollen vorgelegten Mustererklärungen sind häufig fehlerhaft, weil die Beschäftigten nicht vollständig über die Konsequenzen bei Datenschutzverstößen aufgeklärt werden. In einer großen Anzahl der Fälle weisen die Verpflichtungserklärungen zwar auf

70 § 43 Abs. 2 Nr. 1 BDSG

71 § 34 Abs. 1 Satz 1 BDSG

72 § 43 Abs. 1 Nr. 8a BDSG

73 § 5 Satz 2 BDSG

mögliche strafrechtliche Konsequenzen hin. Der Hinweis auf die Möglichkeit zur Verhängung von empfindlichen Bußgeldern wird aber zumeist vergessen.⁷⁴

Obwohl das Bundesdatenschutzgesetz bereits seit mehr als 30 Jahren in Kraft ist, erleben Unternehmen immer wieder böse Überraschungen, wenn die Aufsichtsbehörde ihre Datenverarbeitung vor Ort überprüft. Solche Überraschungen sind vermeidbar, wenn bestimmte Grundregeln beachtet werden. Heutzutage kann es sich kein Unternehmen mehr leisten, den Datenschutz zu unterschätzen.

⁷⁴ Ein Muster für die Verpflichtung auf das Datengeheimnis findet sich unter http://www.lida.bayern.de/lida/datenschutzaufsicht/lda_daten/verpflichtung_datengeheimnis.pdf.

3 Öffentliche Sicherheit

3.1 Antiterrordatei auf dem Prüfstand

In der seit 2007 geführten Antiterrordatei (ATD)⁷⁵ sind bundesweit ca. 16.000 Personen gespeichert, die im Zusammenhang mit internationalem Terrorismus bekannt geworden sind. Hierzu gehören auch Personen, die als Befürworter, Unterstützer oder schuldlos („dolos“) handelnde Kontaktpersonen anzusehen sind. In die ATD stellen insgesamt 38 verschiedene Sicherheitsbehörden Daten ein. Neben den Grunddaten (z. B. Name, Geschlecht, Geburtsdatum, (frühere) Anschriften, körperliche Merkmale, Lichtbilder) werden auch erweiterte Grunddaten zentral gespeichert (z. B. Bankverbindungen, Religionszugehörigkeit, besuchte Orte, Ausbildung/Beruf, Gefährlichkeit, Waffenbesitz, besondere Bemerkungen). Auf diese erweiterten Grunddaten dürfen die Sicherheitsbehörden grundsätzlich nur aufgrund einer Anfrage bei der einstellenden Behörde zugreifen.

Bereits 2007 haben wir über die ATD, unsere Kritikpunkte an dieser Datei und unsere ersten Prüfergebnisse beim Polizeipräsidenten in Berlin berichtet.⁷⁶ Wir überprüften die Datei nunmehr erneut beim Polizeipräsidenten sowie beim Berliner Verfassungsschutz. Dabei stellten wir fest, dass die behördlichen Datenschutzbeauftragten beider Behörden keine anlasslosen Prüfungen vorgenommen haben, um die Eingaben in die ATD auf ihre Richtigkeit und Aktualität zu überprüfen. Beiden Behörden war unbekannt, wie Datensätze in der Datei gesperrt werden können. Offen blieb auch, ob und wie unserer Behörde eine elektronische Auswertung der Protokolldaten, die beim Bundeskriminalamt gespeichert werden, ermöglicht werden kann. Beim Polizeipräsidenten stellten wir außerdem fest, dass Verwaltungsvorschriften, die eine einheitliche Auslegung der unbestimmten Rechtsbegriffe des Antiterror-Datei-Gesetzes ermöglichen, nicht vorhanden bzw. nicht bekannt waren. Kennzeichnungspflichtige Daten⁷⁷

75 Hierzu Artikel 1 des Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder – Gemeinsame Dateien-Gesetz –, BGBl. I 2006, S. 3409

76 JB 2007, 3.2.2

77 § 3 Abs. 2 ATDG

wie die Telefonnummer, die mithilfe eines IMSI-Catchers ermittelt worden war,⁷⁸ waren bei der Polizei in der ATD zudem nicht gekennzeichnet.

Im November fand beim Bundesverfassungsgericht die mündliche Verhandlung über eine schon 2007 erhobene Verfassungsbeschwerde gegen das Antiterrordateigesetz statt. Dabei wurde deutlich, dass das Gericht Bedenken zumindest hinsichtlich der Erforderlichkeit der Speicherung der erweiterten Grunddaten und der Daten von unbeteiligten Kontaktpersonen hat. Ob es auch die zunehmende Erosion des Trennungsprinzips zwischen Polizei und Nachrichtendiensten korrigieren wird, bleibt abzuwarten. Die Entscheidung des Gerichts steht noch aus.

Der Vollzug des Gesetzes zur ATD ist nicht einwandfrei. Gegen das Gesetz bestehen außerdem erhebliche verfassungsrechtliche Einwände.

3.2 Rechtsextremismus-Datei: Ideenlose Imitation der Antiterrordatei

Nach den Fahndungspannen im Zusammenhang mit den terroristischen Aktivitäten des rechtsextremen Nationalsozialistischen Untergrunds (NSU) hat der Bundesgesetzgeber die Einrichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus, die sog. Rechtsextremismus-Datei (RED), beschlossen. Diese wurde im September in Betrieb genommen.⁷⁹

Die RED soll einen gemeinsamen Datenbestand verschiedenster Sicherheitsbehörden ermöglichen (Bundeskriminalamt, Kriminalämter und Verfassungsschutzämter des Bundes und der Länder). In der RED werden die Daten erfasst,

⁷⁸ § 100 i StPO

⁷⁹ Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus vom 20. August 2012, BGBl. I, S. 1798

die bisher in anderen Dateien zu Personen, Gruppierungen und Objekten, die mit gewaltbezogenem Rechtsextremismus zu tun haben, bereits gespeichert sind. Ähnlich wie beim Vorbild „Antiterrordatei (ATD)“⁸⁰ werden in der RED Grunddaten und erweiterte Grunddaten gespeichert, wobei auch hier der Zugriff auf die erweiterten Grunddaten nur nach Freigabe der einstellenden Stelle oder im Eilfall erfolgen kann. Die beteiligten Behörden erhalten keine neuen Befugnisse zur Datenerhebung oder zum Datenaustausch, sie dürfen „nur“ ihre bisher erfassten Informationen in diese neue Verbunddatei eingeben.

Ungeachtet des dringenden Erfordernisses, den Rechtsextremismus zu bekämpfen, bestehen allerdings Bedenken gegen die Erforderlichkeit der Errichtung einer zusätzlichen (zentralen) Datei. Die Fehlerquellen bei der Fahndung zum NSU sind bisher nicht ausreichend lokalisiert und analysiert worden. Es ist unklar, in welchem Maße die Sicherheitsbehörden die gesetzlichen Eingriffsbefugnisse fehlerhaft vollzogen haben. Im Übrigen werden schon seit 2000 rechtsorientierte politisch motivierte Straftaten, insbesondere Gewalttaten, in verschiedenen Verbunddateien gespeichert (z. B. INPOL, „Gewalttäter rechts“ beim Bundeskriminalamt). Inwiefern die RED zukünftig dazu beitragen kann, Fahndungsspannen wie beim NSU entgegenzuwirken, ist daher ungewiss.

Gegen das Gesetz zur RED bestehen zudem ähnliche Bedenken wie bei dem Gesetz zur ATD. Zwar enthält das Gesetz zur RED einige Verbesserungen (z. B. vorgesehene Befristung, Vorgabe einer qualifizierten Evaluierung). Begriffe wie „gewaltbezogen“ oder „Rechtsextremismus“ werden allerdings im Gesetz selbst nicht definiert. Die verfassungsrechtlichen Grundsätze der Normenbestimmtheit und Normenklarheit geben jedoch vor, dass die betroffenen Personen anhand einer gesetzlich vorgesehenen Datenverarbeitungsbefugnis zumindest im Grundsatz erkennen können müssen, ob und durch welche Stellen sie mit einer staatlichen Erfassung rechnen müssen. Es besteht die Gefahr, dass den Betroffenen zu Unrecht ein bestimmtes Gedankengut unterstellt wird und sie in dieser Datei erfasst werden.

Gegen das Gesetz zur RED bestehen ähnliche verfassungsrechtliche Einwände wie gegen das ATD-Gesetz.

80 Siehe 3.1

3.3 Akkreditierung für den Papstbesuch

Wie bei früheren Großveranstaltungen (z.B. der Fußball- oder der Leichtathletik-Weltmeisterschaft) hat die Polizei auch beim Papstbesuch Zuverlässigkeitsüberprüfungen bei Beschäftigten des Veranstalters, Service/Catering, der privaten Sicherheitsdienste, Technik und Sanitätsdienste (etwa 2.000 Personen) durchgeführt. Personen, die unmittelbaren Kontakt zum Papst hatten, und Journalisten wurden vom Bundeskriminalamt überprüft.

Mit dem 9. Gesetz zur Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) ist 2011 die lange geforderte Rechtsgrundlage geschaffen worden.⁸¹ Von einer bei anderen Großveranstaltungen heftig kritisierten Beteiligung des Verfassungsschutzes und des Bundesnachrichtendienstes hat das Landeskriminalamt diesmal abgesehen. Auch die Beschäftigten der Feuerwehr wurden (anders als bei der Fußball-Weltmeisterschaft 2006)⁸² nicht in die Überprüfung einbezogen. Dem Veranstalter wurden keine konkreten Einzelheiten übermittelt, sondern nur mitgeteilt, dass „keine Erkenntnisse im Sinne des Kriterienkataloges“ oder „Erkenntnisse im Sinne des Kriterienkataloges“ vorlagen.

Das 2011 novellierte ASOG gibt den Rahmen für die Zuverlässigkeitsüberprüfungen bei Großveranstaltungen vor. Dieser Rahmen wurde beim Papstbesuch eingehalten.

3.4 Stille SMS

Der Presse war zu entnehmen, dass die niedersächsischen Sicherheitsbehörden zum Versenden der „Stillen SMS“ den Server eines privaten Anbieters von Telekommunikationsdienstleistungen nutzen.

81 § 45a ASOG, siehe JB 2011, 3.1

82 JB 2006, 2.2

Die Berliner Polizei nutzt seit längerem das Instrument der „Stillen SMS“ im Rahmen der Telekommunikationsüberwachung, wenn keine tatsächliche Kommunikation beim technisch überwachten Mobilanschluss stattfindet.⁸³ Das Mobiltelefon ignoriert diese SMS, aber der Netzbetreiber sendet einen Verkehrsdatensatz, der den Funkzellenstandort enthält, ohne dass die Betroffenen es bemerken. Damit kann man bei Bedarf den ungefähren Standort des Mobiltelefons heimlich lokalisieren. Die Polizei hat die Funktionalität „Versenden von Stillen SMS“ im Januar 2005 in die polizeieigene TKÜ-Anlage implementiert, bedient sich also keines privaten Dienstleisters. Hierdurch ist es der TKÜ-Sachbearbeitung nach Vorlage eines richterlichen Beschlusses möglich, anders als in anderen Bundesländern eigenständig an der TKÜ-Auswerteeinheit den Versand von „Stillen SMS“ im Rahmen von Überwachungsmaßnahmen einzurichten, zu denen sie berechtigt ist.

Das Versenden „Stiller SMS“ ist eine Einzelmaßnahme, die im Rahmen angeordneter TKÜ-Maßnahmen durchgeführt wird. Sie richtet sich nach den Bestimmungen der Strafprozessordnung,⁸⁴ bedarf keiner besonderen Einzelanordnung und kann mehrfach im Rahmen einer Telekommunikationsüberwachung erfolgen. Eine Eingriffsbefugnis aus anderen gesetzlichen Bestimmungen, insbesondere zu präventiven Zwecken nach Polizeirecht, besteht in Berlin nicht.

Die „Stille SMS“ ist als Teil der TKÜ mit richterlicher Anordnung zur Aufklärung von Straftaten zulässig und wird in Berlin mit der polizeieigenen TKÜ-Anlage durchgeführt.

3.5 Protokollierung des Abfragegrundes

Zur Bearbeitung einer Eingabe war es erforderlich, die Protokollbänder des polizeilichen Informationssystems daraufhin auswerten zu lassen, wer aus welchem Grund auf den Datensatz einer Petentin zugegriffen hat.

⁸³ Siehe JB 2003, 3.1 (S. 28 f.)

⁸⁴ § 100a StPO

Die Prüfung ergab, dass allein in diesem Fall wiederholt der Abfragegrund nicht im System protokolliert war. Dies bestätigt die Berechtigung unserer Forderung, dass bei Anfragen im polizeilichen Informationssystem POLIKS das Feld „Abfragegrund“ mit einem Aktenzeichen oder aussagekräftigem Stichwort belegt werden muss.

Der Polizeipräsident hat zwar auf eine Geschäftsordnung hingewiesen, wonach die Abrufenden verpflichtet sind, den Abfragegrund im System zu dokumentieren (wobei der Katalogbegriff „Vorgangsbearbeitung“ nicht ausreichend ist). Die behördliche Datenschutzbeauftragte hat alle Direktionen und Ämter wiederholt auf die Einhaltung dieser Vorgaben hingewiesen und darum gebeten, die Mitarbeiterinnen und Mitarbeiter in geeigneter Weise auf diese Pflicht hinzuweisen. Ferner sind diese Schreiben für jede Frau und jeden Mann im Polizeidienst im polizeiinternen Kommunikationsnetz INTRAPOL nachzulesen. Das alles scheint aber nicht ausreichend zu sein. Hier sollte der Polizeipräsident prüfen, ob diese Verstöße nicht dienstrechtlich zu verfolgen sind.

Der Abfragegrund ist im polizeilichen Informationssystem zu dokumentieren. Katalogbegriffe reichen dafür nicht aus.

3.6 Unbefugter Abruf aus INPOL

Ein Petent, der einen PC bei eBay zum Verkauf angeboten hatte, prellte den Käufer, indem er nach Anzahlung nicht lieferte. Auf Mahnungen reagierte der Petent nicht. Zuletzt drohte der Käufer per E-Mail unter Hinweis darauf, er sei Polizist, dem Verkäufer eine Strafanzeige an. Um dieser Drohung Nachdruck zu verleihen, war der E-Mail ein Foto des Petenten angehängt, das im Polizeipräsidium Bremen von ihm gemacht wurde.

Die Auswertung der Protokollbänder beim Bundeskriminalamt hat ergeben, dass von der Berliner Polizei auf den Datensatz des Petenten im INPOL-Datenbestand zugegriffen wurde. Sie beschäftigte aber keinen Mitarbeiter mit den Personalien des Käufers. Bei der Überprüfung des Vorgangs hat die Schwester des Käufers, eine Polizistin, gestanden, das erkenntnisdienliche

Lichtbild des Petenten in INPOL aufgerufen, ausgedruckt und ihrem Bruder zur Verfügung gestellt zu haben. Das Amtsgericht Tiergarten hat eine Geldstrafe verhängt.

Der Zugriff auf dienstlich geführte Datenbestände für private Zwecke ist verboten und kann strafrechtlich geahndet werden.

3.7 Unzulässige Datenspeicherung – Führerschein weg

Ein Petent kam in eine anlasslose Fahrzeugkontrolle. Bei der routinemäßigen Halterabfrage erhielten die Polizisten den Hinweis, dass der Petent „BTM-Täter“ sei. Daraufhin wurden ein Alkoholtest (unter 0,5 Promille) und ein Drogenschnelltest (THC-positiv) durchgeführt sowie eine Blutentnahme durch den Amtsarzt vorgenommen. Im Ergebnis führte dies zum Verlust der Fahrerlaubnis.

Bei einer früheren – ebenfalls anlassunabhängigen – Verkehrskontrolle in 2005 war der Petent auf Drogenkonsum angesprochen worden. In der deshalb begehrten Auskunft über die zu seiner Person gespeicherten Daten wurden ihm ein 2001 eingestelltes Ermittlungsverfahren wegen des Verstoßes gegen das Betäubungsmittelgesetz und der personengebundene Hinweis mitgeteilt. Nach einem Löschantrag des Petenten stellte der Polizeipräsident fest, dass diese Daten für die ordnungsgemäße Aufgabenerfüllung nicht mehr erforderlich sind, und sicherte die Löschung zu. Tatsächlich gelöscht wurde 2005 nur der Anlassvorgang. Aufgrund eines Büroversehens ist die Löschung des personengebundenen Hinweises „BTM-Konsument“ unterblieben. Dieser Hinweis blieb also im polizeilichen Informationssystem weiter abrufbar.

Die unvollständige Löschung der Daten wurde beanstandet. Nach dem ASOG⁸⁵ sind personenbezogene Daten u. a. dann zu löschen und die dazugehörigen Unterlagen zu vernichten, wenn aus Anlass einer Einzelfallbearbeitung festge-

85 § 48 Abs. 2

stellt wird, dass die Kenntnis der Daten für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Die Bearbeitung des Auskunftersuchens und das sich anschließende Lösungsbegehren war eine Einzelfallbearbeitung im Sinne dieser Vorschrift.

Wenn die gesetzlichen Voraussetzungen für Löschungen vorliegen, sind diese nicht nur zuzusagen, sondern auch zu vollziehen.

3.8 Wiedereinführung der taktischen Hinweise?

1988 hatte das Abgeordnetenhaus in einem Beschluss den Senat aufgefordert, bestimmte personengebundene Hinweise wie „Geisteskrank“ (GEKR), „Ansteckungsgefahr“ (ANST) oder „Land- und Stadtreicher“ in polizeilichen Informationssystemen zu löschen.⁸⁶ Der Beschluss, den der Senat auch umgesetzt hatte, war auf die Kritik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder⁸⁷ zurückzuführen.

Die Senatsverwaltung für Inneres und Sport hat uns darüber informiert, dass dieser Beschluss wegen der vergangenen Zeitspanne keine politische Bindungswirkung entfalte. Damit hat die Senatsverwaltung einen Beschluss des AK II der Innenministerkonferenz⁸⁸ in Berlin umgesetzt. Die personengebundenen Hinweise „GEKR“ und „ANST“ werden nun wieder verwendet.

Bei der Vergabe von personengebundenen Hinweisen, die jedem Zugriffsberechtigten beim Aufrufen des Namens im polizeilichen Informationssystem POLIKS angezeigt werden, ist Zurückhaltung geboten. Die Praxis hat gezeigt, dass die Hinweise „GEKR“ und „ANST“ für die geltend gemachte Eigenversicherung der Polizei nicht erforderlich sind; insbesondere gab es keine Fälle von Ansteckung durch eine infizierte Person. Die Hinweise wirken stigmatisie-

86 Abgh.-Drs. 10/2304 und 10/2688 sowie Plenarprotokoll vom 1. Dezember 1988, S. 2591

87 JB 1987, 5.3

88 Beschluss vom 20./21. Oktober 2011, TOP 22

rend. Die Betroffenen geraten leicht in Gefahr, abgestempelt zu werden. Deshalb ist die Zielrichtung des Beschlusses des Abgeordnetenhauses von 1988 immer noch aktuell.

Auch wenn der Leitfaden für die Vergabe von personengebundenen Hinweisen mittlerweile weitaus enger gefasst ist als es vor 25 Jahren Praxis war, bestehen Zweifel an der Erforderlichkeit der Hinweise „GEKR“ und „ANST“.

4 Melde- und Ausländerwesen

4.1 Bundesmeldegesetz

Am Entwurf des Bundesmeldegesetzes⁸⁹ haben die Datenschutzbeauftragten insbesondere zu folgenden Punkten Kritik geübt:

- Wiedereinführung der erst kürzlich abgeschafften Vermietermeldepflicht
- Beibehaltung der Hotelmeldepflicht
- Keine Widerspruchsmöglichkeit gegen einfache Melderegisterauskünfte
- Weiterhin keine Einwilligungslösung bei Melderegisterauskünften in besonderen Fällen
- Erweiterte Melderegisterauskünfte schon bei berechtigtem Interesse

Das alles wurde vom Gesetzgeber nicht aufgegriffen. Vielmehr wurde der Entwurf im Vorfeld der legendären 57 Sekunden dauernden zweiten und dritten Lesung⁹⁰ (zunächst fast unbemerkt von der Öffentlichkeit) dahingehend geändert, dass Unternehmen Melderegisterauskünfte selbst bei einem Widerspruch der oder des Meldepflichtigen für Zwecke der Werbung und des Adresshandels erhalten, wenn die Daten ausschließlich zur Berichtigung oder Bestätigung bereits vorhandener Daten verwendet werden. Davon würden vor allem Auskunfteien und Adresshändler profitieren. Das bedeutet eine massive Verschlechterung des Datenschutzniveaus gegenüber der bisherigen Rechtslage.

Das Bundesmeldegesetz ist zustimmungspflichtig. Der deshalb befasste Bundesrat hat u. a. wegen der äußerst umstrittenen einschränkenden Wirkung des Widerspruchs bei der Weitergabe zur Berichtigung oder Bestätigung der Daten an Unternehmen den Vermittlungsausschuss angerufen; das Ergebnis ist offen. Zuvor hatten bereits die Datenschutzbeauftragten gefordert, das Melderecht datenschutzkonform zu gestalten.⁹¹

⁸⁹ BT-Drs. 17/7746

⁹⁰ BT-Plenarprotokoll 17/187, S. 22464

⁹¹ Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. August 2012: Melderecht datenschutzkonform gestalten!, siehe Dokumentenband 2012, S. 17

Wenn das Widerspruchsrecht Wirkung entfalten soll, dürfen keine Melde-registerauskünfte zur Bestätigung oder Berichtigung bereits vorhandener Daten zulässig sein. Konsequenter wäre es, wenn der Bundesgesetzgeber die Nutzung von Meldedaten für Werbezwecke an die Einwilligung der Betroffenen knüpfen würde.

4.2 Zugriff auf das Melderegister für private Zwecke

Ein überall nur mit seinem Vornamen bekannter Petent hat von einer früheren Bekannten eine Glückwunschkarte erhalten, die sämtliche seiner Vornamen enthielt. Auf Befragen habe ihm ihr Lebensgefährte erklärt, dass die frühere Bekannte im Bezirksamt Charlottenburg-Wilmersdorf arbeite und auf die Meldedaten zugreifen könne. Zwei andere Petenten beschwerten sich, dass Mitarbeiterinnen des Bürgeramtes ihre Meldedaten abgerufen und diese Kenntnis zu Mobbingzwecken genutzt haben.

In allen Fällen konnte durch die Auswertung der Protokollbänder der Abruf der Daten durch Beschäftigte des Bezirksamtes festgestellt werden. Die Mitarbeiterin, die die Glückwunschkarte verschickt hatte, hat den Zugriff auf die Meldedaten für diesen privaten Zweck zugegeben. Eine andere Mitarbeiterin hat zwar den Zugriff auf die Meldedaten eingeräumt, konnte sich aber nicht mehr an den Grund erinnern. Die dritte Mitarbeiterin wollte den Zugriff mit der Aktualisierung der Wahlhelferdatei rechtfertigen. Hierfür ist aber die Einwilligung des Wahlhelfers erforderlich, ohne die der Zugriff mangels Rechtsgrundlage unzulässig ist. Die Dienststellenleitung hat die Mitarbeiterinnen auf die Rechtslage hingewiesen. Von weiteren arbeits- oder dienstrechtlichen Maßnahmen wurde abgesehen.

Diese Häufung von festgestellten Verstößen ist nicht hinnehmbar. Wir haben dem Bezirksbürgermeister empfohlen, dies zum Anlass für Strukturverbesserungen zu nehmen und die Beschäftigten in geeigneter Form darauf hinzuweisen, dass bei festgestellten Zugriffen auf das Melderegister für private Zwecke⁹² künftig eine Abmahnung erfolgt.

92 Solche Zugriffe sind ggf. strafbar nach § 32 BlnDSG.

Das Ausnutzen der dienstlichen Stellung für Datenabrufe zu privaten Zwecken ist nicht nur unzulässig, sondern auch strafbar.

4.3 Löschung oder Archivierung von Meldedaten

Ein Erbenermittler klagte darüber, dass über Monate hinweg weder das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) noch das Landesarchiv unter Hinweis auf personelle, technische und organisatorische Schwierigkeiten Auskünfte aus dem Archivbestand erteile und dies die Existenz des Unternehmens bedrohen würde.

Das LABO darf als Meldebehörde Privaten Auskunft aus dem Melderegister erteilen⁹³ und Meldedaten an andere öffentliche Stellen übermitteln.⁹⁴ Die Speicherdauer ist aber nicht unbegrenzt. So sind die Daten nach Ablauf von fünf Jahren nach dem Wegzug oder Tod eines Menschen für die Dauer von 25 Jahren als sog. Archivdatenbestand gesondert aufzubewahren.⁹⁵ In dieser Zeit dürfen sie mit Ausnahme abschließend aufgezählter Daten (dazu gehören u. a. die Grunddaten sowie Tag und Ort der Geburt) nicht mehr genutzt werden. Das bedeutet, dass die Meldebehörde über die beispielhaft aufgezählten Daten auch aus dem archivierten Bestand Melderegisterauskünfte erteilen bzw. Daten an andere öffentliche Stellen übermitteln darf. Die übrigen Daten des Archivbestandes dürfen nur noch in engen gesetzlichen Grenzen genutzt werden.

Nach Ablauf von 30 Jahren (fünf Jahre nach Tod oder Wegzug und 25 Jahre als Archivdatenbestand) sind die Daten zu löschen. Die Mikrofiche (früheres Karteiarchiv West) und die eingescannten Karteikarten (früheres Karteiarchiv Ost) sind Datenträger, auf denen zu löschende Daten mit anderen noch aufzubewahrenden Daten verbunden sind. Sie können nicht voneinander getrennt werden und unterliegen somit einem Verwertungsverbot.

93 §§ 28, 29 Meldegesetz (MeldeG)

94 §§ 25 – 27 MeldeG

95 § 10 MeldeG

Das LABO hat sämtliche archivierten Meldeunterlagen aus dem automatisiert geführten Melderegister sowie die anderen Alt-Unterlagen, die zur Löschung bzw. Vernichtung anstanden, dem Landesarchiv angeboten,⁹⁶ das sie zunächst auch als komplett archivwürdig eingestuft hat.⁹⁷ Bisher war eine Übernahme nicht möglich, weil dem Landesarchiv die technischen Möglichkeiten fehlten, die Daten aus dem automatisiert geführten Melderegister zu übernehmen und nach Archivrecht weiter zu verarbeiten. Ferner muss die Meldebehörde zur Erfüllung ihrer Aufgaben auf die Mikrofiche und die eingescannten Karteikarten zugreifen, da die Speicherfrist noch nicht für alle Daten abgelaufen ist.

Das LABO darf die Alt-Unterlagen ausschließlich zur eigenen Aufgabenerfüllung unter Berücksichtigung der Aufbewahrungsfristen⁹⁸ nutzen. Den Kunden – wie dem Erbenermittler – teilt das LABO bei Anfragen zu Personen, die länger als 30 Jahre verzogen oder verstorben sind, mit, dass aus rechtlichen Gründen keine Auskunft mehr erteilt werden darf.

Zuletzt hat das Landesarchiv erklärt, dass es die automatisiert geführten und zu löschenden Daten – anders als die verfilmten und gescannten Teile des Melderegisters – für nicht archivwürdig hält. Die archivwürdigen Unterlagen sollen jedoch beim LABO verbleiben. Die Meldebehörde dagegen hat sich für eine Übernahme auch des automatisierten Bestandes durch das Landesarchiv eingesetzt. Sie befürchtet, bei einer Löschung würde eine „Lücke“ entstehen, die später dazu führt, dass z. B. Erbenermittlungen auch nicht mehr über die Archive möglich sind.

Die für archivwürdig erklärten Mikrofiche und eingescannten Karteikarten können beim LABO nur im Rahmen der Auftragsdatenverarbeitung verbleiben. Wir haben das LABO bei der Erstellung einer Verwaltungsvereinbarung mit dem Landesarchiv zur Erteilung von Melderegisterauskünften nach dem Archivgesetz unterstützt.

96 § 4 Archivgesetz (ArchG)

97 § 3 ArchG

98 § 10 MeldeG

Datenbestände sind nach Ablauf der Speicherfrist dem Landesarchiv anzubieten. Wenn dieses innerhalb von zwölf Monaten keine Archiwürdigkeit feststellt, sind die Daten zu löschen. Über die Archiwürdigkeit entscheidet das Landesarchiv.

4.4 Dauerhafte Aufbewahrung von Einbürgerungsanträgen?

Ein Petent, der seinen Einbürgerungsantrag 2006 zurückgezogen hatte, beschwerte sich Anfang August 2011 darüber, dass seine Daten weiterhin beim Bezirksamt Treptow-Köpenick gespeichert werden und darüber hinaus dem Bezirksamt Neukölln Auskünfte aus diesem Vorgang erteilt wurden.

Das Bezirksamt Treptow-Köpenick hat den Sachverhalt bestätigt. Alle Einbürgerungsanträge würden dauerhaft aufbewahrt. Eine nachvollziehbare Begründung konnte uns das Bezirksamt nicht geben. Die Senatsverwaltung für Inneres und Sport teilte uns mit, dass sich bei einer Besprechung der Staatsangehörigkeitsreferenten beim Bundesministerium des Innern (BMI) der Bedarf gezeigt hat, die Aufbewahrung und Archivierung von Einbürgerungsakten zu klären.⁹⁹ Das BMI hat zugesagt, diese Frage grundsätzlich aufzuarbeiten und bei der nächsten Besprechungsrunde im Mai 2013 darüber zu berichten.

Es ist nicht akzeptabel, dass weder die Daten verarbeitende Stelle noch die Fachaufsicht nachvollziehbar und konkret anhand von einschlägigen Rechtsvorschriften erläutern kann, warum die dauerhafte Aufbewahrung von Einbürgerungsvorgängen erforderlich sein soll. „Ewige“ Akten mit Personenbezug kann es im Verwaltungsvollzug nicht geben, weder in Berlin noch anderswo.

⁹⁹ Siehe zu diesem Problem schon JB 2004, 4.2.1 (S. 60 f.)

5 Verkehr

5.1 Videoüberwachung im Straßenverkehr

Die Videoüberwachung im Straßenverkehr wird zu unterschiedlichen Zwecken eingesetzt. Die meisten Kameras dienen der Beobachtung der aktuellen Verkehrssituation und werden von der Verkehrsmanagementzentrale Berlin betrieben. Sie überwacht im Auftrag der Senatsverwaltung für Stadtentwicklung und Umwelt die allgemeine Verkehrslage auf den Straßen. Die mit den Kameras gewonnenen Informationen gibt sie an die Medien weiter, die wiederum die Verkehrsteilnehmenden informieren.

Der Zweck dieser Datenerhebung beschränkt sich darauf, die aktuelle Verkehrslage zu beobachten, um z. B. auf technische Ausfälle von Ampelanlagen schnell zu reagieren oder Umleitungsempfehlungen bei Staubildungen anzubieten. Die Kameras sind häufig in Schilderbrücken über den Fahrbahnen installiert und beobachten großflächig die Verkehrsströme. Sie sind weder zoom- noch schwenkbar. Es werden nur Live-Bilder erhoben und keine Bilddaten aufgezeichnet. Durch die Qualität der Aufnahmen ist eine Erfassung von einzelnen Personen in den Fahrzeugen oder von Passanten auf den Bürgersteigen weitgehend ausgeschlossen.

Eine andere Funktion haben die technischen Einrichtungen, die an Ampeln oder Verkehrsschildern installiert sind. Sie sehen wie Kameras aus und vermitteln durch ihre geringe Entfernung zur Straße den Eindruck, als können sie Detailaufnahmen der Verkehrsteilnehmenden machen. Hierbei handelt es sich allerdings um sog. Anforderungseinrichtungen. Sie erfassen keine Bilddaten, sondern dienen dazu, die Anwesenheit von Fahrzeugen vor einer Ampel zu erkennen. Die Ampel wird dann situationsbedingt, also abhängig von der Verkehrslage geschaltet. Diese Einrichtungen werden zunehmend installiert und verdrängen allmählich die Induktionsschleifen, die in die Fahrbahn integriert sind und die gleiche Funktion haben.

Immer häufiger vergibt die Senatsverwaltung für Stadtentwicklung und Umwelt auch Aufträge an Einrichtungen aus dem nicht-öffentlichen Bereich.

Im Rahmen von Forschungsprojekten sollen z. B. Erkenntnisse zum Fahrverhalten von Verkehrsteilnehmenden oder zur Auslastung von Straßen erlangt werden. Bei den für diese Zwecke eingesetzten Videokameras kann eine Identifizierung einzelner Verkehrsteilnehmer u. U. nicht völlig ausgeschlossen werden.

Verkehrserhebungen mit Videotechnik, die von verantwortlichen Stellen des nicht-öffentlichen Bereichs im Auftrag öffentlicher Stellen durchgeführt werden, sind nach dem Bundesdatenschutzgesetz zu bewerten.¹⁰⁰ Wenn es bei der Verkehrserhebung nicht darauf ankommt, die einzelnen Verkehrsteilnehmenden zu beobachten, sondern das Ziel verfolgt wird, das allgemeine Fahrverhalten oder die Menge des Durchgangsverkehrs zu ermitteln, ist eine Identifizierung von Personen oder Kfz-Kennzeichen nicht erforderlich. In diesem Fall sollten die Bilddaten der Verkehrsteilnehmenden derart verpixelt werden, dass ihre Persönlichkeitsrechte gewahrt bleiben. Diese Verpixelung sollte bereits unmittelbar während der Datenerhebung und nicht erst nachträglich bei der Auswertung der Bilddaten erfolgen. Nur wenn gewährleistet ist, dass schutzwürdige Interessen der Betroffenen, die in den Erfassungsbereich der Kamerabeobachtung geraten, nicht überwiegen, ist der Einsatz der Videotechnik zulässig.

Zur Kontrolle, ob ein bestimmtes Fahrzeug berechtigt ist, in die Umweltzone zu fahren, ist allerdings eine Kennzeichenerfassung notwendig. Um die Anforderungen an den Datenschutz zu erfüllen, sollte ein Kennzeichenerfassungssystem sofort nach der Erfassung des Kennzeichens in der Kamera eine sog. Fahrzeugsignatur erzeugen. Direkt bei der Erfassung eines Kennzeichens wird diesem eine zufällig erzeugte Zeichenfolge (Salt) vorangestellt und das Kennzeichen mittels einer Streuwertfunktion (Hash) verschlüsselt. Das Ergebnis dieser Verschlüsselung bezeichnet man als Signatur (im vorliegenden Fall als Fahrzeugsignatur). Mit der Erzeugung einer Fahrzeugsignatur kann ein Bezug zum Kennzeichen im Nachhinein nicht mehr hergestellt werden. Eine derartige Verschlüsselung ist datenschutzgerecht.

Wesentlich problematischer dürfte allerdings die Umsetzung der Forderung nach § 6b Abs. 2 BDSG sein.¹⁰¹ Weithin sichtbare Schilder, die auf eine Ver-

100 § 6b Abs. 1 Nr. 3 BDSG

101 Danach sind der Umstand der Beobachtung und die datenverarbeitende Stelle durch geeignete Maßnahmen erkennbar zu machen.

kehrserhebung hinweisen, oder Vorabinformationen in der örtlichen Presse würden den Projektablauf und das Ergebnis vermutlich beeinflussen. Dennoch sollten erklärende Informationen zum Projektablauf direkt vor Ort durch Projektmitarbeiterinnen und -mitarbeiter publik gemacht werden. Das sollte z. B. die Zielsetzung des Projekts, den Zeitpunkt / Zeitraum der Verkehrserhebung, die Anzahl und Erfassungsbereiche der Kameras, die Aufzeichnung / Speicherdauer und Weiterverwendung der Bilddaten umfassen. Für weitergehende Fragen sollten sich interessierte Verkehrsteilnehmende an die verantwortliche datenverarbeitende Stelle wenden können.

Videoüberwachung im Straßenverkehr ist zulässig, wenn keine personenbezogenen Daten erhoben werden. Andernfalls sind die Daten bei ihrer Erhebung oder unmittelbar danach zu verpixeln oder zu verschlüsseln.

5.2 Verkehrserhebung: Verschlüsselung der Kfz-Kennzeichen auf der Tangential-Verbindung Ost

Die Tangential-Verbindung Ost ist ein Projekt zur Errichtung einer kreuzungsarmen Stadtschnellstraße. Sie soll die östlichen und südöstlichen Bezirke mit dem Berliner Ring im Norden und der A 113 im Süden verbinden und das Stadtstraßennetz vom Durchgangsverkehr entlasten.

Das Bezirksamt Marzahn-Hellersdorf hat uns gegenüber dargelegt, dass die Erforderlichkeit der Anbindung an die Tangential-Verbindung Ost in Biesdorf zwischen der zukünftigen Trasse und der Köpenicker Straße strittig war. Durch eine Anbindung würde ein Parallelverkehr und damit eine unzumutbare Belastung des Siedlungsgebietes Biesdorf erwartet. Um den Durchgangsverkehr bzw. die Verkehrsströme zu ermitteln, hat ein Ingenieurbüro im Auftrag der Senatsverwaltung für Stadtentwicklung und Umwelt eine Kfz-Kennzeichenerfassung durchgeführt.

Mittels Videotechnik sollten die Kennzeichen der ein- und ausfahrenden Fahrzeuge im Berufsverkehr an vier verschiedenen Stellen auf der Strecke erfasst und nach verschiedenen Kriterien wie Uhrzeit, Zählstelle, Fahrtrichtung und

Kfz-Kennzeichen aufbereitet werden. Aus der Zeitdifferenz (wieder)erkannter Kennzeichen sollten der Anteil des Quell-, Ziel- und Durchgangsverkehrs sowie die regionale Herkunft der Fahrzeuge abgeleitet werden. Da über die Kfz-Kennzeichen die Fahrzeughalterinnen und -halter ermittelt werden können, sind die Kennzeichendaten als personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes zu betrachten.

Wir haben bereits im Vorfeld die Erforderlichkeit der Erhebung der vollständigen Kennzeichen bezweifelt. Zur Erreichung des Projektziels war eine teilweise Kennzeichenerfassung ausreichend. Eine andere Möglichkeit der anonymen Datenverarbeitung war die unmittelbare Verschlüsselung der Daten direkt bei der Erhebung. Entsprechend unseren Hinweisen hat das Ingenieurbüro daraufhin eine Teilverschlüsselung der Daten vorgenommen: Die Buchstaben der Kennzeichen (Ortskennung und folgende Buchstaben) blieben bei der Erfassung erkennbar, da sie zwingend für die Beurteilung des Durchgangsverkehrs benötigt wurden. Sämtliche Zahlen der Kennzeichen wurden sofort bei der Erfassung verschlüsselt.

Aufgrund unseres kurzfristigen Eingreifens ist die Kfz-Kennzeichenerfassung mithilfe eines Verschlüsselungsverfahrens durchgeführt worden. Mit der Teilverschlüsselung der Kfz-Kennzeichen unmittelbar bei der Erfassung wurde gewährleistet, dass keine Rückschlüsse auf die Fahrzeughalterinnen und -halter gezogen werden konnten. Zudem haben wir erreicht, dass die Senatsverwaltung für Stadtentwicklung und Umwelt öffentlich auf die Verkehrserhebung hingewiesen hat.

5.3 Fahrkarten und Parktickets übers Handy

Fahrkarten übers Handy

Handys und Smartphones bieten den Nutzenden vielfältige Möglichkeiten, die über die ursprünglichen Grundfunktionen des Telefonierens sowie den Versand und Empfang von Kurzmitteilungen weit hinausgehen. Durch Internetzugang und die Nutzung von Software-Applikationen

(„Apps“) haben sich insbesondere Fahrplanauskünfte als hilfreiche Unterstützung für die einfache und schnelle Planung von Reisen im öffentlichen Nah- und Fernverkehr bei den Anwendern etabliert. Aufbauend auf dieser Entwicklung bieten die Anbieter des öffentlichen Personennahverkehrs (ÖPNV) sowie die Deutsche Bahn im Fernverkehr zunehmend Lösungen für den Erwerb, die Nutzung und die Bezahlung des Fahrtickets über das Mobiltelefon an.

Seit 2002 befassen sich national und international zahlreiche Projekte damit, das **elektronische Ticketing** zu etablieren. Darunter wird der bargeldlose Erwerb sowie die elektronische Speicherung und Verwaltung von Fahrtberechtigungen für den öffentlichen Personenverkehr auf elektronischen Medien verstanden. Neben dem Einsatz von Handys und Smartphones umfasst dies auch den Erwerb und die Nutzung von Fahrscheinen in Form einer Chipkarte.

In Deutschland haben sich insbesondere das HandyTicket Deutschland vom Verband Deutscher Verkehrsunternehmen (VDV) und das „Touch & Travel“-Angebot der Deutschen Bahn (DB) etabliert. Das HandyTicket Deutschland kann als App für Smartphones sowie per Handy über das mobile Internet oder als fest installiertes Java-Programm genutzt werden. In einigen Regionen besteht auch die Möglichkeit, nach der Registrierung ein Ticket per Internet, per kostenlosen Telefonanruf oder per SMS zu bestellen. Das Ticket wird anschließend jeweils per SMS übermittelt. Aktuell kann das HandyTicket Deutschland u. a. in Augsburg, Bielefeld, Dresden, Freiburg, Hamburg, Nürnberg, Stuttgart und Ulm genutzt werden.¹⁰² Bei diesem Angebot werden ebenso wie bei den herkömmlichen Vertriebswegen der DB und beim DB-Handyticket nur die nötigen Daten (Name, Anschrift, E-Mail-Adresse, gewünschter Zahlungsweg, Kontrollmedium) erhoben und keine Bewegungsprofile erzeugt.

In Berlin bietet die BVG aufbauend auf dem von der DB für den Fernverkehr entwickelten System „Touch & Travel“ seit Juli 2011 elektronische Tickets in Form einer Smartphone-App an. Hierzu muss sich die Kundin oder der Kunde im Internet unter der Adresse <https://www.touchandtravel.de/> registrieren und die für das eigene Mobiltelefon geeignete App herunterladen.

¹⁰² Eine vollständige Übersicht über alle Regionen, die das HandyTicket Deutschland anbieten, findet sich unter <http://www.handyticket.de/regionen.html>.

Von der BVG und der S-Bahn werden laut eigener Auskunft im Rahmen des „Touch & Travel“-Systems keine Kunden- oder Bewegungsdaten erhoben. Die Erhebung und Verarbeitung der Daten erfolgt durch die DB Mobility Logistics AG, die auch bei der Nutzung durch die Nahverkehrsbetriebe datenschutzrechtlich verantwortliche Stelle ist. Dies ist für den Fahrgast jedoch nicht immer eindeutig erkennbar; die Transparenz sollte hier erhöht werden. Über die Datenschutzprobleme im Zusammenhang mit „Touch & Travel“ haben wir bereits berichtet.¹⁰³ Leider ist hier in den letzten zwölf Monaten keine signifikante Verbesserung vor allem bezüglich datensparsamer Nutzungsalternativen erfolgt. In unseren Gesprächen mit der DB konnte jedoch erreicht werden, dass die Nutzungsdaten der Fahrgäste nicht mehr zehn Monate gespeichert bleiben, wie es zu Beginn des Projektes für Forschungszwecke mit den Pilotkunden vereinbart war, sondern nur noch 55 Tage ab Rechnungsversand.

Personen, die aus Datenschutzgründen von einer Nutzung des „Touch & Travel“-Angebots absehen wollen, können alternativ auch das Handyticket der DB oder alle herkömmlichen Vertriebswege nutzen.

Personen, die den Erwerb und die Nutzung von Fahrscheinen über das Mobiltelefon ausprobieren wollen, sollten das HandyTicket Deutschland nutzen oder im Fernverkehr weiterhin auf die herkömmlichen Vertriebswege der DB oder auf das DB-Handyticket zurückgreifen. Beim „Touch & Travel“-Angebot werden demgegenüber auch umfangreiche Bewegungsdaten des Fahrgasts verarbeitet.

Parktickets übers Handy

Aktuell bieten in Berlin sechs verschiedene Betreiber den Erwerb von Parkscheinen mithilfe des Mobiltelefons an. Um das Angebot zu nutzen, ist es zunächst erforderlich, sich bei dem Betreiber zu registrieren. Eine Vignette, die im Auto hinter der Windschutzscheibe angebracht wird, signalisiert den Beschäftigten des Ordnungsamtes bei Kontrollen, dass der Parkschein per Handy erworben wurde. Der Erwerb kann über den

103 JB 2011, 4.1

Anruf einer Servicenummer oder alternativ per SMS oder über eine Smartphone-App erfolgen. Am Monatsende erhält die Kundin oder der Kunde dann vom jeweiligen Betreiber eine Sammelrechnung über alle registrierten Parkvorgänge für alle angemeldeten Fahrzeuge. Dieses Angebot ist für alle Mobilfunkkunden nutzbar, unabhängig davon, ob diese eine Prepaidkarte oder einen dauerhaften Mobilfunkvertrag nutzen.

Eine etwas datenschutzfreundlichere Alternative bieten die Anbieter EasyPark und sunhill technologies an. Beim **SMS-Parken** von EasyPark kann das Angebot auch ohne Vorregistrierung genutzt werden. Hierfür ist nur die kostenlos im Internet erhältliche Vignette auszudrucken und jeweils eine SMS an den Anbieter zu schicken, wenn ein Parkticket benötigt wird. Die Abrechnung der Kosten erfolgt über die Telefonrechnung, sofern der Mobilfunkanbieter der Kundin oder des Kunden das Angebot unterstützt. Das Unternehmen sunhill technologies bietet seit Dezember 2011 in Zusammenarbeit mit dem Bezirk Pankow das System „sms & park“ an. Bei diesem System sind keine Registrierung und keine Vignette nötig. Die oder der Nutzende sendet nur das Kfz-Kennzeichen und die gewünschte Parkdauer per SMS an die ausgeschilderte Kurzwahlnummer der jeweiligen Parkzone. Anschließend erhält sie oder er eine SMS, die als virtueller Parkschein dient und den Bezahlvorgang bestätigt.¹⁰⁴ Die Parkgebühr wird automatisch mit der monatlichen Handyrechnung abgebucht oder mit dem Prepaid-Guthaben der Kundin oder des Kunden verrechnet. Die Mitarbeiterinnen und Mitarbeiter der Parkraumüberwachung können durch eine Abfrage des Kfz-Kennzeichens eine Überprüfung des virtuellen Parkscheins vornehmen. Laut Auskunft von sunhill technologies werden außer dem Kennzeichen keine weiteren Daten an die Stadt übermittelt.

Die Angebote für das Handyparken mit Registrierung sind akzeptabel, da nicht mehr personenbezogene Daten (Name, Anschrift, E-Mail-Adresse, Kfz-Kennzeichen, Handynummer und gewünschter Zahlungsweg) erhoben werden als erforderlich. Die Systeme ohne Registrierung sind dem jedoch eindeutig vorzuziehen, da hier dem Anbieter nur das Kfz-Kennzeichen und die Handynummer der Nutzerin oder des Nutzers bekannt sind.

104 Siehe http://www.sunhill-technologies.com/files/pdf/smspark_BerlinPankow_Flyer_.pdf

Alle Systeme führen zur Erstellung von Bewegungs- und Nutzungsprofilen, da jeweils die Nutzungshäufigkeit der Kunden zu Abrechnungszwecken sowie die genutzten Parkzonen erhoben und gespeichert werden. Da die in Berlin tätigen Anbieter auch in anderen deutschen Städten aktiv sind, besteht hier die Gefahr einer umfassenden Profilbildung, sofern jemand das System eines Anbieters in mehreren Städten nutzt.

6 Justiz

6.1 Zentrale Auskunftsstelle Justizvollzug

Das 2011 in Kraft getretene Justizvollzugsdatenschutzgesetz¹⁰⁵ sieht u. a. die Einrichtung einer zentralen Auskunftsstelle für die Übermittlung personenbezogener Daten Gefangener an öffentliche und nicht-öffentliche Stellen außerhalb des Justizvollzugs vor.¹⁰⁶ Bei dieser Stelle kann z. B. das Opfer einer Straftat sowie dessen Rechtsnachfolger Auskunft über die Entlassungsadresse oder die Vermögensverhältnisse von Gefangenen verlangen, soweit diese Auskunft zur Feststellung oder Durchsetzung von Rechtsansprüchen im Zusammenhang mit der Straftat erforderlich ist.¹⁰⁷

Die zentrale Auskunftsstelle ist räumlich und organisatorisch der Justizvollzugsanstalt Moabit zugeordnet.¹⁰⁸ Es ist gesetzlich vorgesehen, dass dort zwar die Übermittlung personenbezogener Daten an externe Stellen konzentriert wird, die Auskunftsstelle selbst jedoch keine eigenen Dateien mit personenbezogenen Daten Gefangener führt. Diese Daten werden weiterhin dezentral bei den Justizvollzugsanstalten gespeichert und dort von der Auskunftsstelle zur Beantwortung von Anfragen abgerufen.¹⁰⁹

Bei der Einrichtung der zentralen Auskunftsstelle wurden wir um technische und rechtliche Beratung gebeten. So konnten wir Hinweise geben, in welcher Form sich die anfragende Stelle vor der Auskunft über einen Gefangenen identifizieren muss, welche Zugriffsmöglichkeiten die Beschäftigten der zentralen Auskunftsstelle im Hinblick auf die bei den Justizvollzugsanstalten gespeicherten Gefangenenendaten haben sollen und wie eine erfolgte Auskunftserteilung zu dokumentieren ist. Daneben haben wir bei den künftigen Beschäftigten der zentralen Auskunftsstelle eine datenschutzrechtliche Schulung durchgeführt.

105 JB 2011, 2.2.3

106 § 47 Justizvollzugsdatenschutzgesetzes (JVollzDSG)

107 § 46 Abs. 2 Nr. 1 JVollzDSG

108 Siehe ABl. vom 22. Juni 2012, S. 986

109 § 48 Abs. 1 Satz 2 JVollzDSG

Wie bereits bei der Ausarbeitung des Justizvollzugsdatenschutzgesetzes wurde uns auch bei der Einrichtung der zentralen Auskunftsstelle der Justiz von den verantwortlichen Stellen frühzeitig und umfassend die Möglichkeit zur Stellungnahme gegeben. Denkbaren Fehlern bei der praktischen Durchführung des Auskunftsverfahrens konnte auf diese Weise vorgebeugt werden.

6.2 Einsichtnahme in frühere Examensklausuren

In der juristischen Ausbildung besteht bei Studierenden und Referendaren insbesondere im Hinblick auf die beiden Examina ein großes Interesse, ehemalige Prüfungsaufgaben einzusehen. Ein Student, dem das Gemeinsame Juristische Prüfungsamt der Länder Berlin und Brandenburg (GJPA) die Einsicht in frühere Examensklausuren zur Vorbereitung der Ersten juristischen Staatsprüfung verweigert hatte, beschwerte sich bei uns hierüber unter Berufung auf das Informationsfreiheitsgesetz (IFG).

Wir teilten ihm mit, dass das Juristenausbildungsgesetz (JAG) abschließend die Informationsrechte im Hinblick auf Unterlagen regelt, die das Prüfungsverfahren betreffen.¹¹⁰ Danach wird dem Prüfling nach Beendigung der Prüfung Einsicht in die über ihn geführten Prüfungsakten gewährt. Ein Dritter darf nur mit schriftlichem Einverständnis des Prüflings dessen Prüfungsakte einsehen. Weitergehende Informationsrechte des Prüflings oder Dritter aufgrund anderer Rechtsgrundlagen sind ausdrücklich ausgeschlossen. Der Ausschluss weitergehender Informationsrechte betrifft auch Unterlagen, die der Vorbereitung und Durchführung von Prüfungen dienen, jedoch nicht (nur) für bestimmte Prüfungsvorgänge verwendet werden wie etwa Aufgabentexte und Lösungsskizzen. Das GJPA hat dem Studenten daher zu Recht die Einsicht in die Klausurunterlagen verweigert.¹¹¹

110 § 23 Abs. 2 JAG

111 Siehe auch den Beschluss des OVG Berlin-Brandenburg vom 3. Dezember 2007 (OVG 12 N 40.07)

Das JAG schränkt die Informationsrechte für Prüfungsunterlagen ein, während das IFG keine Anwendung findet.

6.3 Auslagerungen gerichtlicher Archivakten

Einige Gerichte haben uns darauf aufmerksam gemacht, dass sie aus Kapazitätsgründen Akten durch private Unternehmen auslagern lassen bzw. dies derzeit planen. Uns wurde mitgeteilt, dass die BIM Berliner Immobilienmanagement GmbH (BIM), die die Räume für die Auslagerungen zur Verfügung stellt, in dieser Angelegenheit koordinierend tätig wird und entsprechende Verträge für die Gerichte abschließt.

Gerichte sind für die Archivierung ihrer Aktenbestände selbst verantwortlich; eine Weitergabe von Akten an Dritte und eine dortige Verwahrung der Akten mit der Möglichkeit des Zugriffs auf den Inhalt ist nur bei einer Auftragsdatenverarbeitung zulässig. Diese unterliegt bestimmten gesetzlichen Anforderungen.¹¹² Der Auftrag ist durch das betreffende Gericht schriftlich zu erteilen. Hierbei muss insbesondere der Gegenstand des jeweiligen Auftrags genau beschrieben werden. Es muss konkret bestimmt sein, welche Akten für welchen Zeitraum in welcher Form durch den Vertragspartner archiviert werden sollen. Dem Auftraggeber sind hierbei umfassende Kontrollrechte und Weisungsbefugnisse einzuräumen.

In diesem Fall besteht zum einen die Möglichkeit, dass die BIM selbst im Auftrag der Gerichte die Archivierung vornimmt oder bei entsprechender vertraglicher Vereinbarung durch Unterauftragnehmer vornehmen lässt. Zum anderen können die Gerichte auch direkt mit den privaten Unternehmen Verträge über die Auftragsdatenverarbeitung abschließen, soweit gewährleistet ist, dass die BIM als Eigentümerin der für die Archivierung genutzten Räume keinen Zugang zu den Akten hat. Für diese Alternative haben sich die Gerichte entschieden.

112 § 3 BlnDSG

Die Auslagerung gerichtlicher Archivakten unter Beteiligung privater Unternehmen ist nur im Rahmen der gesetzlichen Vorgaben für die Auftragsdatenverarbeitung zulässig.

7 Finanzen

7.1 Einsichtnahme in Steuerakten – Neubewertung von Gebäudeteilen

Aus der Praxis

Ein Ehepaar teilte uns mit, es habe 2003 zusammen mit anderen Investoren in Frankfurt/Oder ein Grundstück gekauft, das mit Bungalows bebaut sei. Diese würden überwiegend zu Wohnzwecken, teilweise aber auch für gastronomische, Verwaltungs- und Lagerzwecke genutzt werden. Aus den Einnahmen für die Vermietung und Verpachtung bestreite das Ehepaar neben der Altersrente den Lebensunterhalt. Durch eine plötzliche rückwirkende Änderung der Besteuerung – zurückzuführen auf eine vom Finanzamt vorgenommene Neubewertung der Gebäudeanteile – seien diese Einnahmen erheblich reduziert worden. Die Bitte um Übermittlung dieser Neubewertung sei von den Finanzbehörden ebenso abgelehnt worden wie die beantragte Einsichtnahme der Unterlagen.

Das Recht auf Einsichtnahme der eigenen Steuerunterlagen durch die Steuerpflichtige oder den Steuerpflichtigen ist seit Jahren umstritten.¹¹³ Die Einsichts- und Auskunftsrechte der oder des Betroffenen nach § 16 BlnDSG werden von der Senatsverwaltung für Finanzen unter Hinweis auf den angeblichen Vorrang der bereichsspezifischen Regelungen in der Abgabenordnung abgelehnt. Bisher hat es der Bundesgesetzgeber jedoch versäumt, entsprechende Regelungen in die Abgabenordnung aufzunehmen. Die Diskussionsentwürfe des Bundesministeriums für Finanzen sahen zunächst vor, dass Betroffene ein berechtigtes Interesse für ihr Einsichtsbegehren darzulegen haben. Im Oktober 2011 wurde vom Ministerium ein Entwurf vorgelegt, der auf diese Darlegungspflicht verzichtet. Auch wenn im Hinblick auf den Entwurf weiterhin Ergänzungs- und Änderungsbedarf besteht, ist dieser Sinneswandel grundsätzlich zu begrüßen.

Wir haben die Senatsverwaltung für Finanzen vor dem Hintergrund dieser Entwicklung gebeten, dem Petenten eine umfassende Einsichtnahme in seinen Steuervorgang zu gewähren. Die Senatsverwaltung teilte uns mit, dass

113 JB 2006, 4.4.1

dem Petenten die notwendigen Unterlagen zur Neubewertung der Gebäudeanteile bereits übersandt wurden. Dem Auskunftsanspruch des Petenten sei damit bereits entsprochen worden. Darüber hinaus sei das Finanzamt jedoch bereit, mit dem Petenten einen Termin zur Einsichtnahme der Steuerakten im Finanzamt zu vereinbaren.

Im Vorgriff auf die Einführung einer Regelung in der Abgabenordnung ist den Betroffenen auf Antrag Auskunft und Einsichtnahme ihrer eigenen Steuervorgänge zu gewähren. Dabei ist auf die Darlegung des Informationsinteresses durch die antragstellende Person zu verzichten.

7.2 Steuerfahndung in der Fahrschule

Der Datenschutzbeauftragte der DEKRA informierte uns darüber, dass das Finanzamt für Fahndung und Strafsachen zur steuerlichen Überprüfung der Einnahmen von Fahrschulen um die Übersendung der sog. DEKRA-Prüflisten von 178 Fahrschulen für die Jahre 2008 bis 2010 mit Namen und Anschriften aller Prüflinge sowie Angaben zur Anzahl der abgelegten Prüfungen, dem Datum der theoretischen und praktischen Prüfungen mit Führerscheinklassen sowie der Anzahl der Wiederholungsprüfungen gebeten habe. Zur Begründung habe das Finanzamt vorgetragen, dass anlässlich von Außenprüfungen der Steuerverwaltungen von Berlin und anderen Bundesländern festgestellt worden sei, dass Fahrschulen ihre steuerlichen Verpflichtungen nicht immer ordnungsgemäß erfüllen. In einer Vielzahl von Fällen seien Einnahmen ganz oder teilweise nicht erklärt worden.

Die Senatsverwaltung für Finanzen hat dies bestätigt. Der Hintergrund sei, dass bei Betriebsprüfungen in 132 Fahrschulen in den vergangenen Jahren in 80 Fällen ein Mehrergebnis festgestellt worden sei. Grundsätzlich bestehe das Problem, dass die Einnahmen, die durch das „Weglassen von Fahrstunden oder Fahrschülern“ nicht vollständig erklärt werden, für die Außenprüfdienste der Steuerverwaltung nicht feststellbar seien. Dies könne durch den Abgleich der Aufzeichnungen des Unternehmens mit den sog. TÜV/DEKRA-Prüflisten

beholden werden. In diesen Listen seien Name und Anschrift jedes einzelnen zur Fahrprüfung angemeldeten und vorzustellenden Prüflings, die Führerscheinklasse und Angaben zur Wiederholungsprüfung enthalten.

Nach der Rechtsprechung setzt die Abgabenordnung¹¹⁴ einen hinreichenden Anlass für ein Tätigwerden der Steuerverwaltung voraus. Ein solcher Anlass liegt vor, wenn aufgrund konkreter Anhaltspunkte oder Erfahrungen die Möglichkeit einer Steuerverkürzung in Betracht kommt und daher eine Anordnung bestimmter Art angezeigt ist. Ermittlungen „ins Blaue hinein“, Rasterfahndungen, Ausforschungsdurchsuchungen oder ähnliche Ermittlungsmaßnahmen sind dagegen unzulässig. Aufgrund der von der Senatsverwaltung dargelegten Tatsachen und der Ergebnisse der Außenprüfungen in den vergangenen Jahren ist davon auszugehen, dass ein hinreichender Tatverdacht im Sinne der Abgabenordnung für eine Überprüfung von 178 Fahrschulen gegeben ist. Erhebliche Bedenken bestehen jedoch hinsichtlich der Verhältnismäßigkeit des Umfangs der Datenanforderung. Warum die Übermittlung von Name und Anschrift sämtlicher Führerscheinprüflinge von 178 Fahrschulen für die Jahre 2008 bis 2010¹¹⁵ für die Aufklärung zunächst noch unbekannter Steuerfälle und Sachverhalte erforderlich sein soll, ist nicht nachvollziehbar.

Es gilt der Grundsatz der Datenvermeidung und Datensparsamkeit. Verfahren zur Verarbeitung von personenbezogenen Daten haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Dabei ist insbesondere von der Möglichkeit der Pseudonymisierung Gebrauch zu machen.¹¹⁶ Hier ist es zunächst ausreichend, wenn dem Finanzamt die Datenbestände der einzelnen Fahrschulen von der DEKRA in pseudonymisierter Form übermittelt werden. Ergeben sich beim Abgleich der von der DEKRA gemeldeten Prüfungen und den Angaben der Fahrschule in der Steuererklärung Differenzen, können vom Finanzamt in einem zweiten Schritt die personenbezogenen Daten der Fahrschülerinnen und -schüler angefordert werden.

114 § 208 Abs. 1 Nr. 3 AO

115 Dabei handelt es sich um mehr als tausend unbeteiligte Betroffene.

116 § 5a BlnDSG

Das Finanzamt für Fahndung und Strafsachen hat auf unsere Bedenken reagiert und bestätigt, dass es zunächst auf die Übersendung von Datensätzen mit einem Personenbezug (Name, Anschrift der Prüflinge) verzichtet. Nur wenn die personenbezogenen Daten der Fahrschülerinnen und -schüler zur Durchführung einer konkreten Betriebsprüfung einer bestimmten Fahrschule im Einzelfall erforderlich sind, werden sie in einem zweiten Schritt bei der DEKRA erhoben.

Dem Grundsatz der Datenvermeidung und Datensparsamkeit bei der Datenverarbeitung ist durch Verfahren der Pseudonymisierung auch bei Steuerprüfungen verstärkt Rechnung zu tragen.

8 Jugend und Soziales

8.1 WIMES – ein neues Verfahren für die Jugendhilfe

Anfang des Jahres wurden wir auf ein technisches Verfahren aufmerksam, das in einigen Jugendämtern eingesetzt wird. Das webbasierte Verfahren WIMES („Wirkungen messen“) soll in erster Linie dem Zweck dienen, die Wirksamkeit von Hilfen zur Erziehung zu evaluieren, und damit zur Qualitätssicherung beitragen. Das Verfahren wird von einem privaten Dienstleister über ein Webportal angeboten und betrieben.

WIMES wird seit 2010 im Rahmen eines Projektes zur Untersuchung des Ziel-Wirkungs-Zusammenhangs in den Hilfen zur Erziehung von der Senatsverwaltung für Bildung, Jugend und Wissenschaft eingesetzt. An dem Projekt sind derzeit fünf Bezirke beteiligt. Da die Senatsverwaltung fälschlich davon ausging, es würden lediglich anonymisierte Datensätze zur Erstellung von Statistiken verarbeitet, verzichtete sie bei der Einführung des Verfahrens auf die gesetzlich vorgesehene Einbindung unserer Behörde.¹¹⁷

Bei einer Überprüfung des Verfahrens konnten wir feststellen, dass die im Rahmen der Hilfeplanung von den Jugendämtern erhobenen Sozialdaten personenbezogen über ein Webportal in die Datenbank des privaten Dienstleisters eingegeben und dort unverschlüsselt gespeichert wurden. Zudem erstellten die Jugendämter und freien Träger als Leistungserbringer eine gemeinsame personenbezogene Falldokumentation über das WIMES-Webportal, die ebenfalls in der Datenbank des privaten Dienstleisters gespeichert wurde. Eine Pseudonymisierung der Sozialdaten erfolgte dann erst für die statistische Auswertung. Die Speicherung der Daten in personenbezogener Weise bei dem privaten Dienstleister, der statistische Auswertungen vornehmen sollte, war nicht erforderlich. Da zudem weder die notwendigen Verträge zur Auftragsdatenverarbeitung mit dem privaten Dienstleister abgeschlossen noch die – offenbar bereits entwickelten – Maßnahmen zur Verschlüsselung der Sozialdaten bei den

117 § 24 Abs. 3 Satz 3 BlnDSG

Jugendämtern und freien Trägern umgesetzt worden waren, haben wir einen datenschutzrechtlichen Mangel festgestellt.

Die Senatsverwaltung hat daraufhin veranlasst, dass die notwendige Verschlüsselung der Daten in der Datenbank des privaten Dienstleisters als Auftragnehmer der bezirklichen Jugendämter bzw. der Senatsverwaltung umgesetzt wurde. Eine Entschlüsselung der Daten durch den privaten Dienstleister kann nicht mehr erfolgen. Lediglich die Jugendämter und die beteiligten freien Träger haben Zugriff auf die nicht verschlüsselten personenbezogenen Daten des jeweiligen Einzelfalls. Die zuvor beschriebenen Mängel hätten vermieden werden können, wenn ein nach den IT-Sicherheitsgrundsätzen¹¹⁸ vorgeschriebenes verfahrensspezifisches Sicherheitskonzept vor der Verfahrenseinführung erstellt worden wäre.

Da der Gesetzgeber enge Grenzen für die Zulässigkeit einer Auftragsdatenverarbeitung für Sozialleistungsträger, zu denen auch die Jugendämter zählen, gezogen hat, ist das WIMES-Verfahren grundsätzlich als datenschutzrechtlich kritisch zu betrachten. Derzeit wird im WIMES-Verfahren jedoch lediglich ein kleiner Ausschnitt der in den Hilfen zur Erziehung erhobenen Daten genutzt, um die Wirkungen der Hilfen zu evaluieren. Die originäre Fallbearbeitung erfolgt außerhalb des WIMES-Verfahrens. Vor diesem Hintergrund ist das Verfahren nach Einführung der Verschlüsselung datenschutzrechtlich tragbar.

Die von der Senatsverwaltung für Bildung, Jugend und Wissenschaft bereits geplante fachliche Erstreckung des WIMES-Verfahrens auf die Fallbearbeitung ist datenschutzrechtlich sehr problematisch.

8.2 Kinderschutz und Datenschutz

Wie in den vergangenen Jahren nahmen wir auch in diesem Jahr an den Sitzungen der unter Federführung der Senatsverwaltung für Bildung, Jugend und Wissenschaft tagenden Projektgruppe „Netzwerk Kinderschutz“ teil. Ebenso

118 Nr. 2.5 i.V.m. Nr. 4.7 IT-Sicherheitsgrundsätze der Berliner Verwaltung

beteiligten wir uns intensiv an der seit Inkrafttreten des Berliner Gesetzes zum Schutz und Wohl des Kindes Anfang 2010 unter Leitung der Senatsverwaltung für Gesundheit und Soziales tagenden „BegleitAG zum Kinderschutzgesetz“. Uns geht es darum, die datenschutzrechtlichen Belange möglichst frühzeitig einzubringen. Häufig lassen sich auf diese Weise ohne langwierige Abstimmungsprozesse sachgerechte Lösungen im Interesse aller Beteiligten finden. Als Beispiel sind in der Praxis aufgetretene Schwierigkeiten im Umgang mit Adoptionsfällen bei der für das verpflichtende Einladungswesen zuständigen Zentralen Stelle bei der Charité zu nennen. Die betroffenen Familien bedürfen eines besonderen datenschutzrechtlichen Schutzes, der auch im (weitgehend automatisierten) verpflichtenden Einladungswesen zu berücksichtigen ist. Zwischen den beteiligten Senatsverwaltungen für Gesundheit und Soziales sowie Bildung, Jugend und Wissenschaft, der Zentralen Stelle bei der Charité und uns konnte zügig eine datenschutzgerechte Lösung gefunden werden.

Auch im kommenden Jahr werden wir uns konstruktiv an den Sitzungen beteiligen und für die datenschutzrechtlichen Belange im Interesse des Kinderschutzes einsetzen.

8.3 Bezirksamt lädt Vermieter zur Schnüffelei ein

Im letzten Jahr berichteten wir über einen von der Senatsverwaltung für Bildung, Jugend und Wissenschaft erarbeiteten Handlungsleitfaden zur Zusammenarbeit zwischen Gerichtsvollziehern und bezirklichem Jugendamt im Kinderschutz.¹¹⁹ Dieser Handlungsleitfaden erweckte den Eindruck, Gerichtsvollzieher hätten die Aufgabe, bei ihrer Tätigkeit nach Anhaltspunkten für Kindeswohlgefährdungen zu suchen und Meldung gegenüber dem Jugendamt zu machen. Das ist mit ihren gesetzlichen Aufgaben jedoch unvereinbar. Nach erheblicher Kritik unserer Behörde und der Senatsverwaltung für Justiz nahm die Senatsverwaltung für Bildung, Jugend und Wissenschaft den Handlungsleitfaden zurück. Später mussten wir uns erneut mit der Problematik beschäftigen.

119 JB 2011, 7.1.4

Der Verband Berlin Brandenburgischer Wohnungsunternehmen e.V. kam auf die Idee, einen ähnlichen Handlungsleitfaden zu entwickeln. Er bat uns um datenschutzrechtliche Bewertung des Entwurfs der Verhaltensempfehlung „Wohnungsunternehmen und Kinderschutz“. Als Grundlage für den Text diente die Handlungsempfehlung für Gerichtsvollzieher, abgeändert dahingehend, dass die Meldungen nunmehr durch Vermieter bzw. Beschäftigte der Wohnungsunternehmen an das Jugendamt erfolgen sollten.

Bei der datenschutzrechtlichen Bewertung geht es keineswegs darum, Beschäftigten von Unternehmen der Wohnungswirtschaft die Möglichkeit zu nehmen, bei eindeutigen Anzeichen von Kindeswohlgefährdung tätig zu werden. Sie können sogar verpflichtet sein, zur Abwehr einer akuten Gefährdung die Polizei einzuschalten – eine Pflicht, die jedermann obliegt. Die Kritik richtet sich vielmehr darauf, dass es keine Möglichkeit gibt, die Beschäftigten soweit zu professionalisieren, dass sie fachlich in der Lage sind, anhand vorgegebener Kriterien Verdachtsmomente für unterhalb dieser Schwelle einzuordnende Kindeswohlgefährdungen aufzudecken. Personen, die bei Wohnungsunternehmen beschäftigt sind und gänzlich andere Aufgaben haben, wären schlichtweg überfordert. Wie sollen – wie im Kriterienkatalog beispielhaft vorgegeben – Mitarbeiterinnen und Mitarbeiter von Hausverwaltungen richtig beurteilen, ob dem Kind ungestörter Schlaf oder emotionale Zuwendung fehlt, körperliche Entwicklungsverzögerungen oder starke Bildungsdefizite vorliegen? Eine fachlich richtige Einordnung muss Personen überlassen bleiben, die aufgrund ihrer Ausbildung dazu qualifiziert sind. Wird dagegen von Wohnungsunternehmen und ihren Beschäftigten verlangt, Informationen über ihre Mieterinnen und Mieter, deren Familien und ihre häuslichen Verhältnisse zu erheben und anhand vorgegebener Kriterien Einschätzungen vorzunehmen, besteht immer die Gefahr, dass aus Sorge, Anzeichen für Kindeswohlgefährdungen zu übersehen, Jugendämter informiert werden, obwohl vielleicht gar keine Gefahren für das Kind bestehen. Die Folgen für die Familien und das weitere Mietverhältnis sind nicht absehbar.

Viel wichtiger ist es, Wohnungsunternehmen und ihre Beschäftigten aufzufordern, nicht wegzuschauen, wenn ihnen Beunruhigendes auffällt oder durch andere Nachbarn bekannt wird, sie darauf aufmerksam zu machen, dass die „Berliner Hotline Kinderschutz“ 24 Stunden am Tag besetzt ist und Rat erteilen kann, und ihnen Kontaktdaten der Krisendienste der bezirklichen

Jugendämter in die Hand zu geben. Oft wird es nicht einmal nötig sein, personenbezogene Daten der Familien weiterzugeben, wenn Beschäftigte Beratung über ihre Wahrnehmungen in Anspruch nehmen. Sie können darauf vertrauen, dass sowohl die bei der Hotline Kinderschutz als auch bei den bezirklichen Jugendämtern Tätigen in der gebotenen Weise mit den Hinweisen umzugehen wissen und weiterführenden Rat erteilen.

Im November war der Tagespresse zu entnehmen, dass das Bezirksamt Lichtenberg mit der Wohnungsbaugesellschaft HOWOGE eine Kooperationsvereinbarung zum Kinderschutz abgeschlossen hat. Ein Mitarbeiter pro Kundenzentrum der HOWOGE soll verantwortlich für die Bewertung der eingegangenen Meldungen zu Kindeswohlgefährdungen sein. Mitarbeiter der HOWOGE sollen anhand des – eigens für Fachkräfte der Jugendhilfe – entwickelten berlin-einheitlichen Katalogs Risikofaktoren zur Erkennung und Einschätzung von Gefährdungssituationen bewerten und dann mit einem Schnellmeldebogen die Daten an das Jugendamt weitergeben. Das Jugendamt soll dann standardisiert eine Rückmeldung an die HOWOGE geben. Das Verfahren ist aus den oben dargelegten Gründen mit den gesetzlichen Datenschutzregelungen des Kinder- und Jugendhilferechts, aber auch mit den für die HOWOGE geltenden Datenschutzvorschriften unvereinbar. Leider haben weder das Bezirksamt Lichtenberg noch die HOWOGE unsere Behörde beteiligt. Erst durch Nachfrage erhielten wir die Kooperationsvereinbarung. Wir haben dem Bezirksamt unsere datenschutzrechtlichen Bedenken mitgeteilt und die HOWOGE in unserer Funktion als Aufsichtsbehörde nach dem Bundesdatenschutzgesetz¹²⁰ aufgefordert, das vereinbarte Verfahren nicht fortzuführen.

Beschäftigte von Wohnungsbaugesellschaften zu verpflichten, bei ihrer Tätigkeit Informationen über Familien zu sammeln und in einem vorgegebenen Verfahren an das Jugendamt zu melden, lässt keinen verbesserten Kinderschutz erwarten. Wichtiger ist es, sie zu sensibilisieren, nicht wegzusehen, wenn ihnen etwas merkwürdig erscheint. Sie sollten ermuntert werden, sich – ohne die Familie namentlich zu benennen – fachkundigen Rat bei der Hotline Kinderschutz oder dem Krisendienst des Jugendamtes einzuholen.

120 § 33 BlnDSG i.V.m. § 38 BDSG

8.4 Überschießende Datenerhebung im Sozialamt

Ein Petent bezog Sozialleistungen in Form des sog. Persönlichen Budgets von einem Sozialamt. Beim Persönlichen Budget handelt es sich um eine alternative Leistungsform. Die Leistungsempfangenden erhalten jeden Monat einen festen Geldbetrag zur Verwendung für Betreuungs- und Hilfeleistungen und können ihn für die benötigten Hilfen selbstständig einsetzen sowie diese eigenständig organisieren. Sie treten in diesem Zusammenhang als Arbeitgeber auf und schließen für die notwendige Betreuung und Pflege sozialversicherungspflichtige Arbeits- bzw. Honorarverträge mit den jeweiligen Betreuungskräften ab.

Im Rahmen der halbjährlichen Überprüfung der zweckgebundenen Verwendung des Persönlichen Budgets verlangte das Sozialamt von dem Petenten, lückenlose und ungeschwärzte Unterlagen einzureichen. Bei diesen Unterlagen handelte es sich um Arbeits- und Honorarverträge, Kontoauszüge mit Nachweisen über die Zahlungsempfänger und Beträge, Abrechnungsbelege vom Lohnbüro und die Jahresabrechnung des Steuerberaters.

Die Datenerhebung des Sozialamts war unzulässig. Für die Überprüfung der zweckgebundenen Verwendung des Persönlichen Budgets ist es nicht notwendig, gänzlich ungeschwärzte Unterlagen anzufordern. Sowohl bei den in den angeforderten Unterlagen enthaltenen personenbezogenen Daten des Petenten sowie der Angestellten handelt es sich um Sozialdaten. Das sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person (Betroffener), die von einem Sozialleistungsträger im Hinblick auf die ihm nach dem Sozialgesetzbuch obliegenden Aufgaben erhoben, verarbeitet oder genutzt werden.¹²¹ Die oder der Betroffene muss demnach keine leistungsempfangende Person sein bzw. keinen Antrag auf Sozialleistungen gestellt haben. Der Anspruch auf Wahrung des Sozialgeheimnisses steht jeder Person zu, von der ein Sozialleistungsträger Daten erhebt, verarbeitet oder nutzt.

121 Siehe § 67 Abs. 1 Satz 1 SGB X

Sozialdaten dürfen nur dann erhoben werden, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle, hier also des Sozialamtes, erforderlich ist. Erforderlichkeit in diesem Sinne bedeutet nicht, dass bestimmte Angaben lediglich als Hintergrundinformationen wünschenswert wären. Vielmehr ist die Kenntnis der Daten nur dann erforderlich, wenn das Sozialamt ohne diese Daten im konkreten Einzelfall die ihm gesetzlich zugewiesenen Aufgaben nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann.

Auch anhand teilweise geschwärzter Unterlagen lässt sich nachvollziehen, ob die leistungsempfangende Person Pflegepersonal beschäftigt und ob sie entsprechende Überweisungen getätigt hat. So wäre es z. B. bei Kontoauszügen ausreichend, wenn aus ihnen der Verwendungszweck und die überwiesene Summe ersichtlich wird. Unterlagen, aus denen sich Sozialdaten des angestellten Pflegepersonals ergeben, sind für die Kontrolle des zweckentsprechenden Einsatzes des Geldes nicht erforderlich. Ohnehin lässt sich weder anhand geschwärzter noch anhand ungeschwärzter Unterlagen überprüfen, ob die Leistung vom Pflegepersonal tatsächlich erbracht worden ist.

Wir haben die Verfahrensweise des Sozialamtes förmlich beanstandet.¹²² Der Bezirksbürgermeister hält jedoch an der Anforderung gänzlich ungeschwärzter Belege für die Überprüfung der zweckgebundenen Verwendung des persönlichen Budgets fest, sodass dem datenschutzrechtlichen Mangel nicht abgeholfen werden konnte.

Für die Überprüfung der zweckgebundenen Verwendung des persönlichen Budgets ist es nicht notwendig, ungeschwärzte Unterlagen anzufordern. Auch anhand teilweise geschwärzter Unterlagen lässt sich nachvollziehen, ob die leistungsempfangende Person Pflegepersonal beschäftigt und ob sie entsprechende Überweisungen getätigt hat.

122 § 26 Abs. 1 BlnDSG

8.5 Fremde Daten in der Schwerbehindertenakte

In der beim Landesamt für Gesundheit und Soziales (LAGeSo) geführten Schwerbehindertenakte eines Petenten waren fremde Unterlagen abgeheftet. Dies hat der Petent bei einer Akteneinsicht festgestellt. Es handelte sich um Unterlagen einer namensgleichen Person, die im gleichen Jahr wie der Petent, jedoch an einem anderen Tag geboren ist. Wegen eines beim Sozialgericht anhängigen Verfahrens ist die Akte mit den fremden Daten an das Sozialgericht übermittelt worden.

Das LAGeSo hat die Verwechslung mit einer namensgleichen Person aus Halle an der Saale bestätigt. Es habe die Akte des Petenten zwar unter Angabe des korrekten Geburtsdatums beim Versorgungsamt Halle/Saale angefordert, es sei jedoch die falsche Akte übermittelt worden. Dies sei keiner der beiden Behörden aufgefallen.

Die Speicherung der Daten der namensgleichen Person beim LAGeSo, die Datenübermittlung an den Petenten bei der Akteneinsicht sowie die Datenübermittlung an das Sozialgericht waren rechtswidrig. Bei den fremden Daten, die an den Petenten und das Sozialgericht übermittelt wurden, handelte es sich um personenbezogene Daten aus einer Schwerbehindertenakte und damit zumindest auch um Gesundheitsdaten. Speichert oder übermittelt ein Sozialleistungsträger wie das LAGeSo personenbezogene Daten, handelt es sich dabei um Sozialdaten. Deren Speicherung ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Sozialleistungsträgers liegenden gesetzlichen Aufgaben erforderlich ist und für Zwecke erfolgt, für die die Daten erhoben worden sind.¹²³ Eine Übermittlung von Sozialdaten, also das Bekanntgeben an Dritte, ist nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis bzw. eine Einwilligung der betroffenen Person vorliegt.¹²⁴

In diesem Fall sind nicht die Sozialdaten des Petenten, sondern einer anderen namensgleichen Person in der Schwerbehindertenakte des Petenten gespeichert worden. Diese fremden Daten stehen inhaltlich in keinem Zusammenhang mit der Angelegenheit des Petenten. Sie sind für die gegenüber dem

123 § 67 c Abs. 1 Satz 1 SGB X

124 § 67 d Abs. 1 i.V.m. § 67 b Abs. 1 Satz 1 SGB X

Petenten ergehenden behördlichen Entscheidungen ohne Belang. Daher hätten die fremden Sozialdaten weder in der Schwerbehindertenakte des Petenten gespeichert noch im Rahmen der Akteneinsicht an ihn und auch nicht – im Zusammenhang mit dem anhängigen Gerichtsverfahren – an das Sozialgericht übermittelt werden dürfen.

Wir haben gegenüber dem LAGeSo einen datenschutzrechtlichen Mangel festgestellt¹²⁵ und auf die in solchen Fällen bestehende Informationspflicht hingewiesen.¹²⁶ Diese obliegt der übermittelnden Stelle u. a. gegenüber der Datenschutzaufsichtsbehörde und der betroffenen Person, wenn besondere Arten personenbezogener Daten unrechtmäßig übermittelt wurden. Das LAGeSo hat uns gegenüber versichert, dass die komplette Akte des Petenten beim Sozialgericht bereinigt worden ist.

Werden bei einem Sozialleistungsträger gespeicherte Gesundheits- und Sozialdaten unrechtmäßig übermittelt, ist er verpflichtet, die zuständige Datenschutzaufsichtsbehörde und die betroffene Person darüber zu informieren.

125 § 26 Abs. 2 BlnDSG

126 § 83a Satz 1 SGB X

9 Gesundheitswesen

9.1 Neue Hygieneverordnung

Im Rahmen der Novellierung des Bundesinfektionsschutzgesetzes im August 2011 wurden die Bundesländer verpflichtet,¹²⁷ bis 31. März 2012 für Krankenhäuser, Einrichtungen für ambulantes Operieren u. a. die erforderlichen Maßnahmen zur Verhütung, Erkennung, Erfassung und Bekämpfung von nosokomialen Infektionen und Krankheitserregern mit Resistenzen zu regeln. Ende Juni ist die Verordnung der Senatsverwaltung für Gesundheit und Soziales zur Regelung der Hygiene in medizinischen Einrichtungen (Hygieneverordnung)¹²⁸ in Kraft getreten. Wir hatten die Erarbeitung der Verordnung im Rahmen eines konstruktiven Austauschs mit der Senatsverwaltung begleitet.

Die neue Verordnung erlaubt u. a. die Weitergabe von Informationen an aufnehmende Einrichtungen und niedergelassene Ärztinnen und Ärzte, wenn bei den Patienten eine entsprechende Infektion festgestellt worden ist. Eine Einwilligung der Patienten ist dafür nicht erforderlich. Wir konnten aber erreichen, dass eine Informationspflicht ihnen gegenüber in die Regelung aufgenommen wurde.

Nach dem Inkrafttreten der Verordnung wurde öffentlich diskutiert, ob die medizinischen Einrichtungen und insbesondere Krankenhäuser zu mehr Transparenz im Umgang mit resistenten Keimen verpflichtet werden sollen. Wir haben eine entsprechende Forderung der Patientenbeauftragten des Senats gegenüber dem Senator für Gesundheit und Soziales unterstützt und darauf hingewiesen, dass in die Hygieneverordnung eine solche Pflicht aufgenommen werden sollte. Der Senator will die weitere Entwicklung abwarten. Einige Kliniken haben sich bereits dazu entschlossen, die Daten aus ihren Häusern öffentlich zugänglich zu machen. Die Konferenz der Informationsfreiheits-

127 § 23 Abs. 8 IfSG

128 GVBl. 2012, S. 215

beauftragten hat sich ebenfalls dafür und insbesondere für bundesweit einheitliche Hygienestandards ausgesprochen.¹²⁹

Im Sinne des Patientenschutzes ist mit der Hygieneverordnung ein erster wichtiger Durchbruch gelungen. Der überwiegende Teil unserer Hinweise zum Patientendatenschutz wurde berücksichtigt. Eine Pflicht zur Veröffentlichung von Hygienedaten für die medizinischen Einrichtungen würde darüber hinaus zu mehr Transparenz im Gesundheitswesen und zu einem erhöhten Schutz der Patienten führen.

9.2 Ungesicherte Datenbaustellen in der Zentralen Stelle nach Kinderschutzgesetz

Zwei Jahre nach Inkrafttreten des Berliner Kinderschutzgesetzes¹³⁰ haben wir die Abläufe in der bei der Charité eingerichteten Zentralen Stelle geprüft.

Die Zentrale Stelle hat die Aufgabe, das Einladungswesen zu den freiwilligen Vorsorgeuntersuchungen für Kinder durchzuführen. Sie erhält vorher die jeweiligen Meldedaten der in Berlin wohnenden Kinder und gleicht sie mit den von den Kinderärztinnen und -ärzten übersandten Rückmeldungen über durchgeführte Untersuchungen ab. Sie erinnert die Eltern, wenn diese die Vorsorgeuntersuchungen nicht rechtzeitig wahrnehmen. Ist für eine Familie der Untersuchungszeitraum verstrichen und keine Meldung einer Kinderärztin oder eines -arztes eingegangen, informiert die Zentrale Stelle den Kinder- und Jugendgesundheitsdienst, damit er der betroffenen Familie einen Hausbesuch anbieten kann.

Der Fokus unserer Prüfung lag auf der technischen Sicherung der umfangreichen (auch sensitiven) Datenbestände und auf der rechtzeitigen Löschung der genutzten Daten, wenn sie nicht mehr benötigt werden. Wir mussten feststel-

129 Entschließung vom 27. November 2012: Mehr Transparenz bei Krankenhaushygienedaten, siehe Dokumentenband 2012, S. 187; siehe auch 18.1

130 Siehe JB 2009, 7.1.2

len, dass elementare Maßnahmen des technischen Datenschutzes nicht getroffen, Daten weit verstreut auch außerhalb der hierfür vorgesehenen Datenbanken gespeichert und nicht gelöscht wurden. Zusätzlich verkompliziert wurde das Bild durch die Vermengung von Tätigkeiten einzelner Beschäftigter der Zentralen Stelle mit der Erledigung anderer Aufgaben für die Charité, bei der die Zentrale Stelle eingerichtet ist. In den Gesprächen mit der Zentralen Stelle und der Senatsverwaltung für Gesundheit und Soziales konnten wir erreichen, dass notwendige Maßnahmen ergriffen wurden: Die Zentrale Stelle hat ihre Prozesse überarbeitet, technische Maßnahmen nachgeholt und ein Löschkonzept entwickelt.

Bei der Errichtung neuer Stellen bedarf es einer sorgfältigen Planung der Prozesse und Vorgehensweisen unter Berücksichtigung des Datenschutzes. Der Leitung dieser Stellen und der Fachaufsicht obliegt es, den Belangen der Menschen auch in Bezug auf den Schutz ihrer Daten ausreichendes Gewicht zu verleihen. Es bleibt die im Kinderschutzgesetz vorgesehene Evaluation der Arbeit der Zentralen Stelle 2013 abzuwarten.

9.3 Termin versäumt – Kinderärztin informiert das Gesundheitsamt

Eine Bürgerin hat sich bei uns darüber beschwert, dass die Kinderärztin ihrer Tochter, ohne sie zuvor darüber zu informieren, den Kinder- und Jugendgesundheitsdienst im Gesundheitsamt Neukölln hinsichtlich eines verpassten Termins benachrichtigt habe. Nach unseren Feststellungen kam es zu der Datenübermittlung, weil der Dienst zuvor an die Kinderärztin herantreten war und sie aufgefordert hatte, ihn zu informieren, falls die Kinderärztin Auffälligkeiten hinsichtlich des Pflegezustands oder der Einhaltung von Arztterminen feststellen würde. Der Kinder- und Jugendgesundheitsdienst hatte sich zu dieser Maßnahme entschlossen, da die Familie des Kindes keine Bereitschaft signalisiert habe, Hilfe durch den Dienst anzunehmen.

Sowohl das Herantreten des Kinder- und Jugendgesundheitsdienstes an die Ärztin als auch die Meldung des versäumten Termins durch die Ärztin an diesen Dienst waren unzulässig, da beides ohne das Wissen und Einverständnis der Mutter und ohne Rechtsgrundlage erfolgt war.

Nicht nachvollziehbar ist, warum der Dienst darauf verzichtet hat, die Eltern zumindest vorab darüber zu informieren, dass er ggf. auch gegen ihren Willen Kontakt zur Kinderärztin aufnehmen wird. Dies gebietet das im Datenschutzrecht geltende Transparenzgebot, nach dem die Betroffenen möglichst zu jeder Zeit wissen sollen, was mit den über sie gespeicherten Informationen geschieht. Lediglich in eng begrenzten Ausnahmefällen, in denen der Schutz des Kindes durch die Information in Frage gestellt wird, ist auf die vorherige Information zu verzichten. Im vorliegenden Fall hat sich jedoch gezeigt, dass die Familie später zur Mitwirkung bereit war und die angebotenen Hilfen angenommen hat, nachdem ein erneutes erläuterndes Gespräch stattgefunden hat. Insofern hätten die Eltern auch bereits im Vorhinein informiert werden können und müssen.

Außerdem ist es im Rahmen einer Kontaktaufnahme durch den Kinder- und Jugendgesundheitsdienst sinnvoll, die Ärztinnen und Ärzte darauf hinzuweisen, dass diese selbstverantwortlich über eine solche Datenweitergabe entscheiden müssen und dass nicht bereits die Anfrage einer öffentlichen Stelle eine Offenbarungsbefugnis darstellt. Vor dem Hintergrund größtmöglicher Transparenz für die Betroffenen und zur Aufrechterhaltung der Vertrauensbeziehung zwischen Arzt und Patient ist es ohnehin empfehlenswert, die Eltern um eine Schweigepflichtentbindungserklärung zu bitten. Sollten diese dazu nicht bereit sein, muss auch hier zumindest eine Information der Eltern über die geplante Datenweitergabe erfolgen. Dies gilt nicht, wenn diese Information aufgrund der Kindeswohlgefährdung den wirksamen Schutz des Kindes in Frage stellen würde. Das wäre jedoch sorgfältig zu prüfen und nur im Ausnahmefall zulässig.

Wir haben diesbezüglich gegenüber dem Gesundheitsamt einen Mangel festgestellt. Es hat sich unserer Rechtsauffassung angeschlossen und in einem Rundschreiben den in Neukölln niedergelassenen Kinderärztinnen und -ärzten die rechtlichen Grundlagen für eine Datenübermittlung an das Gesundheitsamt und das Jugendamt erläutert.

Soweit Kinderärztinnen und -ärzte im Einzelfall Anhaltspunkte für eine konkrete Kindeswohlgefährdung haben, müssen sie eine verantwortungsbewusste Abwägung im Hinblick auf die Offenbarung von Patientendaten vornehmen. Ohne Einwilligung der Sorgeberechtigten kann eine solche Offenbarung nur erfolgen, wenn in dem jeweiligen Einzelfall tatsächliche Anhaltspunkte für eine konkrete Kindeswohlgefährdung vorliegen und diese nicht anders als durch die Datenübermittlung abzuwenden ist.

9.4 Pseudonymisierung in der klinischen Krebsregistrierung

Das Tumorzentrum Berlin e.V. wertet Daten über die Erkrankung und die Behandlung von Krebspatienten in Krankenhäusern aus, um zur Qualität der Behandlung beizutragen. Wir haben den Verein bei der Anpassung seiner Prozesse an den Rechtsrahmen des geänderten Landeskrankenhausesgesetzes (LKG)¹³¹ unterstützt.

Berliner Krankenhäuser sammeln Daten über die Erkrankungen und die Behandlung von Krebspatienten in fünf sog. klinischen Tumorzentren. Die dort geführte Tumordokumentation bietet eine Grundlage für die Steuerung und Beurteilung der Behandlung. In diese Dokumentation gehen auch bereits Daten von Patienten ein, denen noch nicht eröffnet wurde, dass sie an Krebs erkrankt sind, und die demzufolge hierzu keine Einwilligung erteilen können. Das LKG gestattet dies genauso wie eine landesweite Zusammenführung dieser Daten, soweit es der Sicherung der Qualität der Behandlung oder der Forschung dient. Voraussetzung für eine institutionsübergreifende Speicherung ist jedoch, dass Angaben über die Identität der Patienten durch Kennnummern (Pseudonyme) ersetzt werden.

Wir haben das Tumorzentrum Berlin beraten, wie die Kennnummern so gebildet werden können, dass sie die Zusammenführung von Daten aus verschiedenen Krankenhäusern und damit eine Gesamtschau auf die Behandlung eines Patienten erlaubt, auch wenn er, wie es nicht selten geschieht, in mehreren

131 JB 2011, 2.2.2

Krankenhäusern behandelt wurde. Mit der Bildung der Kennnummern dürfen die Krankenhäuser auch eine gemeinsame Vertrauensstelle beauftragen, solange diese selbst bei einem Krankenhaus eingerichtet ist.

Um die Qualität einer Behandlung zu beurteilen, braucht der Beurteilende die Identität des Patienten nicht zu kennen. Rückmeldungen an die behandelnden Stellen sind über einheitlich vergebene Kennnummern möglich.

9.5 Das Endoprothesenregister Deutschland

Das bundesweite Endoprothesenregister sammelt auf freiwilliger Basis Daten über implantierte Endoprothesen, um Qualitätsproblemen auf die Spur zu kommen und bei Schwachstellen die Patienten zu informieren.

Vielfach publizierte Probleme mit Endoprothesen, wie z. B. künstlichen Hüftgelenken, haben die Aufmerksamkeit auf eine wirksame Kontrolle der Qualität dieser Medizinprodukte gelenkt. Um Erkenntnisse über Faktoren zu gewinnen, welche die Qualität beeinflussen, sammelt das Endoprothesenregister Deutschland (EPRD) Daten über die implantierten Prothesen, ihre Haltbarkeit und ggf. Auswechslung. Die Ärztinnen und Ärzte der am Register beteiligten Kliniken bitten ihre Patienten hierzu um ihr Einverständnis. Die Patienten tragen die Prothesen über einen langen Zeitraum. Um eine langfristig konsistente Akte über die Prothesen führen und bei Bedarf die Patienten kontaktieren zu können, ohne selbst identifizierende Angaben über die Patienten speichern und aktuell halten zu müssen, kooperiert das EPRD mit einer großen Zahl von Orts- und Ersatzkrankenkassen.

Wir haben das EPRD dabei beraten, seine Prozesse so zu gestalten, dass jede beteiligte Institution genau die Informationen vorhält, die es für ihre Rolle benötigt. So lässt sich aus den Daten des Registers nicht ersehen, welche Personen die Prothesen tragen. Die Krankenkassen wiederum wissen um die Teilnahme einer versicherten Person an dem Register, erhalten jedoch darüber hinaus keine neuen Daten. Ein mehrstufiger Ersatz der Versichertennummern durch andere Kennzeichen sorgt für eine Trennung der Datenbestände.

Dennoch können behandelnde Ärztinnen und Ärzte mit Einverständnis ihrer Patienten jederzeit und kurzfristig Daten über die getragenen Prothesen erhalten und Informationen, z. B. über Wechseloperationen, zurück an das Register melden. Rückmeldungen über Schwachstellen der Prothesen erreichen die Patienten. Das Register kann seine Daten auf Auffälligkeiten analysieren und anonymisierte Daten, bei denen jedwede Hinweise auf die betroffenen Patienten gestrichen wurden, der Forschung und den Herstellern zur Verfügung stellen.

Frühzeitige Planung und Einbeziehung der Datenschutzaufsichtsbehörden ermöglicht es, auch bei Verfahren mit einer großen Zahl von beteiligten Stellen datensparsame Gestaltungsmöglichkeiten zu finden, welche die Interessen der Patienten wahren und die gesetzten Ziele erreichen.

9.6 Was kann eine Protokollierung der Datenzugriffe in Krankenhäusern leisten?

Für Krankenhäuser ist es schwierig, nur den Beschäftigten den Zugriff auf die Daten eines Patienten zu gewähren, die konkret an der Behandlung teilnehmen oder mit der Abrechnung befasst sind. Kann die Protokollierung aller oder eines Teils dieser Zugriffe dieses Defizit auffangen? Wir prüften zwei große Krankenhäuser (die Charité Universitätsmedizin sowie die Vivantes Netzwerk für Gesundheit GmbH) auf der Grundlage der 2011 beschlossenen Orientierungshilfe Krankenhausinformationssysteme¹³².

Wer sich in einem Krankenhaus behandeln lässt, weiß, dass sich viele Beschäftigte um einen kümmern: Von der Patientenaufnahme über die Pflegekräfte und Ärzte, auf Station und Fachabteilung bis hin zu Laborassistenten, Physiotherapeuten und dem Sozialdienst. Im Hintergrund erfolgen Beratungen, werden Diagnosen und Prozeduren für die Abrechnung mit den Kassen und Versicherungen codiert und Rechnungen erstellt. Für all dies wird der Zugang zu elektronisch geführten Daten über die Kranken benötigt.

132 JB 2011, 7.2.1

Für einige dieser Beschäftigten ist der Kontakt mit einem Patienten gut planbar, und es lassen sich im Voraus die erforderlichen Zugriffsrechte einstellen; andere treten spontan hinzu, sei es, dass wegen Ausfalls einer oder eines Beschäftigten jemand anderes einspringen muss, sei es, dass sofortiges Handeln notwendig ist, weil sich der Zustand der oder des Kranken verschlechtert.

Daher sehen Krankenhausinformationssysteme vielfach vor, dass einigen Beschäftigtengruppen das Recht erteilt wird, die ihnen gewöhnlich auferlegten Zugriffsschranken zu überschreiten. In diesem Fall müssen sie ihr Tun in der elektronischen Akte begründen. Manche Krankenhäuser wie die Charité fassen dagegen schon die regulären Berechtigungen so weit, dass mehr als zehnmal so viele Beschäftigte Zugriffsmöglichkeiten haben, als sie tatsächlich benötigen. Da in beiden Konstellationen das Tor zu Daten einer großen Zahl von Patienten auch dort offen steht, wo ihre Kenntnis nicht benötigt wird, muss Missbrauch festgestellt und sanktioniert werden.

In einem konkreten Verdachtsfall gelang es Vivantes, auf unsere Anforderung hin durch Auswertung der Protokolle einen mutmaßlich unberechtigten Zugriff zu ermitteln. In der Charité mussten wir hingegen feststellen, dass die Protokollierung monatelang ausgefallen war, ohne dass jemand davon Notiz genommen hatte.

Wir haben die Charité daraufhin aufgefordert, die Zugriffsprotokollierung nachhaltig sicherzustellen und ein Konzept zu entwickeln, wie die Protokolle anlassbezogen, aber auch stichprobenhaft ohne Anlass durchzusehen sind. Dennoch können damit die Defizite zu laxer Zugriffsschranken nicht vollständig aufgefangen werden. Die Datenmenge in den Protokollen ist einfach zu groß, und effiziente Werkzeuge zu ihrer Auswertung sind nicht verfügbar.

Zugriffsprotokolle sind – wenn sie ordnungsgemäß geführt werden – eine gute Grundlage, Missbrauch der elektronischen Patientenunterlagen nachzuvollziehen. Angesichts ihres Umfangs und des mit einer anlasslosen Auswertung verbundenen Aufwands wirken die Protokolle jedoch kaum präventiv. Angemessene Zugriffskonzepte werden durch sie nicht entbehrlich.

9.7 Tablet-Computer in der medizinischen Behandlung durch die Charité

Presseberichten entnehmen wir, dass die Charité Tablet-Computer einsetzt, um einigen ihrer Ärztinnen und Ärzte den mobilen Zugriff auf Patientendaten zu gewähren. Wir prüften, ob hierbei die Vertraulichkeit der Daten gewährleistet bleibt.

Ärztinnen und Ärzte sind in ihren Kliniken viel unterwegs und in die Behandlung einer großen Zahl von Kranken eingebunden. Die Arbeit – etwa bei der Visite am Krankenbett – kann durch einen mobilen unkomplizierten Zugriff auf die elektronischen Patientenunterlagen erleichtert werden. Leichte und funktionsstarke Tablet-Computer oder Smartphones bieten hierfür eine mögliche Plattform. Diese Mobilität birgt jedoch auch Risiken. Die Geräte können abhandenkommen, oder sie werden in Umgebungen eingesetzt, für die sie nicht vorgesehen sind. Ein großes Problem stellt das mangelhafte Sicherheitsbewusstsein sowohl der Hersteller als auch vieler Nutzer der Geräte dar.

Der erstgenannten Gefahr begegnet die Charité damit, dass Daten in der Regel nicht auf den Geräten gespeichert werden. Durchbrochen wird diese Regel allerdings bei Bilddaten, etwa Röntgenbildern. Die Datenwege werden durch die Charité gut gesichert. Die Server stehen in einer besonders geschützten Zone. Die Tablets werden durch eine Managementsoftware überwacht und eine Konfiguration durchgesetzt, die ein Mindestmaß an Schutz bietet.

Dagegen werden Gefahren von Schadsoftware völlig ignoriert. Die Nutzenden dürfen beliebige Apps auf den Tablets installieren. Dass auch bösartige Apps ihren Weg in die App-Stores finden, hat die Erfahrung gelehrt. Greift die Nutzerin oder der Nutzer mit dem Gerät auf dem Campus der Charité auf das Internet zu, wird der Datenverkehr auf Bedrohungen gefiltert. Wir wissen nicht, wie effektiv das geschieht. Die Geräte können jedoch auch außerhalb der Charité benutzt werden und unter die Kontrolle Dritter gelangen.

Für die Geräte ist eine lange Liste von Schwachstellen publiziert. So gibt es öffentlich bekannte Wege, den Kennwortschutz der Geräte zu umgehen. Die Schwachstellen waren der Charité, in der niemand für Informationssicherheit

verantwortlich zeichnet und ein Informationssicherheitsmanagement nicht eingeführt ist, nicht bekannt. Genauso wenig bekannt schienen die Konsequenzen, die eine Kompromittierung der Geräte haben kann: Wer die Kontrolle über das Gerät erlangt, hat auch Zugang zu Informationen, die die Tür zu den Patientenunterlagen wenigstens der Klinik vollständig öffnen, in der die Geräte zum Einsatz kommen. Bei einem generellen Einsatz in der Charité wären alle Patienten potentiell betroffen.

Wir haben die Charité aufgefordert, die Verwendung der Tablet-Computer solange einzustellen, bis eine sichere Konfiguration vorgenommen und die Software auf einen Stand gebracht wurde, für den zumindest keine Schwachstellen bekannt sind. Risikobehaftete private Nutzung muss unterbunden und der Zugriff auf das Internet so gestaltet werden, dass die Software des Gerätes nur mit sicheren Inhalten in Berührung kommen kann.

Die Einführung von Tablet-Computern und Smartphones in den Behandlungsalltag eines Krankenhauses bedarf sorgfältiger Planung unter Einbeziehung von Expertise in Informationssicherheit und Datenschutz. Derzeit unumgänglich ist eine Einschränkung der Funktionalität der Geräte auf einen eng umschriebenen ausschließlich dienstlichen Zweck.

9.8 Laxer Umgang mit sensiblen Schreiben im Gesundheitsamt Steglitz-Zehlendorf

Aufgrund einer Eingabe kontrollierten wir die Datenspeicherung in der Beratungsstelle für behinderte Menschen, Krebs- und AIDS-Kranke des Gesundheitsamtes Steglitz-Zehlendorf.

Die Eingabe richtete sich gegen eine Anweisung, Angaben, die zur Speicherung in einer geschützten Datenbank vorgesehen waren, zusätzlich auf allgemeinen Dateiservern des Gesundheitsamtes abzulegen. Diese Angaben sind in elektronischen Kopien von Schreiben der Beschäftigten enthalten, beziehen sich auf die Klienten der Beratungsstelle und sind daher als besonders schutzwürdig einzuordnen. Soweit sie im Zusammenhang mit der ärztlichen Tätigkeit von

Beschäftigten der Beratungsstelle stehen, unterliegen sie zudem der ärztlichen Schweigepflicht.

Unsere Prüfung ergab, dass jedes Schreiben allen Mitarbeiterinnen und Mitarbeitern der Beratungsstelle zugänglich war, unabhängig davon, ob sie in den jeweiligen Vorgang eingebunden waren oder nicht. Keine Person in der IT-Stelle des Bezirksamtes war technisch daran gehindert, die Daten einzusehen. Es ließ sich nicht nachvollziehen, wann wer die Texte eingesehen hatte. Auch eine nachträgliche Verfälschung der Texte wäre nur bei Vergleich mit der Papierkopie aufgefallen. Schließlich bedurfte es nur eines Mausklicks, ein Schreiben versehentlich oder absichtlich an andere (unberechtigte) Beschäftigte des Gesundheitsamtes weiterzugeben, ohne dass dies später hätte nachgewiesen werden können.

Wir haben diesen laxen Umgang mit sensiblen Daten bemängelt und die Beratungsstelle aufgefordert, entweder den Schutz der Schreiben an das Niveau anzupassen, das für die in der Datenbank erfassten Daten gilt, oder deren Speicherung zu beenden.

Alle Behörden haben die Daten, die ihnen von hilfesuchenden Menschen anvertraut werden, vor unberechtigter Kenntnisnahme zu schützen, gleich in welcher Form sie gespeichert werden. So muss eine Verschlüsselung auch alle Ablageorte der Daten erfassen. Schreiben mit sensitivem Inhalt gehören nicht in eine allgemeine Dateiablage, sondern in ein Dokumentenmanagementsystem, mit dem der Zugang gesteuert sowie die Erstellung und Einsichtnahme nachvollzogen werden können.

10 Beschäftigtendatenschutz

10.1 Private Nutzung von Internet und E-Mail

Ein Beschäftigter beschwerte sich darüber, dass sein Arbeitgeber ihn wegen unerlaubter Nutzung seines Internetzugangs zu privaten Zwecken abgemahnt habe. Der Arbeitgeber verwies auf eine Dienstvereinbarung, die eine Speicherung der Nutzerdaten unter Pseudonym und bei begründetem Verdacht eine namentliche Auswertung vorsah, und auf sein Recht, die Einhaltung des Verbots der privaten Nutzung von Internet und E-Mail kontrollieren zu dürfen.

Die vollständige Protokollierung des Nutzerverhaltens stellt eine unzulässige Vollkontrolle der Beschäftigten dar.¹³³ Betriebs- und Dienstvereinbarungen dürfen nicht den Schutz des Bundesdatenschutzgesetzes umgehen.

Die Protokollierung anonymisierter Daten externer E-Mail-Domänen und aufgerufener Internetdomänen ist dagegen zulässig. Dabei dürfen die erstellten Protokolle zunächst ausschließlich für Zwecke der Betriebssicherheit gespeichert werden. Das Protokoll kann im Rahmen einer Domäneanalyse der Systemadministration als statistische Aufbereitung der protokollierten anonymen Kontrolldaten monatlich oder aus gegebenem Anlass gesichtet und ausgewertet werden. Zeigt sich bei diesen Auswertungen, dass eine nicht mehr tolerierbare Häufung offensichtlich privater oder unzulässiger IT-Nutzung vorliegt, kann als Stichprobenkontrolle ab dem Zeitpunkt der Feststellung und für die betreffenden Domänen für eine bestimmte, angemessene Dauer pseudonymisiert protokolliert werden. Bestätigen sich die Auffälligkeiten, kann eine Nutzeranalyse stattfinden. Dazu kann eine statistische Aufbereitung der protokollierten Kontrolldaten angefertigt werden, in der für die betreffenden Domänen und im Zeitraum der Protokollierung die Anzahl der Anrufe bzw. Übertragungsvolumina der pseudonymisierten Nutzenden dargestellt wird. Bevor die Kontrolldaten für die letzte Stufe der personenbezogenen Prüfung herangezogen werden, ist eine Verhältnismä-

133 § 32 BDSG

ßigkeitsprüfung durchzuführen. So kann z. B. schwerwiegendes vertragswidriges Verhalten oder der Verdacht einer Straftat oder eines Gesetzesverstößes weitere Überprüfungsmaßnahmen rechtfertigen. Erst danach ist eine Entpseudonymisierung (Herstellung des direkten Personenbezugs) zulässig. Im Anschluss an diese Maßnahmen sind die personenbezogenen Kontrolldaten unverzüglich zu löschen, sofern sie nicht aus Beweissicherungsgründen für etwaige Gerichtsprozesse erforderlich sind. Die Betroffenen sind möglichst frühzeitig anzuhören und auch im Nachhinein über die durchgeführten Maßnahmen zu benachrichtigen.

Nutzerdaten sind Personaldaten, deren Erhebung und Nutzung dem Erforderlichkeitsgebot unterliegen. Der Arbeitgeber darf deshalb bei der Kontrolle privater Internet-Nutzung durch Beschäftigte einen Personenbezug erst nach einer stufenweisen Ausschöpfung anderer Kontrollmöglichkeiten herstellen.

10.2 Dienstvereinbarung zur Telearbeit im Land Berlin

Die Senatsverwaltung für Inneres und Sport plant den Abschluss einer Dienstvereinbarung über die Durchführung alternierender Telearbeit im Land Berlin (DV Telearbeit). Ziel ist die Schaffung einheitlicher Rahmenbedingungen für die Nutzung dieser Arbeitsform. Neben der persönlichen Eignung der Beschäftigten soll eine Teilnahme an Telearbeit nur dann möglich sein, wenn das Arbeitsgebiet für einen bestimmten Mindestzeitraum (also nicht nur vorübergehend) die Wahrnehmung eines Teils der Aufgaben außerhalb des Dienstgebäudes zulässt.

Wir haben darauf hingewiesen, dass es Aufgaben gibt, die grundsätzlich nicht in Telearbeit erledigt werden sollten. Insbesondere gilt das für jede Art der Verarbeitung sensibler Daten. Dies sollte explizit in die Dienstvereinbarung aufgenommen werden. Auch Tätigkeiten von Berufs- und Amtsgeheimnisträgern sind für Telearbeit ungeeignet. Die Entscheidung über die Zulässigkeit der Teilnahme an Telearbeit sollte anders als im Entwurf vorgesehen nicht nur der Führungskraft überlassen werden.

Zusätzlich ist die persönliche Situation der Telearbeit-Beteiligten zu berücksichtigen. Entscheidungsrelevant kann dabei z. B. sein, ob die Telearbeit in einem Mehrpersonenhaushalt erbracht werden soll, ein separater Arbeitsraum zur Verfügung steht oder abschließbare Schränke vorhanden sind. Eine Prüfung der Räumlichkeiten vor der Genehmigung der Telearbeit ist angezeigt. Die oder der jeweilige behördliche Datenschutzbeauftragte ist bei grundsätzlichen Festlegungen und konkreten Ausgestaltungen der IT-Ausstattung zu beteiligen.

Telearbeit ist nur möglich, wenn der Schutz der personenbezogenen Daten – insbesondere die Datensicherheit – gewährleistet ist.

10.3 Datenerhebung im Rahmen von Präqualifikationsverfahren

Aus der Praxis

Der Geschäftsführer eines Unternehmens wandte sich an uns mit dem Hinweis, die Deutsche Bahn (DB) habe im Rahmen eines sog. Präqualifikationsverfahrens für die Durchführung von Maschinenleistungen für die DB von dem Unternehmen gefordert, an sie personenbezogene Daten von Beschäftigten zu übermitteln, die bei der Bedienung dieser Maschinen eingesetzt werden sollen. Bei diesen Daten handelte es sich um Namen, Adressen, Geburtsdaten sowie um Nachweise der jeweiligen Qualifikation.

Wir haben die DB darauf hingewiesen, dass die Erhebung und Übermittlung der Personaldaten gegen das Erforderlichkeitsgebot verstoßen, da zunächst eine Übermittlung pseudonymisierter Daten der Beschäftigten ausreichend gewesen wäre. Bei den Nachweisen und Referenzbelegen werden künftig statt Klarnamen lediglich Pseudonyme verwendet. Anhand dieser Angaben erfolgt die Prüfung der notwendigen Fachkunde und technischen Leistungsfähigkeit sowie der Mindestanforderungen zur Vorauswahl von fachlich geeigneten und leistungsfähigen Auftragnehmern. Nur in definierten Ausnahmefällen oder falls aufgrund von ersichtlichen Ungereimtheiten oder Angaben Zweifel daran bestehen, ob die Eigenerklärung oder Nachweise korrekt und aktuell sind, werden im Rahmen von Stichproben die Bewerber um die Vorlage von Kopien der Originaldokumente gebeten.

Im Präqualifikationsverfahren für einen Auftrag werden grundsätzlich nur pseudonyme Daten von Beschäftigten des Unternehmens benötigt, das sich um den Auftrag bewirbt.

10.4 Erhebung und Speicherung von Beschäftigtendaten zum Schutz des Urheberrechts?

Die Betreiberin eines Stadtplandienstes verpflichtete die Beschäftigten eines von ihr mit der Erstellung von Stadtplänen beauftragten Unternehmens, ihre persönlichen Arbeitszeiten auf einer Anwendung einzutragen, die in Realzeit bei der Betreiberin des Stadtplandienstes eingesehen und dort gespeichert wurden. Dazu legte die Arbeitgeberin den Beschäftigten eine sog. datenschutzrechtliche Erklärung vor, in der sie sich damit einverstanden erklärten, dass ihre Einträge in die Datenbank online und offline von der Betreiberin personenbezogen mit vollem Namen und jederzeit eingesehen werden können und dauerhaft (mindestens 70 Jahre) zu Dokumentationszwecken gespeichert werden.

Das Unternehmen begründete die Datenerhebung damit, in einem möglichen Gerichtsverfahren über urheberrechtliche Ansprüche den Rechteinhabern lückenlos den Herstellungsvorgang und die dafür eingesetzten Personen, Daten, Uhrzeiten und Bearbeitungsschritte in Bezug auf die Stadtpläne nachweisen zu müssen. Die entsprechenden Personaldaten müssten deshalb 70 Jahre gespeichert bleiben.

Eine wirksame Einwilligung der Beschäftigten der Auftragnehmerin in die Datenspeicherung lag nicht vor, da es wegen der sozialen Abhängigkeit von Beschäftigten grundsätzlich an der Freiwilligkeit mangelt. Die Erhebung und Speicherung der Beschäftigtendaten kann auch nicht auf eine Rechtsvorschrift gestützt werden. Zwar fordern die Gerichte für den Nachweis der Aktivlegitimation von urheberrechtlichen Ansprüchen regelmäßig die Darlegung der lückenlosen Rechteübertragung. Hierfür ist jedoch die Vorlage der vertraglichen Vereinbarung mit Dritten zur Rechteübertragung als Urkundenbeweis ausreichend. Die Rechtsprechung verlangt keinen Nachweis bis hinein in die

Ebene des Herstellungsprozesses. Welche oder welcher Beschäftigte der Auftraggeberin oder eines in ihrem Auftrag handelnden Unternehmens den jeweiligen Kartenausschnitt erstellt hat, spielt deshalb keine Rolle. Es fehlte also an der Erforderlichkeit der Datenverarbeitung.

Es gibt keine urheberrechtlichen Gründe, Beschäftigtendaten 70 Jahre lang aufzubewahren.

11 Wohnen und Umwelt

11.1 Orientierungshilfe Smart Metering – Datenschutz bei intelligenten Stromzählern

Intelligente Energienetze und -zähler (Smart Grids, Smart Meter) sind eine wichtige Voraussetzung für eine ressourcenschonende, umweltfreundliche und effiziente Produktion, Verteilung und Nutzung von Energie. Sie ermöglichen, eine nachhaltige Energieversorgung sicherzustellen. Verbrauchende können mit den intelligenten Zählern ihren Verbrauch regulieren und kontrollieren. Dafür zeichnen Smart Meter detaillierte Verbrauchsdaten auf und ermöglichen eine Übermittlung dieser Daten an externe Marktteilnehmer. Durch eine langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff können sich massive Verletzungen der Privatsphäre der Betroffenen ergeben.¹³⁴

Die Datenschutzbehörden des Bundes und der Länder haben daher eine Orientierungshilfe beschlossen, die Empfehlungen zum datenschutzgerechten Betrieb der neuen intelligenten Zähler gibt.¹³⁵ Mithilfe von Anwendungsfällen werden die einzelnen Datenverarbeitungsprozesse beim Smart Metering beschrieben und bewertet, vom Messen der Strommengen über die Verarbeitung im Zähler bis zur weiteren Nutzung für die Energielieferung und -abrechnung. Die Orientierungshilfe erläutert, wie die zentralen Datenschutzforderungen berücksichtigt werden können, und gibt Hilfestellung zur datenschutzgerechten Konzeption der Geräte. Insbesondere darf eine Verarbeitung der Smart-Meter-Daten nur erfolgen, soweit es für die gesetzlich vorgesehenen Zwecke erforderlich ist.¹³⁶ Alle weiteren Funktionen dürfen nur mit Einwilligung der Betroffenen eingesetzt werden. Smart-Meter-Daten sollen mög-

134 Siehe JB 2009, 1.1.1; JB 2011, 7.4.1

135 Siehe Dokumentenband 2012, S. 16; die Orientierungshilfe selbst ist abrufbar unter http://www.datenschutz-berlin.de/attachments/884/OH_SmartMeter.pdf?1340888359

136 Mit der Novellierung des Energiewirtschaftsgesetzes (EnWG) wurde ein Rechtsrahmen für die Einführung von Smart Metern geschaffen. § 21g Abs. 1 Nr. 1 bis Nr. 8 EnWG führt abschließend die Zwecke auf, für die eine Verarbeitung erfolgen darf.

lichst anonymisiert, pseudonymisiert oder aggregiert und an möglichst wenige Stellen übermittelt werden. Die Ablesintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verbrauchsverhalten gezogen werden können. Die Betroffenen sollen Zugriffe auf das Smart Meter erkennen und im Zweifel unterbinden können. Das entspricht den Vorgaben des Berliner Datenschutzgesetzes für das Fernmessen.¹³⁷ Für den berechtigten Zugang zu den Zählern sind eindeutige Profile zu definieren.

Um die Privatsphäre der Verbrauchenden zu wahren, ihnen die Souveränität über ihre Daten zu sichern und die Möglichkeit zur Intervention zu geben, müssen die gesetzlichen Regelungen konkretisiert und detaillierter ausgestaltet werden. Daneben sind umfangreiche technische und organisatorische Maßnahmen notwendig.

11.2 Berliner Mietspiegel

Im Endbericht zum Berliner Mietspiegel wurden regelmäßig Informationen über eingereichte Änderungswünsche bezüglich der Wohnlagen, die im vorherigen Mietspiegel ausgewiesen wurden, und die Ergebnisse der daraufhin durchgeführten Wohnlagenüberprüfungen veröffentlicht. Die Veröffentlichung der Informationen sollte den Prozess der Wohnlagenüberprüfung transparent gestalten.

Angaben, die unter Bezugnahme auf eine hausnummerngenaue Anschrift veröffentlicht werden, können zumindest dem Grundstückseigentümer zugeordnet werden und sind daher personenbezogene Daten. Die Bewertung der Wohnlagen im Berliner Mietspiegel ist maßgeblich für die Höhe der ortsüblichen Vergleichsmiete. Soweit in dem Endbericht nur eine Anschrift zu einem Änderungswunsch angegeben und die Wunschwohnlage höher ist als die bisherige Wohnlage, kann daher mit relativer Sicherheit davon ausgegangen werden, dass die Vermieterin oder der Vermieter den Antrag gestellt hat. Wenn hingegen die Wunschwohnlage niedriger ist als die bisherige Wohnlage, kann ange-

137 § 31 a BlnDSG

nommen werden, dass eine Mieterin oder ein Mieter den Antrag gestellt hat. Soweit ein Objekt aus nur einem Haushalt besteht, kann somit auf die tatsächliche antragstellende Person geschlossen werden. Diese Rückschlüsse können zumindest die Personen ziehen, die mit den Wohnverhältnissen vertraut sind, insbesondere die Mietparteien. Damit sind die veröffentlichten Angaben personenbeziehbar und dürfen im Rahmen des Mietspiegels nur mit Einwilligung der Antragstellenden veröffentlicht werden.

Aufgrund unserer Hinweise wird die Senatsverwaltung für Stadtentwicklung und Umwelt die Liste mit den Änderungswünschen und den Ergebnissen der Wohnlagenüberprüfungen ab dem Mietspiegel 2013 nicht mehr veröffentlichen. Bei Interesse an den Begründungen für die Wohnlagenentscheidungen gibt die Senatsverwaltung künftig ohne Personenbezug Auskunft.

11.3 Automatisierte Datenübermittlungen – Bodenschutz ohne Datenschutz

Bereits 2009 hat uns die Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz darüber informiert, dass sie ein elektronisches Bodenbelastungskataster betreibt. Darin sind Informationen zu einzelnen Grundstücken wie die Größe und die chronologische Nutzung eines Grundstücks sowie Angaben zu Bodenbelastungen gespeichert. Daneben steht eine Karte zum Bodenbelastungskataster zur Verfügung. Zahlreiche andere Behörden wie die Senatsverwaltungen, Bezirksämter und die Polizei können auf diese Angaben zugreifen.

Dieser Zugriff erfolgt automatisiert, d. h. ohne dass jeweils Mitarbeitende darüber entscheiden, ob er zulässig ist. Daher handelt es sich um ein automatisiertes Abrufverfahren, das durch das Berliner Bodenschutzgesetz zwar grundsätzlich erlaubt ist. Sowohl dieses Gesetz als auch das Berliner Datenschutzgesetz verlangen jedoch, dass das Verfahren durch eine Rechtsverordnung geregelt wird.¹³⁸ Die Senatsverwaltung hätte darin vor Inbetriebnahme des Abrufverfahrens fest-

138 Dies folgt aus § 7 Abs. 7 BlnBodSchG und § 15 BlnDSG.

legen müssen, welche Datenempfänger zu welchem Zweck bestimmte Datenarten abrufen dürfen. Sie müsste weiterhin Maßnahmen zur Datensicherung und Kontrolle vorsehen, z. B. in Bezug auf die Protokollierung der Abrufe.

Die Bereitstellung der Daten im Bodenbelastungskataster zum automatisierten Abruf ist ohne eine solche Rechtsverordnung rechtswidrig. Sie wurde trotz unserer Hinweise noch immer nicht verabschiedet. Bereits im Mai 2011 hatten wir einen datenschutzrechtlichen Mangel festgestellt. Seitdem drängen wir weiter auf den zeitnahen Erlass der Verordnung. Seit der Neubildung des Senats Ende 2011 führt die Senatsverwaltung für Stadtentwicklung und Umwelt das Bodenbelastungskataster.

Die Senatsverwaltung für Stadtentwicklung und Umwelt betreibt in rechtswidriger Weise ein automatisiertes Verfahren zum Abruf personenbezogener Grundstücksdaten. Wenn das Verfahren weiter betrieben werden soll, ist dringend eine Rechtsverordnung zu erlassen.

11.4 Wer darf in die Bauakte schauen?

Es haben uns einige Beschwerden von Grundstückseigentümern erreicht, weil andere Personen beim Bezirksamt Einsicht in ihre Grundstücks- bzw. Bauakten erhalten hatten. Bei unserer Überprüfung hat sich gezeigt, dass bei den Bezirksämtern zum Teil Unsicherheit besteht, unter welchen Voraussetzungen die Einsicht gewährt werden kann.

Der Gesetzgeber hat an verschiedenen Stellen geregelt, wie das Recht auf Informationszugang und das Recht auf den Schutz personenbezogener Daten in Einklang gebracht werden können.¹³⁹ So finden sich im Verwaltungsverfahrensgesetz Berlin und im Berliner Informationsfreiheitsgesetz allgemeine Vorgaben, unter welchen Voraussetzungen Einsicht in Vorgänge der Verwaltung genommen werden kann, die auch persönliche Informationen enthalten. Daraus ergibt sich, dass diejenigen, die z. B. an einem Verfahren beteiligt sind, wie Nachbarn bei einer beantragten Baugenehmigung, umfassendere Einsichts-

139 Siehe dazu schon JB 1995, 5.2

rechte haben als diejenigen, die ein eher allgemeines Interesse an der Tätigkeit der Behörden haben. Für Bauakten gibt es eine spezielle Regelung, um den Besonderheiten des Baurechts und der Tätigkeit der Bauaufsichtsbehörden Rechnung zu tragen.¹⁴⁰ Bei Grundstücksakten muss die Person, die die Einsicht begehrt, ein rechtliches Interesse an der Kenntnis der Daten glaubhaft machen. Die Baubehörde muss dieses abwägen gegen die schutzwürdigen Interessen des Grundstückseigentümers. Wenn hiernach keine Einsicht gewährt werden kann und der Grundstückseigentümer nicht mit der Einsichtnahme einverstanden ist, kann gleichwohl ein Informationszugangsanspruch (Akteneinsicht oder -auskunft) nach dem IFG in Frage kommen. Dieser dürfte allerdings nicht umfassend erfüllt werden, sondern grundsätzlich nur in Bezug auf die „Kerndaten“.¹⁴¹

Baubehörden müssen bei Anträgen auf Einsichtnahme in Bauakten prüfen, welches Interesse an der Einsichtnahme besteht und ob Interessen des Grundstückseigentümers entgegenstehen. Danach richtet sich, welche Informationen herausgegeben werden dürfen.

140 § 59 Abs. 3 BauO Bln

141 Z. B. Namen, Anschrift, Verfahrensbeteiligung; siehe § 6 Abs. 2 IFG

12 Wissen und Bildung

12.1 Forschung

12.1.1 Wenn Lehrkräfte beforscht werden

Aufgrund eines anonymen Hinweises gelangten wir in den Besitz eines Schreibens einer Forschungs Kooperation, das an die Fachlehrerkonferenz einer Schule gerichtet war. Darin wurden Lehrkräfte, die Aufgaben der Konferenzleitung übernommen hatten, zur Teilnahme an einer Online-Befragung eingeladen. Unsere Nachforschungen ergaben, dass die Senatsverwaltung für Bildung, Jugend und Wissenschaft die Befragung genehmigt hatte. Sie richtete sich sowohl an die Fachkonferenzleitungen bestimmter Fächer als auch an die jeweiligen Schulleitungen ausgewählter Schulen. Sie sollten dabei angeben, wie sie den Nutzen von Maßnahmen der schulischen Qualitätssicherung (z. B. Schulvergleiche, Schulinspektionen) einschätzen. Die Schulen sollten nach Auswertung der Ergebnisse eine „schulspezifische Rückmeldung“ erhalten.

Zwar wurden die Betroffenen in der Einladung zur Teilnahme über die Zwecke der Datenverarbeitung hinreichend informiert. Sie wurden auch darüber aufgeklärt, dass die Daten im Anschluss an die Erhebung mit wissenschaftlichen Methoden ausgewertet würden. Zugleich wurden die Teilnehmenden online darauf hingewiesen, dass die Befragung freiwillig ist. Die Freiwilligkeit von Einwilligungen von Beschäftigten bedarf jedoch einer kritischen Prüfung; an ihr bestehen im Arbeitsverhältnis in der Regel Zweifel, da aufgrund des Abhängigkeitsverhältnisses den Beschäftigten häufig keine andere Wahl bleibt als der Datenverarbeitung zuzustimmen. Entscheidend in diesem Fall war, dass den Teilnehmenden auf dem Internetportal der Studie zugleich in Aussicht gestellt wurde, dass ihre Schule nach der Auswertung der Ergebnisse eine „schulspezifische Rückmeldung“ in digitaler Form erhalten sollte. Es musste bei den Lehrkräften dadurch der Eindruck entstehen, dass den Schulleitungen durch die Forschungsstudie in personenbeziehbarer Form bekannt wird, welche Meinungen die eigenen Lehrkräfte bezüglich der Evaluationsmaßnahmen der Schulen

haben. Der Umstand der Teilnahme an dieser Studie sowie die dort gemachten Angaben sind personenbezogene Daten, die die dienstliche Beurteilung der Lehrkräfte beeinflussen können.

Erschwerend kam hinzu, dass nicht bereits in den Anschreiben an die Fachkonferenzleiterinnen und -leiter auf die Freiwilligkeit der Befragung hingewiesen worden ist. Diese Schreiben wurden über die jeweilige Schulverwaltung, vermutlich zumeist über die Schulleitungen, den Lehrkräften ausgehändigt, sodass sich der Eindruck der erzwungenen Teilnahme an der Befragung verstärkte. Schließlich wurde auch eine Verlosung durchgeführt, bei der Gewinne nur für die Fälle der gemeinsamen Teilnahme der Schulleitungen und der Fachkonferenzleitungen vorgesehen waren. Dadurch wurde der Teilnahmedruck auf die Lehrkräfte nochmals erhöht.

Es konnte daher insgesamt nicht mehr davon ausgegangen werden, dass sich die Lehrkräfte unter diesen Umständen freiwillig an der Studie beteiligten. Dass die Forschenden sich zwischenzeitlich dazu entschlossen hatten, die Ergebnisse der Befragung nur in aggregierter, d. h. in über alle Schulen der Stichprobe hinweg zusammengefasster Form, an die Schulen zurückzumelden, war zwar aus datenschutzrechtlicher Sicht zu begrüßen, jedoch letztlich verspätet.

Für die Freiwilligkeit einer Einwilligung ist die Sicht der Betroffenen zum Zeitpunkt der Datenerhebung aufgrund der vorhandenen und durch die verantwortliche Stelle zugeleiteten Informationen entscheidend.

12.1.2 Können Partner sich gegenseitig für Elterninterviews bevollmächtigen?

Die Untersuchung des sozialen Lebensumfelds ist regelmäßiger Bestandteil der Schul- und Entwicklungsforschung von Kindern und Jugendlichen. Fragen wie „Wie viele Bücher habt ihr etwa zu Hause?“ sind zwar an die Kinder gerichtet, ermöglichen aber auch Rückschlüsse auf das Leseverhalten und Bildungsniveau im Elternhaus. Auch die Daten über die Einkommens- oder Arbeitssituation der Eltern oder zur Familienherkunft weisen einen doppelten Personenbezug auf.

Im Datenschutzrecht gilt der Grundsatz der Direkterhebung. Personenbezogene Daten sind danach grundsätzlich bei den Betroffenen mit deren Kenntnis zu erheben. Eine Erhebung von Daten bei Dritten ohne Kenntnis der Betroffenen ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt.¹⁴² Eine Datenerhebung bei Dritten mit Kenntnis der Betroffenen kann auch auf deren Einwilligung gestützt werden. Die Beantwortung von Fragen in einem Forschungskontext setzt daher eine informierte schriftliche Einwilligung aller Betroffenen voraus. Dazu gehören

- das Verständnis dafür, dass an einer wissenschaftlichen Studie teilgenommen wird, und Informationen zu ihrem wesentlichen Inhalt,
- Angaben darüber, wie mit den Daten nach der Erhebung verfahren wird,
- das Wissen, welches Ziel die Studie verfolgt,
- der Hinweis, dass die Erhebung freiwillig ist und die Befragung jederzeit abgebrochen werden kann,
- sowie der Hinweis, dass auch nach Ende der Befragung ein Widerruf unter einer anzugebenden Adresse möglich ist.

Die Erhebung sensibler Daten (z. B. zur Einkommenssituation oder Herkunft) setzt darüber hinaus das gesteigerte Bewusstsein über die Abfrage dieser Daten voraus, das sich deutlich auch auf die Erhebung dieser Daten beziehen muss. Nur die oder der jeweils Betroffene kann allein und autonom bewusst in die Erhebung und Verarbeitung ihrer bzw. seiner Daten einwilligen.

Zwar erlaubt das Schulgesetz die Einwilligung von Schülerinnen und Schülern in die eigene Teilnahme an einer Studie ab Vollendung des 14. Lebensjahres ohne Einbeziehung der Eltern. Bei Fragen mit Personenbezug zu den Eltern muss jedoch in jedem Fall die Einwilligung der Eltern in die Datenerhebung vorliegen. Bei gemeinsam lebenden Erziehungsberechtigten kann die Einwilligung eines Elternteils als ausreichend akzeptiert werden, sofern die oder der Unterzeichnende schriftlich versichert, dass der andere Teil sie oder ihn zur Einwilligung in die Teilnahme an der Studie bevollmächtigt hat und dass die oder dem Vertretenen die Fragen (mit doppeltem Personenbezug) bekannt sind. Lebt das Kind in einer Familie mit nur einer erziehungsberechtigten Person, ist

142 § 10 Abs. 4 BlnDSG

eine gegenseitige Bevollmächtigung der zusammenlebenden Erwachsenen in die Erhebung von Daten über das soziale Umfeld des Kindes nicht ausreichend. Die Datenerhebung ist dann nur mit einer eigenen schriftlichen Einwilligung der nicht erziehungsberechtigten Person zulässig.

Eine Bevollmächtigung zur Einwilligung in ein Partnerinterview mit Fragen zu personenbezogenen, teils sensitiven Daten setzt wegen der Voraussetzung der Informiertheit auch eine nachweisbare Vollmachtserklärung voraus.

12.1.3 Zusammenarbeit mit der Ethik-Kommission des Landes Berlin

Im letzten Jahr berichteten wir über den Fall der Leiterin einer klinischen Prüfung.¹⁴³ Vor ihrem Ausscheiden aus den Diensten der Sponsorin der Prüfung hatte sie eigenmächtig schriftliche und elektronische Studienunterlagen in Kopie für die weitere Forschung bei ihrem zukünftigen Arbeitgeber an sich genommen. Die Einstellung des folgenden Strafverfahrens hatte die Staatsanwaltschaft damit begründet, dass der Professorin der erforderliche Vorsatz zu einem „unbefugten“ Handeln gefehlt habe.

Wir nahmen diesen Fall zum Anlass, der Ethik-Kommission vorzuschlagen, dass sie die studienverantwortlichen Forschenden bei Einreichung ihrer Ethik-Anträge auf die Einhaltung der Datenschutzanforderungen bei wissenschaftlichen Studien, insbesondere auf die strafrechtlichen Konsequenzen einer Nichtbeachtung, gesondert hinweist. Dieses Vorgehen ist aus Gründen des Schutzes des informationellen Selbstbestimmungsrechts zukünftiger Probanden und nicht zuletzt aufgrund der Wahrung von Rechtssicherheit im Umgang mit Probandendaten bedeutsam.

Wir berieten die Kommission bei der Neufassung der Mustererklärung zur Einhaltung des Datenschutzes.¹⁴⁴ In dieser Erklärung bringen nunmehr die

¹⁴³ JB 2011, 8.1.2

¹⁴⁴ Siehe § 7 Abs. 3 Nr. 15 der Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen

verantwortlichen Prüfungsleitungen zum Ausdruck, dass sie bei allen wissenschaftlichen Studien mit personenbezogenen Daten von Prüfungsteilnehmenden in der Verantwortung der Forschungseinrichtung die gesetzlichen Grenzen des Datenschutzes beachten werden. Insbesondere verpflichten sie sich, die gewonnenen Probanden- und Studiendaten und eventuelle Proben nur den in der Einwilligungserklärung der Probanden aufgeführten Stellen in pseudonymisierter Form zu übermitteln, zur Verfügung zu stellen oder sonst in ihren Verantwortungsbereich zu verbringen.

Forschenden wird nun bereits bei der Einreichung der Antragsunterlagen für ein Votum durch die Ethik-Kommission bewusst gemacht, dass die unbefugte Verarbeitung personenbezogener Probandendaten strafbewehrt ist.¹⁴⁵

12.1.4 RFID-Technik in öffentlichen Bibliotheken

Die RFID-Technik ermöglicht eine Objektidentifikation mithilfe von Funkwellen. Die Daten eines mit einem RFID-Chip ausgestatteten Objekts können mit einem Lesegerät berührungslos und ohne Sichtkontakt gelesen und gespeichert werden. Diese Technik soll langfristig zur Verbuchung von Medien in allen öffentlichen Bibliotheken Berlins eingesetzt werden.

Im letzten Jahr hatten wir die Prognose gewagt, dass im Laufe des Jahres 2012 die Verbuchungsvorgänge in den ehrenamtlich geführten Bibliotheken ausschließlich mithilfe von RFID-Selbstverbuchungsanlagen durchgeführt werden.¹⁴⁶ Dadurch können ehrenamtlich Beschäftigte, die keine Berechtigung zur Verarbeitung personenbezogener Daten haben, weiterhin in der Bibliothek tätig sein, ohne Zugriff auf diese Daten zu haben.

Dieses Ziel war zu ambitioniert, da zwischenzeitlich technische Probleme bei den neuen für die Selbstverbuchung vorgesehenen Bibliotheksausweisen aufgetreten sind. Mittlerweile sollen diese Probleme behoben sein. Der Verbund Öffentlicher Bibliotheken Berlins (VÖBB) strebt an, den Austausch der Biblio-

145 § 44 Abs. 1 BDSG bzw. § 32 Abs. 1 BlnDSG

146 JB 2011, 8.1.6

theksausweise innerhalb von vier Monaten zu vollziehen und anschließend, sofern genügend Ausweise getauscht werden konnten, komplett auf die RFID-Chips in den Ausweisen umzustellen.

Inzwischen ist die Einrichtung von RFID-Selbstverbuchungsanlagen fortgeschritten und der Anschluss weiterer Bibliotheken an das Netz der RFID-Verbuchung erfolgt. Bislang ist über die Hälfte der Bibliotheken aller Bezirke vollständig mit RFID-Technik ausgestattet. Von den beiden ausschließlich von ehrenamtlich Beschäftigten betriebenen Bibliotheken funktioniert der RFID-Einsatz bisher nur in der Thomas-Dehler-Bibliothek in Tempelhof-Schöneberg; die Kurt-Tucholsky-Bibliothek in Pankow wird RFID voraussichtlich 2013 einsetzen.

Nachdem die Kurt-Tucholsky-Bibliothek in Pankow mit dem Einsatz der RFID-Technik begonnen hat, werden wir die Bibliotheken, insbesondere die ehrenamtlich betriebenen, entsprechend überprüfen. Dabei soll festgestellt werden, ob der VÖBB sein Informationssicherheitskonzept umgesetzt hat.

12.2 Schule

12.2.1 Schultrojaner

Im November 2011 berichtete die taz¹⁴⁷ in dem Artikel „Schnüffelsoftware auf Schulcomputern“, dass die Schulbuchverlage und die Verwertungsgesellschaften mit den Kultusministerien den Einsatz einer Scan-Software auf Schulcomputern vereinbart hätten, um illegale Kopien von Unterrichtsmaterialien aufzuspüren. Bereits am 21. Dezember 2010 war dazu ein Gesamtvertrag zur Einräumung und Vergütung von Ansprüchen nach § 53 Urheberrechtsgesetz (UrhG) geschlossen worden, in dem auch das Land Berlin als Vertragspartner aufgeführt ist. Es verpflichtete sich in dem Vertrag, mithilfe einer von den Verlagen zur Verfügung gestellten Plagiatssoftware an der Überprüfung von Schulrechnern mit-

147 taz vom 1. November 2011, S. 6

zuwirken und die privaten und kommunalen Schulträger aufzufordern, die Vorgaben des Vertrages anzuwenden.

Die Senatsverwaltung für Bildung, Jugend und Wissenschaft teilte uns dazu mit, dass der Gesamtvertrag am 31. März 2011 mit Zustimmung der Finanzministerkonferenz der Länder in Kraft getreten sei. Er ermögliche es, dass alle Lehrkräfte an allen staatlichen, kommunalen, kirchlichen und privaten Schulen im bisherigen Umfang Vervielfältigungen von urheberrechtlich geschützten Materialien für den Unterricht und für Prüfungen nutzen können. Die Schulbuchverlage hätten in den Vertragsverhandlungen jedoch darauf bestanden, dass die Schulverwaltungen Maßnahmen ergreifen, um die Herstellung, Speicherung und Verbreitung von „Digitalisaten von Unterrichtswerken“ zu unterbinden. Eine Maßnahme sei, von den Schulen eine Bestätigung darüber zu erbitten, dass auf den Schulservern keine „Digitalisate von Unterrichtswerken“ vorhanden sind. Zudem sei die Schulverwaltung verpflichtet, den Einsatz einer sog. Plagiatssoftware zu unterstützen, mit deren Hilfe den Schulen ermöglicht wird festzustellen, ob sich „Digitalisate von Unterrichtswerken“ auf den Schulservern befinden. Der Einsatz der noch nicht vorliegenden Software werde in enger Kooperation mit den wissenschaftlichen Einrichtungen des Landes und unserer Behörde erfolgen.

Auf den genutzten Computern der Schulen wird in der Regel auch eine Vielzahl personenbezogener Daten von Schülerinnen und Schülern sowie Lehrkräften verarbeitet; teilweise unterliegen die Daten sogar dem Fernmeldegeheimnis. Der Zugriff auf sie tangiert auch das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Die Umsetzung der Regelungen des Gesamtvertrages zu § 53 UrhG – insbesondere der Einsatz der Plagiatssoftware – begegnet daher erheblichen Bedenken. Auf sie haben wir im parlamentarischen Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit eindringlich hingewiesen.¹⁴⁸ Eine datenschutzgerechte Gestaltung der Plagiatssoftware setzt voraus, dass mit der Software keine personenbezogenen Daten – weder von Lehrkräften noch von Schulleiterinnen oder -leitern – verarbeitet werden, da weder im Schulgesetz noch im Landesbeamtenengesetz noch in anderen Gesetzen eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten zu diesem Zweck vorhanden ist.

148 Siehe Inhaltsprotokoll zur 3. Sitzung am 6. Februar 2012, Punkt 2, Seite 2 ff.

Angesichts der massiven Kritik von Datenschutzbeauftragten, Verbänden, Gewerkschaften und aus dem politischen Raum wurde die Umsetzung der Regelungen des Gesamtvertrages zunächst ausgesetzt. Mittlerweile ist das Vorhaben, die urheberrechtlich geschützten Werke auf Schulcomputern mithilfe von „Trojanern“ aufzuspüren, aufgegeben worden. Im Dezember schlossen die Kultusministerien der Länder mit dem Verband Bildungsmedien sowie den Wertungsgesellschaften einen neuen Urheberrechtsvertrag, der derartige Maßnahmen nicht mehr vorsieht.¹⁴⁹

Urheberrechte rechtfertigen auch in der Schule keine Eingriffe in das Telekommunikationsgeheimnis oder die Vertraulichkeit und Integrität informationstechnischer Systeme.

12.2.2 Einsatz von privaten Smartphones durch Lehrkräfte zu dienstlichen Zwecken

Zunehmend werden wir gebeten, den Einsatz von Softwareprodukten (Apps)¹⁵⁰ zur dienstlichen Verwaltung von Schülerdaten auf privaten Smartphones und Tablets der Lehrkräfte zu bewerten.

In der Regel werden mit diesen Produkten personenbezogene Schülerdaten (z. B. Name, Vorname, Klasse) verarbeitet. Oftmals bieten die „Apps“ jedoch auch Funktionen, mit denen wesentlich sensitivere Leistungsdaten (z. B. Noten) verwaltet werden können. Die Verarbeitung von derartigen personenbezogenen Schülerdaten auf einem privaten Datenverarbeitungsgerät ist den Lehrkräften – wie anderen Bediensteten der Berliner Verwaltung – grundsätzlich untersagt.¹⁵¹ Unter bestimmten Voraussetzungen kann von der Schulleitung jedoch im Ausnahmefall eine Genehmigung erteilt werden.¹⁵² Dabei sind die technischen und organisatorischen Maßnahmen sowie die Grundsätze der IT-Sicherheit nach § 5 BlnDSG zu berücksichtigen. Da nicht auszuschließen ist, dass auf einem privaten Smartphone oder Tablet-Computer auch unsichere „Apps“ installiert

149 Tagesspiegel vom 10. Dezember 2012, S. 25

150 Z. B. die Smartphone-Software „Teachertool“, siehe www.teachertool.de

151 Siehe 2.3

152 § 64 Abs. 2 Satz 2 und 3 SchulG

sind, deren Kommunikationsverhalten (z. B. durch die Speicherung von Daten in ausländischen Cloud-Diensten) durch den Nutzenden nicht vollständig kontrolliert werden kann, lassen sich diese IT-Grundsätze nicht realisieren. Insofern ist der Einsatz derartiger Software auf privaten Geräten grundsätzlich als datenschutzrechtlich kritisch anzusehen.

Diese Einschätzung wird von der Senatsverwaltung für Bildung, Jugend und Wissenschaft grundsätzlich geteilt. Unser Angebot, zusammen mit der Senatsverwaltung verbindliche Vorgaben für den Einsatz von privaten IT-Geräten durch die Lehrkräfte in den Schulen zu entwickeln, wurde begrüßt. In welcher Form die Umsetzung erfolgt, bleibt abzuwarten.

Der Einsatz von privaten Smartphones durch Lehrkräfte zur Verwaltung von personenbezogenen Schülerdaten ist nicht ohne Weiteres zulässig. Um ihn zu ermöglichen, sind konkrete und verbindliche Vorgaben unter Einbeziehung der datenschutzrechtlichen IT-Grundsätze zu entwickeln und in die Schulen zu kommunizieren.

12.2.3 Veröffentlichungen von Abiturientendaten in der Tagespresse

In jedem Jahr werden nach Abschluss der Abiturprüfungen die erfolgreichen Abiturientinnen und Abiturienten in einer Auflistung mit Namen und Vornamen nach Schulen sortiert in der Tagespresse veröffentlicht. Auf Nachfrage teilte uns die Senatsverwaltung für Bildung, Jugend und Wissenschaft mit, dass nicht sie, sondern die jeweilige Schule die Abiturientendaten an die Presse weitergibt.

Zweifellos handelt es sich bei den Namen, Vornamen und Angaben zu den jeweils besuchten Schulen um personenbezogene Daten der Abiturientinnen und Abiturienten. Die Übermittlung dieser Schülerdaten durch die Schule an die Presse ist nur mit schriftlicher Einwilligung der Betroffenen zulässig.¹⁵³ Wird die Datenverarbeitung auf die Einwilligung der Betroffenen gestützt, sind sie

153 § 64 Abs. 5 Satz 2 Nr. 1 SchulG

zuvor in geeigneter Weise über die Bedeutung der Einwilligung und den Verwendungszweck der Daten aufzuklären. Bei einer beabsichtigten Übermittlung müssen auch der Datenempfänger sowie der Zweck der Datenübermittlung genannt werden.¹⁵⁴ In jedem Fall ist die Einwilligung nur wirksam, wenn sie freiwillig erfolgt.¹⁵⁵

Seit der Verkürzung der Schulzeit bis zum Abitur von bisher dreizehn auf zwölf Jahre stellt sich für die Schulen zwangsläufig die Frage, ob auch minderjährige Abiturientinnen und Abiturienten wirksam in die Übermittlung ihrer Daten an die Presse einwilligen können. Grundsätzlich ist dies zu bejahen. Denn es kommt für die wirksame Abgabe einer Einwilligung in die Datenverarbeitung nicht auf die Geschäftsfähigkeit der Betroffenen an. Maßgeblich ist, ob sie psychisch und intellektuell in der Lage sind, die Tragweite der Entscheidung abzuschätzen. Fehlt diese Einsichtsfähigkeit, bedarf es zwingend der Einwilligung der Erziehungsberechtigten. Anhaltspunkte dafür, in welchen Fällen die Einwilligung der Schülerinnen und Schüler ausreicht oder die der Erziehungsberechtigten einzuholen ist, bieten Regelungen aus anderen Rechtsbereichen. So kann z. B. ein Kind nach Vollendung des 14. Lebensjahres selbst entscheiden, zu welcher Religion es sich bekennen will. Im Ehescheidungsverfahren kann eine 14-jährige Person dem Gericht Vorschläge für die Zuweisung des elterlichen Sorgerechts machen, eine 15-jährige kann Sozialleistungen beantragen und entgegennehmen. Insofern ist davon auszugehen, dass Schülerinnen und Schüler im Alter von 14 bis 15 Jahren in der Regel in der Lage sind, die Folgen der Verwendung ihrer Daten zu beurteilen. Je jünger eine minderjährige Person ist, desto größer muss die Sorgfalt sein, mit der über den Zweck und den Umfang der Datenverarbeitung, über die Löschung der Daten, die Widerspruchs- und Auskunftsrechte aufzuklären ist.

Das Schulgesetz sieht für Minderjährige in mehreren Fällen die Möglichkeit der Einwilligung in die Verarbeitung ihrer Daten vor. So haben Schülerinnen und Schüler bereits ab dem vollendeten 14. Lebensjahr grundsätzlich das Recht, Akten der Schule und der Schulaufsichtsbehörden einzusehen.¹⁵⁶ Die genannte Altersgrenze gilt auch für die Erteilung der Einwilligung in die Übermittlung

154 § 6 Abs. 3 BlnDSG

155 § 6 Abs. 5 BlnDSG

156 § 64 Abs. 7 Satz 1 SchulG

von personenbezogenen Daten an Stellen außerhalb des öffentlichen Bereichs,¹⁵⁷ z. B. die Presse.

Ob die erforderliche (schriftliche) Einwilligung der Abiturientinnen und Abiturienten in die Übermittlung ihrer Daten an die Presse an allen Schulen eingeholt wird, ist nicht bekannt. Die Senatsverwaltung für Bildung, Jugend und Wissenschaft hat angekündigt, dass sie die Schulen im Frühjahr 2013 in einem Rundschreiben über das Erfordernis der Einwilligungen informieren und so im Vorfeld der Presseanfragen für das Problem sensibilisieren wird.

Die Übermittlung von Abiturientendaten durch die Schule an die Presse bedarf der schriftlichen Einwilligung der Betroffenen. Die Schulleitungen haben sicherzustellen, dass die Einwilligungen bei den Betroffenen vor einer Übermittlung eingeholt werden.

12.2.4 Das Abiturzeugnis des Regierenden Bürgermeisters

Der Süddeutschen Zeitung¹⁵⁸ war zu entnehmen, dass ein ehemaliger Schulleiter einer Journalistin der Zeitung die Einsichtnahme des Abiturzeugnisses des Regierenden Bürgermeisters ermöglicht hat. Dazu verschaffte er sich und der Journalistin während der Ferien unter Verwendung der Schulschlüssel Zugang zum Schulgebäude, den Räumen des Direktorats und zu dem Schrank, in dem die Abiturzeugnisse aufbewahrt wurden. Auf Nachfrage teilte uns der derzeitige Schulleiter mit, dass in der Schule alle Abiturzeugnisse von 1928 bis 2009 in gebundener Form vorliegen. Darüber hinaus würden an der Schule alle Abgangszeugnisse und alle Abschlusszeugnisse seit 1924 in einem verschlossenen Schrank im Dienstzimmer des Schulleiters aufbewahrt. Sein Vorgänger, der ihn in den vergangenen elf Jahren bei der Leitung der Schule unterstützt hat, habe einen Generalschlüssel für die Schule besessen. Während seiner Abwesenheit habe sein Vorgänger ihn ver-

157 § 64 Abs. 7 Satz 1, 2. Halbsatz SchulG

158 Süddeutsche Zeitung vom 10. Oktober 2011, S. 3

treten, Aufgaben im Sekretariat versehen und auch den Stundenplan erstellt. Die Senatsverwaltung für Bildung, Jugend und Wissenschaft teilte uns mit, dass eine Vertretung der Schulleitung durch aus dem Dienst ausgeschiedene Schulleiterinnen oder Schulleiter unüblich sei und dass sie von der Zusammenarbeit der beiden Schulleiter nichts wusste.

Die Aufbewahrungsfristen für Zeugnisse und Prüfungsunterlagen sind für alle Schulen verbindlich und abschließend in der Schuldatenverordnung geregelt. Durchschriften von Abschluss- oder Abgangszeugnissen und von Zeugnissen über die Teilnahme an Prüfungen sind 50 Jahre nach Abschluss des Jahres, in dem sie ausgestellt wurden, aufzubewahren.¹⁵⁹ Nach Ablauf der Frist sind die Unterlagen jahrgangsweise zu vernichten.¹⁶⁰ Diese Vorgaben wurden an der Schule nicht umgesetzt. Die Aufbewahrung (Speicherung) der Zeugnisse über die Frist von 50 Jahren hinaus ist datenschutzrechtlich unzulässig. Soweit landesarchivrechtliche Vorgaben dem nicht entgegenstehen, sind die Unterlagen umgehend zu vernichten.

Jede Daten verarbeitende Stelle im Anwendungsbereich des Berliner Datenschutzgesetzes hat die erforderlichen technisch-organisatorischen Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit).¹⁶¹ Weder der ehemalige Schulleiter noch die Journalistin der Süddeutschen Zeitung waren in diesem Sinne „befugt“. Der ehemalige (pensionierte) Schulleiter war zu diesem Zeitpunkt nicht mehr im aktiven Schuldienst. Als „schulfremde“ Person hatte er keine Berechtigung, personenbezogene Daten über einen ehemaligen Schüler an Dritte zu übermitteln. Für diesen erheblichen Datenschutzverstoß trägt der jetzige Schulleiter die Verantwortung. Indem er seinem Vorgänger einen Generalschlüssel zur Schule überlassen hat, war die Vertraulichkeit der personenbezogenen Daten an der Schule nicht mehr gewährleistet. Der derzeitige Schulleiter hat durch sein Handeln ermöglicht, dass Unbefugte die personenbezogenen Zeugnisdaten des Regierenden Bürgermeisters zur Kenntnis nehmen konnten. Durch die aktive Vertretung des jetzigen Schulleiters bei dessen Abwesenheit, die Übernahme von Aufgaben im Sekretariat und durch die Erstellung

159 § 13 Satz 1 SchuldatenVO

160 § 13 Satz 2 SchuldatenVO

161 § 5 Abs. 4 i. V. m. § 5 Abs. 2 Nr. 1 BlnDSG

des Stundenplans hatte der ehemalige Schulleiter über einen Zeitraum von elf Jahren unberechtigten Zugang zu personenbezogenen Daten der Schülerinnen und Schüler, ihrer Erziehungsberechtigten und der Lehrkräfte. Durch ihre „Zusammenarbeit“ haben der ehemalige und derzeitige Schulleiter in erheblichem Umfang gegen eine Vielzahl von datenschutzrechtlichen Bestimmungen verstoßen. Die Anzahl der Betroffenen, in deren Recht auf informationelle Selbstbestimmung dabei massiv eingegriffen wurde, ist ebenfalls erheblich. Wir haben die Verstöße beanstandet.¹⁶²

In ihrer Stellungnahme hat die Senatsverwaltung für Bildung, Jugend und Wissenschaft den Verstoß gegen Datenschutzrecht an der Schule bestätigt. Der Schulleiter sei auf die Datenschutzregelungen hingewiesen, über die Notwendigkeit der Einhaltung des Datenschutzes belehrt und zur Vernichtung der überfälligen Akten aufgefordert worden.

Die Schulen haben dafür Sorge zu tragen, dass keine Unbefugten in die Durchschriften von Abschluss- oder Abgangszeugnissen und von Zeugnissen über die Teilnahme an Prüfungen Einsicht nehmen können. Unbefugt sind auch ehemalige Lehrkräfte und Schulleitungen. Soweit das Landesarchivrecht dem nicht entgegensteht, sind die Unterlagen 50 Jahre nach Abschluss des Jahres, in dem sie erstellt wurden, in den Schulen zu vernichten.

12.2.5 Werbefilm aus der Basketball-AG

Eine Mutter beschwerte sich darüber, dass ihr Sohn im Rahmen einer Basketball-AG in der Schule von einem Filmteam gefilmt worden sei. Das Bildmaterial sei vom Betreiber des Internats an der Schule für einen Imagefilm über das Internat verwendet worden. Sie sei über die Maßnahme nicht informiert gewesen und habe dem auch nicht zugestimmt. Von der Schulleitung wurde der Sachverhalt im Wesentlichen bestätigt. Der Film sei nicht von der Schule, sondern in der Verantwortung des (privatrechtlichen) Betreibers des Internats gedreht worden. Diesem sei von der Schulleitung eine

162 § 26 Abs. 1 BlnDSG

Dreherlaubnis in den Räumen der Schule erteilt worden. Alle Schülerinnen und Schüler, die während der Filmaufnahmen Basketball spielen und teilweise kurz im Bild zu sehen sind, seien vorher über den Verwendungszweck der Filmaufnahmen aufgeklärt und gebeten worden, die Halle zu verlassen, wenn sie im Film nicht erscheinen wollen.

Ein Teil des Bildmaterials für den Imagefilm wurde in den Gebäuden der Schule während einer Schulveranstaltung (AG Basketball) aufgenommen. Auch wenn der Film von dem privaten Betreiber des Internats aufgenommen wurde, liegt die datenschutzrechtliche Verantwortung für diesen Teil der Bildaufnahmen bei der Schule. Durch die Aufnahme des Bildmaterials wurden personenbezogene Daten der an der Schulveranstaltung (AG Basketball) teilnehmenden Schülerinnen, Schüler und evtl. Lehrkräfte verarbeitet. Dabei ist es grundsätzlich unerheblich, wie lange die einzelnen Personen zu sehen sind oder ob sie sich im Hintergrund aufhalten. Einer der Betroffenen war jedenfalls unstreitig der Sohn der Petentin.

Nach dem Schulgesetz¹⁶³ darf eine Schule personenbezogene Schülerdaten nur verarbeiten, wenn dies zur Erfüllung der schulbezogenen Aufgaben erforderlich ist. Da es sich bei der Erstellung des Imagefilms für das privatrechtlich betriebene Internat nicht um eine schulbezogene Aufgabe gehandelt hat, kann die Datenverarbeitung nicht auf die genannte Rechtsvorschrift gestützt werden.

Auch hat der Betroffene nicht wirksam eingewilligt. Soll die Datenverarbeitung auf seine Einwilligung gestützt werden, so ist er in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären.¹⁶⁴ Die Einwilligung bedarf grundsätzlich der Schriftform, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist. Die Einwilligung kann auch von Minderjährigen wirksam erteilt werden, soweit ihre Einsichtsfähigkeit ausreicht, die Folgen ihrer Erklärung abzuschätzen.¹⁶⁵ Eine konkludente, mutmaßliche oder stillschweigende Einwilligung ist nicht ausreichend. Der Erklärungswille muss vielmehr deutlich (z. B. mündlich) artikuliert werden. Der Sohn der Petentin wurde vor den Filmaufnahmen über

163 § 64 Abs. 1 SchulG

164 § 6 Abs. 3 BlnDSG; § 4 a Abs. 1 BDSG

165 Siehe 12.2.3

deren Verwendungszweck aufgeklärt und wie die anderen Schülerinnen und Schüler aufgefordert, die Turnhalle zu verlassen, wenn er nicht in dem Film zu sehen sein will. Er ist dieser Aufforderung nicht gefolgt. Es ist nicht ersichtlich, dass dem Sohn der Petentin ein Nachteil dadurch entstanden wäre, wenn er die Turnhalle verlassen hätte. Er hat sich jedoch für den Verbleib in der Turnhalle entschieden. Als 17-jähriger Schüler hatte er auch die Einsichtsfähigkeit, die Folgen seines Handelns einzuschätzen. Ungeachtet dessen kann das konkludente Handeln des Betroffenen (Verbleib in der Turnhalle) nicht als eine wirksame Einwilligung in die Datenverarbeitung gewertet werden. Insofern war ein datenschutzrechtlicher Mangel festzustellen.

Wir haben der Schule für zukünftige vergleichbare Projekte dringend empfohlen, bereits im Vorfeld der Datenverarbeitung von den betroffenen Schülerinnen, Schülern und Lehrkräften eine schriftliche Einwilligung einzuholen. Bei jüngeren Schülerinnen und Schülern sollte in jedem Fall auch eine vorherige Information der Eltern erfolgen und deren Einverständnis eingeholt werden.

Die Einwilligung in die Datenverarbeitung hat grundsätzlich schriftlich zu erfolgen. Eine mündliche Einwilligung ist nur im Ausnahmefall möglich. Eine konkludente, mutmaßliche oder stillschweigende Einwilligung kann nicht unterstellt werden und ist unwirksam.

12.2.6 Die Hausaufgabenliste und ein Datenaustausch „unter Brüdern“!

Die Eltern von zwei Brüdern, die unterschiedliche Schulen besuchen, haben sich darüber beschwert, dass die Schulen Daten über die Anwesenheitszeiten ihrer Kinder ausgetauscht haben, obwohl dazu keine Veranlassung bestanden habe. Darüber hinaus habe die Klassenlehrerin des einen Sohnes eine Liste über angefertigte bzw. nicht angefertigte Hausaufgaben von einer Mitschülerin führen lassen. Die Schulleitungen bestätigten uns die Schilderung der Eltern im Wesentlichen. Der Schulleiter der anfragenden Schule gab an, dass er wegen des Verdachts einer Schulpflichtverletzung überprüft habe, ob die Schulpflicht tatsächlich verletzt und damit eine Schulversäumnisanzeige

notwendig sei. In diesem Zusammenhang habe er bei der ihm bekannten Schule des Geschwisterkindes nachgefragt, ob es seinerseits die Schulpflicht erfülle. Die Schulleitung der befragten Schule erklärte, die Sekretärin habe mitgeteilt, dass auch das Geschwisterkind in der Schule fehle. Dies sei im Rahmen der Amtshilfe geschehen, da die anfragende Schule eine Schulversäumnisanzeige stellen wollte.

Unbestritten handelt es sich bei den Angaben über die Fehlzeiten eines Schülers um personenbezogene Daten. Werden diese Daten von einer Schulsekretärin an eine andere Schule weitergegeben, werden sie sowohl übermittelt als auch (von der anfragenden Schule) erhoben.¹⁶⁶ Der allgemeine Grundsatz der Amtshilfe kann nicht als Rechtsgrundlage herangezogen werden. Nach dem Schulgesetz¹⁶⁷ darf eine Schule jedoch die personenbezogenen Daten einer Schülerin oder eines Schülers an eine andere Schule nur übermitteln, wenn dies zur rechtmäßigen Erfüllung der gesetzlichen Aufgaben der übermittelnden oder der empfangenden Schule erforderlich ist.

In diesem Fall kam es somit entscheidend darauf an, ob die Übermittlung der Fehlzeiten des Geschwisterkindes für die Aufgabenerfüllung der übermittelnden Schule oder der Schule, die die Daten empfangen hat, erforderlich war. Die Verfolgung von Schulpflichtverletzungen ist Bestandteil des gesetzlichen Bildungs- und Erziehungsauftrags einer Schule. Er erstreckt sich jedoch jeweils nur auf die Schülerinnen und Schüler, die an einer Schule angemeldet sind. Von der Schule des Geschwisterkindes wurde im Zeitpunkt der Übermittlung von dessen Fehlzeiten kein Schulversäumnisverfahren geführt. Die Datenübermittlung war daher für die Aufgabenerfüllung der übermittelnden Schule nicht erforderlich. Da das Geschwisterkind kein Schüler der anfragenden Schule war, waren die übermittelten Daten auch für die Aufgabenerfüllung dieser Schule (das Schulversäumnisverfahren wurde gegen den Bruder geführt) nicht erforderlich. Die Übermittlung der Fehlzeiten des Geschwisterkindes war somit weder für die rechtmäßige Erfüllung der gesetzlichen Aufgaben der übermittelnden noch der empfangenden Schule erforderlich. Die Übermittlung der Schülerdaten konnte somit nicht auf das Schulgesetz gestützt werden und war

166 § 12 Abs. 1 Satz 1 i. V. m. § 11 Abs. 2 Satz 1 Nr. 1, § 6 Abs. 1 BlnDSG

167 § 64 Abs. 3 SchulG

unzulässig. Dasselbe galt für die Erhebung der Daten durch die Schule, die ein Schulversäumnisverfahren prüfte.

Zu dem Vorwurf, die Klassenlehrerin lasse die Hausaufgabenliste von einer Schülerin führen, teilte die Schulleitung mit, dass die Liste von der Klassenlehrerin geführt werde. Im Rahmen der Übertragung von Verantwortung habe die Lehrkraft jedoch auch Eintragungen in die Liste durch eine Schülerin vornehmen lassen. Die Schulleitung hat die Lehrkraft angewiesen, alle Eintragungen ausschließlich selbst vorzunehmen.

Auch bei der Verarbeitung von Daten über Geschwisterkinder ist darauf zu achten, dass die Datenverarbeitung für die eigene (schulbezogene) Aufgabenerfüllung erforderlich ist.

12.2.7 Videoüberwachung an Schulen

Der Einsatz von Videoüberwachungstechnik führt zu einer intensiven Kontrolle, die grundsätzlich mit Eingriffen in die Grundrechte der davon erfassten Personen verbunden ist. Auch an Schulen nimmt die Videoüberwachung stetig zu. Beleg dafür sind die sichtbaren Anlagen an den Außenfassaden von Schulgebäuden, vereinzelte Eingaben von Betroffenen und diverse Pressemeldungen zu diesem Thema.

Wir haben die Videoüberwachung an Schulen bereits 2009 ausführlich behandelt¹⁶⁸ und darauf hingewiesen, dass weder das Schulgesetz noch die dazu ergangenen Verordnungen bereichsspezifische Regelungen zur Videoüberwachung an Schulen enthalten. Im Ergebnis haben wir festgestellt, dass angesichts des erheblichen Eingriffs in die Grundrechte der Betroffenen grundsätzlich von einer Videoüberwachung an Schulen abgesehen werden sollte.

Ungeachtet dessen fehlten uns bislang verlässliche Informationen, in welchem Ausmaß, zu welchem Zweck und unter welchen technisch-organisatorischen Rahmenbedingungen die Videotechnik an Schulen eingesetzt wird. Deshalb

168 JB 2009, 2.2

haben wir die bezirklichen Schulämter gebeten, eine Umfrage an den Schulen in ihrem Zuständigkeitsbereich durchzuführen. Auf der Grundlage eines von uns erstellten Fragebogens haben sich die Schulleitungen der öffentlichen Schulen direkt oder stellvertretend ihre bezirklichen Schulämter zu diesem Thema geäußert. Anhand der Rückmeldungen wurde deutlich, dass sich unsere Vermutung einer zunehmenden massiven „Aufrüstung“ mit Videotechnik an Schulen nicht bestätigt hat. Im Gegenteil: Vergleichsweise wenige Schulen betreiben eine Videoüberwachungsanlage, wobei hervorzuheben ist, dass viele Kameras lediglich als „verlängertes Auge“ dienen, d. h. weder über eine Aufzeichnungs- oder Speicherfunktion verfügen noch die Innenbereiche von Schulgebäuden überwachen.

Nach Auswertung der Informationen haben wir festgestellt, dass an sechs Schulen eine Videoüberwachung mit Aufzeichnung von Bilddaten stattfindet.¹⁶⁹ Wir haben datenschutzrechtliche Kontrollen vor Ort vorgenommen. Bei fünf der sechs Schulen sind höchstens ein bis drei Kameras im Einsatz, die in erster Linie die Haupteingänge zu den Schulgebäuden und die Fahrradständer auf dem Schulgelände erfassen. In allen Fällen sind die Kameras installiert worden, nachdem Vorfälle gemeldet wurden. Im Bereich der Haupteingänge kam es zu Gewaltandrohung und Gewaltanwendung durch unbefugte Dritte, im Bereich der Fahrradständer waren Diebstähle zu verzeichnen. Die Videokameras im Haupteingangsbereich und an den Fahrradständern dieser Schulen sind nach unserer Auffassung geeignet, da sie potenzielle Straftäter beim Betreten des Geländes abschrecken könnten. Nach Installation der Kameras ist die Anzahl der Vorfälle an den kontrollierten Schulen deutlich zurückgegangen.

Eine Ausnahme bildete allerdings die Carl-Zeiss-Oberschule in Tempelhof-Schöneberg. Hier war die Anzahl der Kameras mit 22 unverhältnismäßig hoch. Zudem waren die Kameras als reine Vorsichtsmaßnahme installiert worden, weil es oft Schmierereien am alten Schulgebäude gab. Am neuen Gebäude war es bisher nur zu einem Vorfall gekommen, wobei die Auswertung des Bildmaterials nicht zur Täteridentifizierung führte. Wir haben die Geeignetheit der Videoüberwachung in diesem Einzelfall bezweifelt. Durch die dargelegten Vor-

169 Kurt-Tucholsky-Grundschule in Mitte, Otto-Hahn-Oberschule und Heinrich-Mann-Oberschule in Neukölln, Christoph-Förderich-Grundschule und Bertold-Brecht-Oberschule in Spandau, Carl-Zeiss-Oberschule in Tempelhof-Schöneberg

fälle haben wir die Videoüberwachung an der Carl-Zeiss-Oberschule weder als verhältnismäßig noch als erforderlich angesehen. Die meisten Kameras waren nicht zweckorientiert; sie überwachten Bereiche, in denen es zu keinen Vorfällen gekommen war. Die Schulleitung der Carl-Zeiss-Oberschule wurde aufgefordert, die Anzahl der Kameras deutlich zu verringern.

Angesichts des erheblichen Eingriffs in die Grundrechte der Betroffenen begrüßen wir den zurückhaltenden Einsatz von Videoüberwachung an Berliner Schulen.

13 Wirtschaft

13.1 Banken und Versicherungen

13.1.1 Bankrecht ersetzt nicht Datenschutzrecht

Das Wertpapierhandelsgesetz (WpHG), das Geldwäschegesetz (GwG) und das Kreditwesengesetz (KWG) enthalten bereichsspezifische Datenschutzvorschriften. Da hier aber zumeist nur Teilaspekte geregelt werden, ist daneben das BDSG zu beachten.

Nach dem GwG darf derjenige, der die Identität seines Vertragspartners prüfen muss, das ihm vorgelegte Ausweisdokument kopieren, um auf diese Weise die bei der Identitätsprüfung erhobenen Angaben aufzuzeichnen.¹⁷⁰ Die Personalausweiskopie enthält jedoch Daten, die nach dem GwG nicht benötigt werden.¹⁷¹ Das Geldwäschegesetz regelt nicht, ob die überschüssigen Daten zu löschen sind. Diese Verpflichtung ergibt sich aber aus dem Erforderlichkeitsprinzip und dem Grundsatz der Datensparsamkeit¹⁷² nach dem BDSG.

Kreditinstitute sind verpflichtet, angemessene Datenverarbeitungssysteme zu betreiben und zu aktualisieren, mittels derer geldwäscherelevante Transaktionen zu erkennen sind.¹⁷³ Das KWG berechtigt die Institute inzwischen ausdrücklich, personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, soweit dies zur Erfüllung der Pflicht, ein entsprechendes Research-System zu betreiben, erforderlich ist. Die Gesetzesänderung führte bei der Deutschen Kreditwirtschaft zu dem Missverständnis, dass das Arbeitspapier der Aufsichtsbehörden „Datenschutzrechtliche Anforderungen für Research-Systeme zur Aufdeckung von Geldwäsche“¹⁷⁴ obsolet sei. Die in diesem Papier niedergelegten Grundsätze der Zweckbindung der Speicherung, der Nachvollziehbarkeit der ver-

170 § 8 Abs. 1 Satz 3 GwG

171 § 4 Abs. 3 Ziff. 1 GwG i.V.m. § 8 Abs. 1 GwG

172 § 3a BDSG

173 § 25 c Abs. 2 Satz 1 KWG

174 Gem. § 25c Abs. 2 Satz 2 KWG; das Arbeitspapier ist abrufbar unter www.die-deutsche-kreditwirtschaft.de/uploads/media/201107_Anlage-Stellungnahme-GwBekErgG.pdf

wendeten Parameter und der Grundsatz der frühestmöglichen Datenlöschung gemäß wissenschaftlich-statistischer Kenntnis gelten jedoch auch weiterhin. Es ist auch zu beachten, dass die Ermächtigungsgrundlage im KWG nicht ausreicht, um sensitive Daten¹⁷⁵ zu rastern.

Mit Genehmigung der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) dürfen Institute interne Sicherungsmaßnahmen im Rahmen von vertraglichen Vereinbarungen von einem Dritten durchführen lassen.¹⁷⁶ Die Banken gehen zu Unrecht davon aus, dass durch die Genehmigung der BaFin auch die datenschutzrechtlichen Voraussetzungen erfüllt seien. Die Übertragung der Geldwäschaufgaben bedarf einer Rechtsvorschrift.¹⁷⁷ Zur Wahrung der schutzwürdigen Interessen der Betroffenen ist dabei eine Kontrolle des Dritten erforderlich, die im Wesentlichen den Anforderungen des § 11 BDSG entspricht. Auch ist die Benachrichtigungsverpflichtung nach § 33 BDSG zu beachten.

Wertpapierdienstleistungsunternehmen sind verpflichtet, von Kunden in bestimmtem Umfang Informationen über Kenntnisse und Erfahrungen, Anlageziele und finanzielle Verhältnisse einzuholen.¹⁷⁸ Die von den Banken hierzu entwickelten Fragebögen berücksichtigen häufig nicht, dass der Umfang der Daten kunden- und produktorientiert sein sollte.

Unternehmen sind verpflichtet, Auskunftersuchen der Aufsichtsbehörde unverzüglich zu beantworten. Dies betrifft auch noch nicht bekannt gemachte, datenschutzrechtlich relevante Informationen von Aktiengesellschaften, die den Börsenkurs der Wertpapiere des Unternehmens erheblich beeinflussen können (ad-hoc-Meldung). Die Aufsichtsbehörde ist allerdings gehalten, bei Anfragen nach dem IFG oder dem Presserecht keine Informationen zu noch nicht veröffentlichten ad-hoc-Meldungen zu geben.

Das BDSG und die allgemeinen datenschutzrechtlichen Grundsätze sind auch bei der Anwendung von bankrechtlichen Normen zu beachten.

175 § 3 Abs. 9 BDSG

176 § 25 c Abs. 5 Satz 1 KWG

177 § 4 i.V.m. § 28 Abs. 1 Satz 1 Nr. 2 BDSG

178 § 31 Abs. 4 WpHG

13.1.2 Ist das ec-cash-Verfahren sicher?

Bankkundinnen und -kunden gehen im allgemeinen davon aus, dass das PIN-gestützte ec-cash-Verfahren sicher ist. Viele Betroffene kontrollieren deshalb Abbuchungen im ec-cash-Verfahren weniger sorgfältig als normale Lastschriftabbuchungen. Auch vor Gericht dürfte man wohl kaum eine Chance mit der Einrede haben, eine PIN-gestützte Abbuchung nicht vorgenommen zu haben.

Ein Fall in Norddeutschland zeigte nun Sicherheitsprobleme beim ec-cash-Verfahren auf. Ein Kunde gab an einer Tankstelle eine falsche Tanksäule an, sodass ihm ein geringerer Betrag berechnet wurde. Er bezahlte im ec-cash-Verfahren mit PIN-Eingabe. Um den fehlenden Betrag von dem Kunden zu erhalten, veranlasste der Tankstelleninhaber eine Mitarbeiterin der Abrechnungsstelle seiner Netzbetreiberin, den fehlenden Betrag beim Kunden einzuziehen. Die Mitarbeiterin kopierte den alten Buchungssatz und wählte als Transaktionstyp ec-cash. Auf dem Kontoauszug des Kunden erschien als Verwendungszweck „Einlösungsgarantiert, ec-cash-Verfahren Inland“.

Der Fall veranlasste die Aufsichtsbehörden, von der Deutschen Kreditwirtschaft eine Verbesserung der Datensicherheit beim ec-cash-Verfahren zu fordern. Die Möglichkeit, manuell Transaktionen im ec-cash-Verfahren auszulösen, ist eine erhebliche Sicherheitslücke. Diese wollte die Deutsche Kreditwirtschaft dadurch schließen, dass Netzbetreiber vertraglich dazu verpflichtet werden sollen, keine manuell zahlungsgarantierten ec-cash-Transaktionen nachzuerfassen. Diese rein vertragliche Sicherstellung, die noch nicht einmal durch entsprechende Compliance-Regelungen der Beschäftigten der Netzbetreiber ergänzt wird, ist nicht ausreichend, um eine Manipulation der Daten und eine zusätzliche Generierung von Datensätzen zu verhindern.¹⁷⁹ Die Aufsichtsbehörden haben die Deutsche Kreditwirtschaft deshalb aufgefordert, technische Maßnahmen zu treffen, um künftig manuelle Buchungen im ec-cash-Verfahren – die für Betroffene nicht einmal als solche erkennbar sind – zu unterbinden.

179 Nr. 4 der Anlage zu § 9 Satz 1 BDSG

Die Deutsche Kreditwirtschaft ist aufgefordert, die erhebliche Sicherheitslücke im ec-cash-Verfahren zu schließen.

13.1.3 Kuvertierungsprobleme in einer Bank

Aus der Praxis

Eine Bank hat Kunden Infobriefe zugesandt, in deren Sichtfenstern eine Personennummer als internes Ordnungsmerkmal eingedruckt war, um Rücksendungen bearbeiten zu können, ohne den Brief öffnen zu müssen. Bei einigen Kunden war die Personennummer mit der Kontonummer identisch.

Die Bank hat eingeräumt, fehlerhaft gehandelt zu haben, da sie die Kontonummer Dritten zugänglich gemacht habe. Sie habe übersehen, dass die verwendete Personennummer bei einigen Kunden mit der Kontonummer identisch sei. Die Bank hat ihr Verfahren umgestellt und verwendet bei Mailingaktionen nur noch intern nachvollziehbare, fortlaufende Nummern, sodass im Sichtfenster eines Briefes keine schützenswerten personenbezogenen Daten mehr sichtbar sind.

Aus der Praxis

Ein Kreditkartenkunde der Bank wunderte sich nicht schlecht, als er von ihr einen Werbebrief für Kreditkartenkunden erhielt, in dem sich auch Werbeschreiben an andere Bewohner seiner Stadt (einer bayerischen Kleinstadt) befanden.

Durch den Kuvertierungsfehler hat der Petent die Information erhalten, wer in seiner Nachbarschaft ebenfalls Kreditkartenkunde der Bank ist. Der Briefversand erfolgte durch maschinelle Kuvertierung. Es gab zwar eine Doppeleinzugskontrolle, die bei einem Mehrfacheinzug von Briefen die Maschine anhielt, sodass die Fehlkuvertierungen manuell aussortiert werden konnten. Die Beschäftigten haben es aber versäumt, die Fehlkuvertierungen auch tatsächlich auszusortieren. Sie wurden geschult, damit sich ähnliche Vorfälle nicht wiederholen.

Fehler bei der Kuvertierung bei Banken gefährden nicht nur die Datensicherheit, sondern können auch das Bankgeheimnis verletzen.

13.1.4 Vorsicht bei Online-Bonitätsprüfungen!

Nach einer Bestellung in einem Online-Shop erhielt ein Bürger von einer Auskunftsei die Mitteilung, dass seine personenbezogenen Daten bei ihr gespeichert seien. Der Betroffene konnte sich jedoch nicht erinnern, dass ihn der Online-Shop für diese Abfrage bei der Auskunftsei um eine Einwilligung gebeten oder ihn informiert hatte.

Der Kauf auf Rechnung ist bei Geschäften im Internet sehr beliebt. Um dabei das Ausfallrisiko zu minimieren, setzen Online-Shops Bonitätsprüfungen ein. Häufig sind bereits die angezeigten Auswahlmöglichkeiten für die Zahlungsarten (Vorkasse, Nachnahme, PayPal oder auf Rechnung) das Ergebnis einer durchgeführten Bonitätsprüfung, ohne dass die bestellende Person in diese Bonitätsabfrage bei einer Auskunftsei einwilligt oder sie über diese Abfrage ausreichend informiert wird. Das Verfahren der Online-Bonitätsprüfungen kann auf zwei Arten datenschutzkonform gestaltet werden:

1. Soll bereits das Angebot der Zahlungsart von der Bonität der bestellenden Person abhängig sein, so muss eine Einwilligung eingeholt werden, und zwar bevor mit der Datenübermittlung an eine Auskunftsei begonnen wird.¹⁸⁰ Inhalt und Umfang der Einwilligung müssen genau bezeichnet werden. Die Einwilligung muss über eine Check-Box eingeholt und protokolliert werden.
2. Die bestellende Person wählt zunächst aus den ohne Einschränkung angezeigten Zahlungsarten die gewünschte aus und schließt den Kaufvorgang ab. Soweit nicht die Bezahlung per Vorkasse, Nachnahme oder PayPal ausgewählt wird, trägt der Online-Shop bei diesem Kauf das kreditorische Risiko, da er die Ware vor Zahlung liefert. In diesem Fall darf die Bonitätsprüfung ohne

¹⁸⁰ § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist nicht anwendbar, da zu diesem Zeitpunkt kein berechtigtes Interesse vorliegt, zumal unklar ist, ob die Bestellung überhaupt vorgenommen wird.

Einwilligung durchgeführt werden, soweit über das Verfahren transparent aufgeklärt wird.

Bonitätsprüfungen dürfen auch bei Internetgeschäften nicht heimlich erfolgen. Abhängig von der Gestaltung des Bestellprozesses ist entweder die Einwilligung einzuholen oder die Bonitätsabfrage erst bei einem kreditrisikoreichen Risiko vorzunehmen.

13.2 Industrie- und Handelskammer

13.2.1 IHK als Adresshändler

Der Gesetzgeber hat den Industrie- und Handelskammern das Recht eingeräumt, mit den personenbezogenen Daten der Kammerzugehörigen zur Förderung des Wirtschaftsverkehrs Adresshandel zu betreiben.¹⁸¹ Kammerzugehörige wurden vor dem ersten Adressverkauf von der IHK Berlin schriftlich darauf hingewiesen, dass sie der Übermittlung ihrer Daten widersprechen können. Der Hinweis lautete:

„Datenweitergabe

Die IHK Berlin darf Ihren Namen, Ihre Gewerbeanschrift und Ihren Wirtschaftszweig zur Förderung von Geschäftskontakten und zu anderen dem Wirtschaftsverkehr dienenden Zwecken an nicht-öffentliche Stellen übermitteln.

Wenn Sie mit der Übermittlung Ihrer Daten nicht einverstanden sind, teilen Sie uns das bitte umgehend mit.

○ *Mit der Weitergabe meiner Daten bin ich nicht einverstanden.“*

Die IHK Berlin übermittelte aber nicht nur die in dem Hinweis erwähnten Daten, sondern noch weitere, wie etwa Beschäftigtengrößenklassen, Gründungsdatum, Umsätze, Festnetznummer, Fax, E-Mail und Homepage.

¹⁸¹ § 9 Abs. 4 Satz 1-3 Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHK-G)

Industrie- und Handelskammern sind verpflichtet, Kammerzugehörige vor der ersten Übermittlung schriftlich auf ihr Recht auf Widerspruch gegen den Adresshandel durch die IHK hinzuweisen, sofern sich der Datensatz nicht auf Namen, Firma, Anschrift und Wirtschaftszweig beschränkt. Diese Pflicht hat die IHK Berlin verletzt, weil sie nur auf einen Teil der übermittelten Daten – auf „Trivialdaten“ – hingewiesen hat. Deshalb werden viele Kammerzugehörige auf die Einlegung eines Widerspruchs verzichtet haben. Aufgrund des fehlerhaften Hinweises hat die IHK Berlin seit vielen Jahren rechtswidrig Adresshandel betrieben.

Wir haben die IHK Berlin über den Fehler informiert. Sie hat schnell reagiert und sämtliche Unternehmen, von denen sie zukünftig Daten übermitteln will, einen neuen Widerspruchshinweis mit den tatsächlich betroffenen Daten zugeleitet. Es handelte sich um ca. 65.000 Mitglieder.

Durch den fehlerhaften Hinweis zum Widerspruchsrecht war der Adresshandel der IHK Berlin über viele Jahre rechtswidrig. Der Missstand ist jetzt behoben.

13.2.2 Überprüfung der Wahlvorschläge für die IHK-Vollversammlung

Bei einer Vollversammlungswahl einer IHK haben neben IHK-Angehörigen und im Handelsregister eingetragenen Prokuristen auch besonders bestellte Bevollmächtigte von IHK-Zugehörigen das passive Wahlrecht. Der Wahlausschuss für die Vollversammlungswahl der IHK Berlin befürchtete, dass einige der eingereichten Wahlvorschläge zweifelhaft waren, da die Kandidatinnen und Kandidaten nicht den Anforderungen an Rolle und Funktion der besonders bestellten Bevollmächtigten entsprachen. Um Missbräuche – insbesondere auch von IHK-Kritikern – zu vermeiden, mussten alle besonders bestellten Bevollmächtigten, die an der Wahl 2012 teilnehmen wollten, einen umfangreichen Fragebogen ausfüllen. Gefragt wurde u. a. nach der inhaltlichen Funktion, dem zeitlichen Umfang der Tätigkeit, dem Beststellungszeitpunkt und der Darstel-

lung der Eigenverantwortung auch anhand von Beispielen. Außerdem enthielt der Fragebogen Angaben zur Budget- und Personalverantwortung. Schließlich mussten auch Angaben erfolgen, warum sie oder er nicht zur Prokuristin oder zum Prokuristen bzw. zur Geschäftsführerin oder zum Geschäftsführer bestellt wurde. Ein abgelehnter Kandidat hat sich bei uns über das Verfahren beschwert.

Weder das IHK-Gesetz noch die Wahlordnung der IHK Berlin enthalten eine Legaldefinition für den Begriff des „besonders bestellten Bevollmächtigten von IHK-Zugehörigen“. Kriterien sind die leitende Stellung, die unternehmerische Tätigkeit und die Vertretungsmacht für das kammerzugehörige Unternehmen. Wir haben der IHK empfohlen, zur Erhöhung der Rechtssicherheit in der Wahlordnung der IHK Berlin den Begriff „des besonders bestellten Bevollmächtigten“ zu definieren.

Nach der Wahlordnung prüft der Wahlausschuss die Wahlvorschläge.¹⁸² Die Wahlordnung sieht allerdings nur vor, dass der Wahlausschuss Identitäts- und Authentizitätsnachweise verlangen kann, regelt aber nicht, welche Daten der Wahlausschuss für seine Prüfung erheben kann. Die IHK sollte dies in ihrer Wahlordnung regeln.

Das Recht des Wahlausschusses, auch mit Hilfe eines Fragebogens Wahlvorschläge zu überprüfen, ist unstrittig. Allerdings war der verwendete Fragebogen teilweise unverhältnismäßig. Für die Frage, ob die Bewerberin oder der Bewerber die Voraussetzungen der oder des besonders bestellten Bevollmächtigten erfüllt, ist der Zeitpunkt der Kandidatur maßgeblich. Denkbar ist daher sogar, dass die bewerbende Person ihre Tätigkeit erst am Tag der Wahlbewerbung aufnimmt. Die Frage nach dem Bestellungsbeginn ist somit ebenso überflüssig wie die Frage nach Beispielen, die die leitende Stellung belegen. Das gilt erst recht für die Frage, warum sie oder er nicht zur Prokuristin oder zum Prokuristen bzw. zur Geschäftsführerin oder zum Geschäftsführer bestellt wurde.

Wir haben der IHK empfohlen, zukünftig aus Gründen der Datensparsamkeit ein zweiphasiges Prüfkonzept anzuwenden. In der ersten Phase sollte lediglich ein vom Umfang und der Detailtiefe „dünnere“ Fragebogen verwendet wer-

182 § 11 Abs. 4 Satz 1 Wahlordnung der IHK Berlin

den. Erst bei Unklarheiten über die Person der Kandidatin oder des Kandidaten und der Qualifikation als besonders bevollmächtigte Person könnten in einer zweiten Phase durch spezielle Nachfragen (mündlich oder schriftlich) Zweifel beseitigt werden.

Durch Ergänzungen der Wahlordnung und Anwendung des Grundsatzes der Datensparsamkeit sollte die IHK Berlin das informationelle Selbstbestimmungsrecht der Wahlkandidatinnen und -kandidaten besser schützen.

13.3 „fragdenstaat.de“ – jetzt datenschutzgerecht

Der Verein Open Knowledge Foundation unterstützt Bürgerinnen und Bürger bei Anträgen nach dem Informationsfreiheitsgesetz mit dem Internetportal „fragdenstaat.de“. Die Anfragen und Antworten werden dokumentiert und auf dem Portal einer breiten Öffentlichkeit zugänglich gemacht. Bei einer Durchsicht des Portals fiel uns auf, dass bei einigen Antworten personenbezogene Daten der Anfragenden nicht geschwärzt waren, obwohl der Verein darauf hinwies, dass die Adressen der Anfragenden auf keinen Fall veröffentlicht würden. Es war unklar, ob in diesen Fällen eine Einwilligung zur Veröffentlichung der personenbezogenen Daten vorlag.

Webseitenbetreiber haben dafür zu sorgen, dass personenbezogene Daten nur veröffentlicht werden, wenn die Betroffenen eingewilligt haben oder die Veröffentlichung auf eine Rechtsgrundlage gestützt werden kann. Ansonsten ist die Veröffentlichung rechtswidrig.¹⁸³ Der Verein hat aufgrund unserer Bitte um Stellungnahme alle Dokumente auf ungewollte Veröffentlichungen hin überprüft und bereinigt. Außerdem hat er das Verfahren so geändert, dass es zukünftig nicht mehr zu ungewollten Veröffentlichungen von personenbezogenen Daten kommen sollte. Die jeweiligen Dokumente können zunächst nur die Nutzerinnen und Nutzer selbst einsehen. Diese entscheiden darüber, ob sie das Dokument auf der Webseite veröffentlichen wollen. Soweit personenbezogene

183 § 4 Abs. 1 BDSG

Daten auf die Webseite eingestellt werden sollen, holt der Verein eine ausdrückliche Zustimmung der Betroffenen ein. Auf diese Weise unterstützt das Portal „fragdenstaat.de“ jetzt in datenschutzgerechter Weise Menschen, die ihr Recht auf Informationsfreiheit ausüben wollen.

Vor der Veröffentlichung von Informationen auf Webseiten ist sorgfältig zu prüfen, ob auch personenbezogene Daten eingestellt werden sollen. Ist dies der Fall, so muss sichergestellt sein, dass es nicht zu unbefugten Datenübermittlungen kommt.

13.4 Festplatten-Crash – Was passiert mit den Daten bei der Reparatur?

Ein Rechtsanwalt brachte sein defektes Notebook zur Reparatur. Der Reparaturbetrieb stellte fest, dass die Festplatte einen irreparablen Schaden aufwies, und tauschte sie durch eine neue aus. Dem Rechtsanwalt teilte das Unternehmen mit, dass es die defekte Festplatte im Rahmen der Garantieverlängerung, wie in den Versicherungsbedingungen festgelegt, an den Versicherer übergeben habe, da die defekte Festplatte in dessen Eigentum übergegangen sei.

Der Versicherungsvertrag enthielt lediglich einen Hinweis auf die zivilrechtliche Eigentumsübertragung der Festplatte. Auf unsere Aufforderung hin hat das Unternehmen mit dem Versicherer der Garantieleistung die Versicherungsbedingungen so geändert, dass folgende Grundsätze beachtet und gegenüber den Betroffenen transparent gemacht werden:

Grundsätzlich sollte die Kundin oder der Kunde schon vor der Auftragserteilung selbst dafür sorgen, dass Daten auf den zu reparierenden Datenträgern gelöscht oder gesichert werden. Ist eine Datensicherung aufgrund des Defektes nicht möglich und erhält der Reparaturdienst einen Hinweis, dass auf dem Datenträger personenbezogene Daten gespeichert sind, so muss der Reparaturdienst bei einem Austausch des defekten Datenträgers dafür sorgen, dass die Daten auf dem alten Datenträger gelöscht werden. Sind auf dem defekten

Datenträger Daten gespeichert, die einer besonderen Schweigepflicht unterliegen (z. B. bei Ärzten und Rechtsanwälten),¹⁸⁴ sollte die Löschung dieser Daten beim Reparaturdienst in Anwesenheit der Kundin oder des Kunden so erfolgen, dass diese Daten nicht zur Kenntnis genommen werden können.

Der Reparaturbetrieb hat dem Petenten inzwischen eine Bestätigung über die Vernichtung des Datenträgers zugesandt.

Hinweise auf den Eigentumsübergang bei Reparaturen sind datenschutzrechtlich irrelevant. Der Reparaturbetrieb hat Vorsorge dafür zu treffen, dass personenbezogene Daten auf defekten Geräten nicht unbefugt in die Hände des Versicherers gelangen.

13.5 Video- und Kameraeinsatz zu künstlerischen und werbewirksamen Zwecken

Öffentliche Live-Aufführungen von Konzerten oder Theaterstücken werden von verantwortlichen Stellen immer häufiger aufgezeichnet. Bei diesen Aufnahmen kann es vorkommen, dass nicht nur die Bühne, auf der sich das Geschehen abspielt, sondern auch das Publikum im Erfassungsbereich der Kameras liegt. Dabei können personenbezogene Daten erhoben werden, wenn einzelne Personen im Publikum erkennbar und identifizierbar sind. Diese Datenerhebung in Form von Bild- und Tonaufnahmen ist nach Bundesdatenschutzgesetz (BDSG) zu bewerten.

§ 6b BDSG nennt die Voraussetzungen, nach denen die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) zulässig ist. Allerdings ist es zweifelhaft, ob es sich z. B. bei einem Konzertmitschnitt tatsächlich um eine „Überwachung“ im wörtlichen Sinne handelt. Insofern liegt die Anwendbarkeit von § 28 BDSG näher, der die Zulässigkeitsvoraussetzungen der Datenerhebung, -verarbeitung und -nutzung für

184 § 203 StGB

eigene Zwecke im Allgemeinen benennt, unabhängig von der Art und Weise der Erhebung.

In der Regel dienen Bild- und Tonaufnahmen in erster Linie dem Zweck, die Stimmung und Atmosphäre auf der Bühne und im Publikum einzufangen und anschließend im Internet zu veröffentlichen. Unter der Voraussetzung, dass die verantwortlichen Stellen die Urheber- und Nutzungsrechte an den Aufnahmen haben, ist dieses Vorgehen nicht zu beanstanden. Durch die Veröffentlichung z. B. auf einem Videoportal im Internet sind die Aufnahmen allgemein zugänglich. Die Datenerhebung in Form von Bild- und Tonaufnahmen kann als Werbekampagne angesehen werden, um eine musikalische Darbietung oder ein Theaterstück bekannter zu machen und die Popularität zu steigern. Im Erfassungsbereich der aufzeichnenden Kameras während einer Aufführung liegt hauptsächlich die Bühne. Selbst wenn bei mehreren Kameraschwenks über die Köpfe des Publikums teilweise Einzelpersonen erkennbar sind, stehen diese weder im Fokus noch sind sie der primäre Zweck der Aufzeichnungen; sie sind nur als „Beiwerk“ zu betrachten.¹⁸⁵

Im Ergebnis ist daher festzustellen, dass nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG im Fall einer Datenerhebung durch Bild- und Tonaufnahmen die schutzwürdigen Interessen der betroffenen Konzertbesucher hinter den berechtigten Interessen der verantwortlichen Stelle zurückstehen.

Wenn Bild- und Tonaufnahmen von öffentlichen Aufführungen gemacht werden, bei denen das Publikum nicht im Fokus steht und Einzelpersonen nicht identifizierbar sind, ist diese Art der Datenerhebung nach § 28 BDSG zulässig.

185 § 23 Abs. 1 Nr. 2 Kunsturhebergesetz

13.6 Aus der Arbeit der Sanktionsstelle

Eine Datenschutzaufsicht arbeitet nur dann effektiv, wenn datenschutzrechtliche Verstöße nicht ungeahndet bleiben, sondern die vom Gesetzgeber bereitgestellten Instrumentarien genutzt werden. In den sieben von uns eingeleiteten Ordnungswidrigkeitenverfahren haben wir Bußgeld- oder Verwarnungsbescheide erlassen und Geldbußen von insgesamt 7.735 Euro festgesetzt. In sechs Fällen haben wir einen Strafantrag gestellt.

Beispielsweise kam es bei zwei Unternehmen zur ungewollten Veröffentlichung von Bewerberdaten im Internet. Unbefugte Veröffentlichungen im Internet stellen eine rechtswidrige Datenübermittlung dar, die bei vorsätzlichem Handeln mit einer Geldbuße von bis zu 300.000 Euro und bei Fahrlässigkeit mit einer Geldbuße von bis zu 150.000 Euro geahndet werden kann.¹⁸⁶ Unternehmen sind zu einem sorgsamem Umgang mit personenbezogenen Daten verpflichtet. Auch ungewollte Datenschutzverstöße können mit hohen Strafen geahndet werden.

In einem anderen Fall veranlasste ein Rechtsanwalt eine Mitarbeiterin eines ihm gut bekannten Wohnungsunternehmens zu einer Bonitätsdatenabfrage bei einer Auskunft. Anschließend verwendete er die Daten in dem für seinen Mandanten geführten Zivilprozess gegen die gegnerische Partei. Die Bonitätsabfrage konnte auf keine Einwilligung oder Rechtsgrundlage gestützt werden. Zwischen dem Wohnungsunternehmen und den Betroffenen bestand keine Vertragsbeziehung und damit auch kein berechtigtes Interesse am Erhalt dieser Auskünfte. Die Mitarbeiterin des Wohnungsunternehmens gab gegenüber der Auskunft den Abfragegrund unrichtig mit „Wohnraumvermietung“ an und erschlich sich so personenbezogene Daten der Betroffenen.¹⁸⁷ Da der Rechtsanwalt diese Abfrage veranlasst hatte, war er selbst an der Ordnungswidrigkeit beteiligt.¹⁸⁸ Wir haben ein Bußgeld in vierstelliger Höhe festgesetzt.

Nicht für alle Datenschutzverstöße hat der Gesetzgeber einen Bußgeldtatbestand vorgesehen. Wenn die verantwortliche Stelle den Verstoß nicht besei-

186 § 43 Abs. 2 Nr. 1 BDSG, § 17 Abs. 2 OWiG

187 § 43 Abs. 2 Nr. 4 BDSG

188 § 14 OWiG

tigt, können wir Maßnahmen zur Beseitigung anordnen.¹⁸⁹ Hiervon haben wir in drei Fällen Gebrauch gemacht. So wurde eine Anordnung erlassen, weil ein Unternehmen innerhalb von telefonischen Zufriedenheitsnachfragen standardisiert Einwilligungen in Werbung per Telefon, E-Mail oder SMS abgefragt hat, obwohl die Kundinnen und Kunden beim Vertragsabschluss nicht in eine Ansprache per Telefon eingewilligt hatten. Die telefonischen Zufriedenheitsnachfragen waren nach unserer Auffassung lediglich ein Vorwand, um eine Einwilligung in weitere Werbeformen zu erhalten. Dies wurde schon daran deutlich, dass der Gesprächsleitfaden keine Dokumentation der Kundenbeschwerden vorsah. In einem anderen Fall haben wir von einem Sportverein verlangt, die in den Clubräumen installierten Videokameras zu entfernen. Gegen beide Anordnungen ist Klage vor dem Verwaltungsgericht erhoben worden.

Datenschutzverstöße können auch bei fahrlässigem Handeln mit hohen Bußgeldern geahndet werden. Unternehmen haben daher Maßnahmen zu ergreifen, um solche Verstöße zu verhindern.

189 § 38 Abs. 5 BDSG

14 Europäischer und internationaler Datenschutz

14.1 Neuer europäischer Rechtsrahmen

Im Januar hat die Europäische Kommission den Entwurf eines neuen Rechtsrahmens¹⁹⁰ vorgestellt, der zu den umfassendsten gesetzgeberischen Novellierungsbestrebungen auf EU-Ebene zählt und einen Gesetzgebungsauftrag des Vertrags von Lissabon umsetzen soll.¹⁹¹ Erster Teil des Reformpakets ist der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (**Datenschutz-Grundverordnung**).¹⁹² Der zweite Teil beinhaltet den Vorschlag für eine **Richtlinie über die justizielle und polizeiliche Zusammenarbeit**.¹⁹³ Mit dieser Reform soll die bislang geltende Europäische Datenschutzrichtlinie 95/46/EG von 1995 ebenso ersetzt werden wie der Rahmenbeschluss des Rates¹⁹⁴ von 2008, der bislang den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen regelt. Die Kommission strebt mit der Grundverordnung eine Vollharmonisierung im Bereich des Datenschutzes an und begründet dies u. a. damit, dass die bisherigen Regelungen angesichts des Ausmaßes der Datenverarbeitung insbesondere in der digitalen Welt nicht mehr zeitgemäß seien.¹⁹⁵ Für die Bereiche Polizei und Justiz hat die Kommission eine Vollharmonisierung nicht für durchsetzbar

190 Siehe schon JB 2011, 10.1

191 Art. 16 Vertrag über die Arbeitsweise der Europäischen Union

192 KOM(2012) 11 endg. vom 25. Januar 2012

193 KOM(2012) 10 endg. vom 25. Januar 2012: Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

194 Rahmenbeschluss 2008/977/JI vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30. Dezember 2008, S. 60)

195 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 25. Januar 2012, KOM(2012) 9 endg.: Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, Ziff. 2.

gehalten und sich deshalb auf eine Richtlinie beschränkt. Nach den Vorstellungen der für den Entwurf verantwortlichen Vizepräsidentin und Justizkommissarin Viviane Reding soll der neue Rechtsrahmen den Datenschutz europaweit in den nächsten 30 Jahren festlegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies in zwei Entschlüssen verdeutlicht¹⁹⁶ und in umfassenden Stellungnahmen¹⁹⁷ eine Vielzahl von Einzelaspekten bei der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtsetzungsprozess ausgesprochen.¹⁹⁸ Kernaussagen der Konferenz beziehen sich auf die sog. delegierten Rechtsakte, technische und organisatorische Maßnahmen, die Profilbildung, den sog. One-Stop-Shop und das Kohärenzverfahren¹⁹⁹ sowie auf die Grundsätze der Datenverarbeitung, die schutzbedürftigen Datenkategorien und die Betroffenenrechte.²⁰⁰

Die Meinungen innerhalb der Europäischen Union, ob künftig ein einheitliches Datenschutzregime (also eine unmittelbar anwendbare EU-Verordnung) in allen Mitgliedstaaten gelten soll, gehen auseinander. Zu den prinzipiellen Befürwortern gehören neben der Bundesrepublik auch Bulgarien, Frankreich, Griechenland, Irland, Italien, Luxemburg, die Niederlande und Spanien. Die Gegner dieser Ansicht bevorzugen eine neue europäische Richtlinie für alle Bereiche, die durch nationale Gesetzgebung umzusetzen ist. Dazu gehören Belgien, Dänemark, Großbritannien, Schweden, Slowenien und Ungarn. Uneinigkeit herrscht auch bei der Frage, ob die Grundverordnung – wie bisher die Datenschutzrichtlinie von 1995 – die Datenverarbeitung im öffentlichen

196 Entschließung vom 21./22. März 2012: Ein hohes Datenschutzniveau für ganz Europa!, siehe Dokumentenband 2012, S. 10 ; Entschließung vom 7./8. November 2012: Europäische Datenschutzreform konstruktiv und zügig voranbringen!, siehe Dokumentenband 2012, S. 19

197 Stellungnahmen zu den Entwürfen der Grundverordnung sowie der Richtlinie vom 11. Juni 2012, beide abrufbar über das Internet-Angebot der Konferenzvorsitzenden, der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg: www.lda.brandenburg.de/cms/detail.php/bb1.c.299089.de

198 Siehe auch Einleitung sowie 2.2

199 Kernpunkte der Stellungnahme vom 11. Juni 2012 zum Entwurf der Datenschutz-Grundverordnung, siehe www.lda.brandenburg.de/cms/detail.php/bb1.c.299089.de

200 Ebenda

Bereich erfassen soll (soweit nicht Polizei und Justiz betroffen sind, die unter die neue Richtlinie fallen). Eine Ausklammerung des öffentlichen Bereichs aus der Grundverordnung wäre ein massiver Rückschritt gegenüber dem bisherigen EU-Recht. Allerdings muss in der Verordnung sichergestellt werden, dass das geltende deutsche Recht z. B. für den Sozialdatenschutz, aber auch die Landesdatenschutzgesetze weitergelten. Die Rechtsangleichung in Europa darf nicht zu einer Absenkung des gegenwärtigen Datenschutzniveaus nach Art eines „race to the bottom“ führen. Der Kommissionsvorschlag für eine Richtlinie zum Datenschutz bei Polizei und Justiz enthält nach Einschätzung des Europäischen Datenschutzbeauftragten unannehmbar schwache Regelungen und bleibt weit hinter der Grundverordnung zurück. Selbst gegen diesen schwachen Entwurf gibt es bei den Regierungen der Mitgliedstaaten noch stärkere Vorbehalte als gegen die Grundverordnung. Die Beratungen des Reformpakets im Europäischen Parlament und im Rat sind in vollem Gange und müssen bis zum Sommer 2013 (dem Ende der irischen Ratspräsidentschaft) abgeschlossen sein, wenn die Novelle Chancen haben soll, noch vor den Europawahlen im Juni 2014 verabschiedet zu werden. Das Europäische Parlament muss sich mit den im Rat vertretenen Regierungen der Mitgliedstaaten und der Kommission in derzeitigen Verhandlungen (Trilog) verständigen, bevor das Reformpaket in Kraft treten kann.

14.2 Weitere Ergebnisse aus Brüssel

Im Juli ist das neue Abkommen zur **Übermittlung von Fluggastdaten (Passenger Name Records – PNR) in die USA**²⁰¹ in Kraft getreten, nachdem das Europäische Parlament ihm mehrheitlich zugestimmt hatte. Damit dürfen Informationen über jeden EU-Passagier erhoben werden, auf die die US-Behörden zuzugreifen, wenn ein Verdacht wegen terroristischer Handlungen oder anderer schwerer Verbrechen vorliegt.²⁰² Das soll nun auch Standard in Europa werden, denn die EU-Innenminister haben sich über ein vergleichbares System verständigt und beschlossen, die Daten sämtlicher Fluggäste auf Vorrat für fünf Jahre zu speichern, und zwar nicht nur zu Flügen aus Drittstaaten in die EU,

201 KOM(2011) 807 endg. vom 23. November 2011

202 Siehe zuletzt JB 2011, 10.1 (S. 157)

sondern auch zu Flügen innerhalb der EU.²⁰³ Dazu müssen die Mitgliedstaaten eine PNR-Zentralstelle einrichten, die die Daten entgegennimmt und verwaltet. Dies wäre ein weiterer Schritt zur lückenlosen Überwachung alltäglichen Verhaltens und dürfte den Vorgaben des Bundesverfassungsgerichts von 2010 im Zusammenhang mit der Vorratsdatenspeicherung zuwiderlaufen.²⁰⁴ Danach darf die Freiheitswahrnehmung der Menschen nicht total erfasst und registriert werden. Dennoch hat die Bundesregierung sich bei der Abstimmung im Europäischen Rat lediglich der Stimme enthalten, statt – entsprechend der deutschen Verfassungsrechtsprechung – gegen die Richtlinie zu stimmen.

Die **Art. 29-Datenschutzgruppe**, in der wir die Bundesländer vertreten und die nach den Reformvorschlägen der Kommission künftig als Europäischer Datenschutzausschuss verstärkt koordinierend wirken soll, hat wieder mehrere Papiere verabschiedet. Vorrangig hat sie sich mit den Vorschlägen zum neuen Rechtsrahmen befasst und zwei umfangreiche Stellungnahmen veröffentlicht.²⁰⁵ Daneben hat sie eine Orientierungshilfe zu Datenschutzfragen beim Pilotprojekt epSOS erstellt, das Menschen in der EU grenzüberschreitende elektronische Gesundheitsdienste anbietet.²⁰⁶ Ein Papier befasst sich mit der Gesichtserkennung bei Online- und Mobilfunkdiensten; diese Technologie war einst Science Fiction, wird mittlerweile aber gängig z. B. in sozialen Netzwerken und bei Smartphones verwendet.²⁰⁷ Weitergehend hat sich die Datenschutzgruppe in einem Grundsatzpapier mit den Entwicklungen im Bereich biometrischer Technologien auseinandergesetzt.²⁰⁸ Anlässlich der Neufassung der sog. e-Privacy-Richtlinie²⁰⁹ wurde analysiert, bei welcher Art von verwendeten Cookies

203 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität, KOM(2011) 32 endg. vom 2. Februar 2011

204 Urteil vom 2. März 2010, abgedruckt in NJW 2010, S. 833 ff.; siehe auch JB 2010, 13.1

205 Stellungnahme 1/2012 zu den Reformvorschlägen im Bereich des Datenschutzes vom 23. März 2012 (WP 191); Stellungnahme 8/2012 mit weiteren Beiträgen zur Diskussion der Datenschutzreform vom 5. Oktober 2012 (WP 199)

206 Arbeitspapier 1/2012 zu epSOS vom 25. Januar 2012 (WP 189)

207 Stellungnahme 2/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten vom 22. März 2012 (WP 192), siehe Dokumentenband 2012, S. 63

208 Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien vom 27. April 2012 (WP 193), siehe Dokumentenband 2012, S. 76

209 Richtlinie 2009/136/EG (auch „Cookie-Richtlinie“ genannt)

eine Einwilligung der Nutzenden nicht erforderlich ist.²¹⁰ Zudem wurden erstmals Grundsätze für bindende Unternehmensregeln im Fall der Auftragsdatenverarbeitung formuliert.²¹¹ Schließlich hat die Art. 29-Gruppe ein Grundsatzpapier zum **Cloud Computing** verfasst,²¹² in das auch die Erkenntnisse aus der Orientierungshilfe Eingang gefunden haben, die im letzten Jahr von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und dem Düsseldorf-Kreis verabschiedet worden war.²¹³

Die Art. 29-Gruppe hat darüber hinaus eine spezielle Anwendung des Cloud Computing analysiert, nämlich das Produkt „Office 365“ von Microsoft. Der US-Konzern bietet damit die Dienstleistung an, personenbezogene Daten mit Microsoft-Anwendungen (z. B. Office, E-Mail und Kalender sowie Kollaborationsanwendungen) in der Cloud zu verarbeiten. Dazu betreibt das Unternehmen ein globales Netzwerk mit Rechenzentren. Datenschutzrechtlich stehen Verträge zur Auftragsdatenverarbeitung im Raum, die die Nutzer des Angebots als Auftraggeber mit Microsoft als Auftragnehmer abschließen müssen, wenn sie den Dienst nutzen wollen. Microsoft schaltet die Rechenzentren wiederum als Unterauftragnehmer ein. Dabei stellen sich, wie so häufig im Zusammenhang mit dem Cloud Computing,²¹⁴ auch Fragen der Zulässigkeit von Datenübermittlungen in sog. unsichere Drittstaaten, d. h. in Staaten außerhalb des EWR ohne angemessenen Datenschutz. Voraussetzung für die Datenübermittlung ist hier, dass bei dem Empfänger im Drittstaat ausreichende Datenschutzgarantien geschaffen werden. Das kann bei der Auftragsdatenverarbeitung dadurch erreicht werden, dass der Auftraggeber mit dem Auftragnehmer im Drittstaat einen Vertrag über die erforderlichen Datenschutzpflichten schließt. Die Europäische Kommission hat zu diesem Zweck sog. Standardvertragsklauseln²¹⁵ anerkannt, die, wenn sie ohne Änderungen vom Auftraggeber und Auftragnehmer genutzt werden, eine Datenübermittlung in den Drittstaat ermög-

210 Stellungnahme 4/2012 zur Ausnahme von Cookies von der Einwilligungspflicht vom 7. Juni 2012 (WP 194)

211 Arbeitsdokument 2/2012 vom 6. Juni 2012 mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter (WP 195)

212 Stellungnahme 5/2012 zum Cloud Computing vom 1. Juli 2012 (WP 196), siehe Dokumentenband 2012, S. 129 ; siehe auch 16.7 zum Sopot-Memorandum der „Berlin Group“

213 JB 2011, 2.1.1

214 JB 2011, 2.1.1

215 Beschluss 2010/87/EU vom 5. Februar 2010, siehe Dokumentenband 2010, S. 70

lichen, ohne dass es zusätzlich einer Genehmigung der Datentransfers durch die zuständige Aufsichtsbehörde bedürfte.²¹⁶ Diese Standardvertragsklauseln sehen speziell die Einschaltung von Subunternehmern vor.²¹⁷

Microsoft hat für den Drittstaatentransfer im Zusammenhang mit „Office 365“-Dienstleistungen ein Vertragswerk entwickelt und sich damit an verschiedene Datenschutzbehörden in Europa gewandt. Aufgrund der Vielzahl der möglichen Betroffenen in ganz Europa leitete die Art. 29-Datenschutzgruppe eine koordinierte Beurteilung des Vertragswerks ein. Sie kam zu dem Ergebnis, dass das Vertragswerk erheblich von den Standardvertragsklauseln der Europäischen Kommission abweicht und somit genehmigungsbedürftig ist. Auch seien die Abweichungen so gravierend in ihrer Wirkung für die Rechte und schutzwürdigen Interessen der Betroffenen, dass Datenübermittlungen auf der Grundlage dieses Vertragswerks nicht genehmigungsfähig seien. Die Art. 29-Gruppe hat ihre Anmerkungen und Änderungsanforderungen im Oktober in einem Brief an Microsoft formuliert. Darin kritisierte sie auch, dass das Vertragswerk nur unzureichende Informationspflichten gegenüber den Nutzern (Auftraggebern) vorsieht für den Fall, dass der Auftragnehmer (Microsoft) durch gesetzliche Vorgaben im Drittstaat verpflichtet ist, Daten gegenüber Dritten (wie Sicherheitsbehörden) zu offenbaren. Schließlich wurde beanstandet, dass die Bedingung für die Vergabe von Unteraufträgen nicht bestimmt genug ist und es an Transparenz für die Auftraggeber fehlt. Die Art. 29-Gruppe legte Microsoft nahe, den Vertragstext so zu formulieren, dass er den Standardvertragsklauseln entspricht. Eine Antwort steht noch aus.

216 § 4c Abs. 2 BDSG

217 JB 2010, 11.1

15 Datenschutzmanagement

15.1 Bundesweite Premiere: Anerkennung von Verhaltensregeln nach dem BDSG

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat uns „Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft“ vorgelegt.²¹⁸ Diese waren zuvor in mehrjährigen Verhandlungen mit den Datenschutzaufsichtsbehörden abgestimmt worden. Im November haben wir dem GDV beschieden, dass dieser Verhaltenskodex mit dem geltenden Datenschutzrecht vereinbar ist.²¹⁹

Nach dem BDSG können Berufsverbände und andere Vereinigungen den zuständigen Aufsichtsbehörden Entwürfe für Verhaltensregeln unterbreiten, die die Durchführung der Datenschutzgesetze fördern (sog. Mehrwert). Die Aufsichtsbehörde prüft, ob die Verhaltensregeln mit dem Datenschutzrecht vereinbar sind. Diese Prüfung und die Kontrolle der Einhaltung der Regeln verbleiben in staatlicher Hand. Sie ersetzen nicht das geltende Recht; im Zweifel gelten die gesetzlichen Vorgaben. Dieses Konzept der sog. regulierten Selbstregulierung konnte bisher nicht mit Leben gefüllt werden. Die wenigen Versuche, Verhaltensregeln zu entwerfen, scheiterten zumeist daran, dass im Wesentlichen der Gesetzestext abgebildet wurde. Ein Mehrwert für den Datenschutz kann aber nur dann entstehen, wenn die gesetzlichen Anforderungen für die branchentypischen Datenverarbeitungen konkretisiert werden und dadurch die Umsetzung dieser Anforderungen in der Branche erleichtert und verbessert wird. Nur dann können die Verhaltensregeln dazu verhelfen, dass die Verbandsmitglieder die Datenschutzgesetze durchgängig einhalten.

In der Versicherungswirtschaft wurden in der Vergangenheit unübersichtliche und weitreichende Einwilligungserklärungen eingesetzt. Häufig konnten die Betroffenen nicht freiwillig entscheiden, ob sie diese Einwilligungs- und Schweigepflichtenbindungserklärungen abgeben wollten, denn der Abschluss

218 Siehe Dokumentenband 2012, S. 37

219 Siehe § 38a BDSG

der gewünschten Versicherung war an die Abgabe der Einwilligung geknüpft.²²⁰ Nunmehr soll die Datenverarbeitung in der Versicherungswirtschaft mit Ausnahme der Verarbeitung von Gesundheitsdaten oder zu Werbezwecken nicht mehr auf die Einwilligung, sondern ausschließlich auf gesetzliche Erlaubnistatbestände gestützt werden. Die gesetzlichen Regelungen werden durch die Verhaltensregeln konkretisiert, die die wichtigsten Datenverarbeitungen in der Branche zusammenstellen und dafür einheitliche Vorgaben machen. Die Verhaltensregeln treffen u. a. Aussagen zu den Anforderungen an einen Datenaustausch mit anderen Versicherern oder in der Unternehmensgruppe, an das Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft, an die Datenübermittlung an Rückversicherer und an die Ausgliederung von Unternehmensfunktionen. Mit dem Beitritt zu den Verhaltensregeln verpflichten sich die Mitgliedsunternehmen des GDV zu ihrer Einhaltung.

Inwieweit der Verhaltenskodex tatsächlich zu einem verbesserten Datenschutz führt, hängt von der konsequenten Umsetzung durch die beigetretenen Mitgliedsunternehmen des GDV ab. In jedem Fall hat der langjährige Austausch zwischen den Datenschutzbehörden und der Versicherungswirtschaft dazu geführt, dass die Verhaltensregeln mehr Transparenz in die komplexen Datenflüsse der Branche bringen und einen Standard festlegen.

Die erhebliche Zeitspanne, die bis zur ersten Anerkennung eines Verhaltenskodexes verstrichen ist, seit der Bundesgesetzgeber 2001 diese Möglichkeit eröffnet hat, spricht nicht gegen das Konzept der regulierten Selbstregulierung. Sie ist zum einen auf die komplexen und sehr unterschiedlichen Datenverarbeitungsprozesse in den einzelnen Sparten der Versicherungswirtschaft, zum anderen aber auch darauf zurückzuführen, dass erstmals dieses neuartige Regelungsinstrument von allen Aufsichtsbehörden akzeptiert worden ist. Es ist durchaus möglich, dass andere Wirtschaftszweige dem Beispiel der Versicherungswirtschaft folgen und eigene Verhaltensregeln entwickeln werden. Das kann ein Gewinn für ein modernes Datenschutzsystem sein, solange Selbstregulierung nicht als möglicher Ersatz für staatliche Regulierung missverstanden wird.

220 JB 2011, 9.1.4

15.2 Informationspflicht bei Datenlecks in Wirtschaft und Verwaltung

Die Anzahl der Mitteilungen bei einer unrechtmäßigen Kenntnisnahme von personenbezogenen Daten durch Dritte ist insbesondere im nicht-öffentlichen Bereich deutlich gestiegen. Häufig machen die Unternehmen und öffentlichen Stellen zunächst „rein vorsorgliche“ Mitteilungen an uns, ohne auch gleichzeitig die Betroffenen zu benachrichtigen. Eine Beratung durch die Aufsichtsbehörde kann zwar hilfreich sein.²²¹ Die im Rahmen der Informationspflicht erforderliche Prognose, ob schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen, kann den meldenden Stellen von der Aufsichtsbehörde aber nicht abgenommen werden. Letztlich tragen sie die Verantwortung, dass bei einer Informationspflicht auch die Betroffenen „unverzüglich“ benachrichtigt und dadurch ggf. Schäden abgewendet werden.

Auffällig ist, dass die meldenden Stellen **bereichsspezifische Informationspflichten** häufig außer Acht lassen und nur die allgemeinen Vorschriften nach BDSG²²² oder BlnDSG²²³ prüfen. Die speziellen Informationspflichten nach § 83a Sozialgesetzbuch Zehntes Buch (SGB X), § 15a Telemediengesetz (TMG) und § 109a Telekommunikationsgesetz (TKG) treffen Sonderregeln für bestimmte Lebensbereiche. Die spezielle Informationspflicht im Sozialrecht richtet sich u. a. an Träger von Sozialleistungen und betrifft besondere Arten personenbezogener Daten.²²⁴ Die Informationspflicht des TMG bezieht sich auf den Bereich der Nutzung von Internetdienstleistungen und betrifft sämtliche Nutzungs- und Bestandsdaten, d. h. sie kann einschlägig sein, wenn E-Mail-Adressen oder Login-Daten abhandenkommen. Bei der Informationspflicht nach dem TKG ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu benachrichtigen. Eine solche Mitteilung kommt immer dann in

221 Siehe unsere FAQs zur Informationspflicht bei Datenlecks nach BDSG sowie BlnDSG, abrufbar unter www.datenschutz-berlin.de

222 § 42a BDSG

223 § 18a BlnDSG

224 Das sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben (siehe § 67 Abs. 12 SGB X).

Betracht, wenn Telekommunikationsanbieter den durch das TKG gewährten Schutz personenbezogener Daten verletzen.

Häufig werden Vorfälle im Zusammenhang mit der Bedienung von **Bürokommunikationsmitteln** gemeldet, so z. B. **Fehlsendungen per Fax**, die durch einen Faxnummernabgleich vor dem Versenden hätten vermieden werden können. Zudem wird uns öfter angezeigt, dass **E-Mails** versehentlich an einen offenen Verteiler versendet wurden, was aufgrund der komfortablen Kommunikationstechnik leicht passiert. Wenn dies im Umfeld von Parteien oder Gewerkschaften geschieht, können dadurch besonders schutzwürdige Arten personenbezogener Daten offenbart werden: Aus der Tatsache, dass eine bestimmte Person Empfängerin einer E-Mail ist, kann geschlossen werden, welche politische Einstellung diese Person hat oder ob sie einer Gewerkschaft angehört. Bevor E-Mail-Adressen in die „An“- oder „Kopie“-Zeile eingetragen werden, sollte gerade bei „sprechenden“ Adressen immer überprüft werden, ob sie jeweils den anderen Empfängern gegenüber offenbart werden dürfen. Ist dies nicht der Fall, müssen die E-Mail-Adressen entweder in die „Blindkopie“-Zeile gesetzt oder es muss die Funktion der Listenerstellung im E-Mail-Programm genutzt werden. Auch sollte stets geprüft werden, ob wirklich eine „Antwort an alle“ notwendig ist, bevor diese Funktion genutzt wird.

Immer wieder werden wir gefragt, ob die **Benachrichtigung** der Betroffenen auch **per Internet bzw. Intranet** erfolgen kann. Das Gesetz macht keine Formvorgaben, sodass die Benachrichtigung schriftlich, elektronisch oder mündlich erfolgen kann. Allerdings muss gewährleistet sein, dass sie die Betroffenen auch tatsächlich erreicht, denn die falsche, unvollständige oder verspätete Benachrichtigung ist bußgeldbewehrt. Wir haben in einem Fall die Benachrichtigung per Internet für ausreichend erachtet, in dem der Betroffenenkreis unüberschaubar war und es sich gleichzeitig um eine Personengruppe handelte, die täglich das Internet als primäres Informations- und Kommunikationsmittel nutzte. In einem anderen Fall hielten wir die Art der Benachrichtigung im Intranet für inakzeptabel, da die Mitteilung in der Informationsrubrik „Aktuelles“ innerhalb kurzer Zeit von der obersten Position durch aktuellere Nachrichten verdrängt wurde. Wir forderten, dass der Artikel mit aussagekräftiger Überschrift an prominenter Stelle im Intranet für mindestens einen Monat bestehen bleibt. Letztlich wurden die Betroffenen per Benachrichtigungsschreiben einzeln unterrichtet.

15.2.1 Datenpannen in der Wirtschaft

Patientenunterlagen im Keller

Aufgrund eines Hinweises aus der Bevölkerung fanden wir auf dem Gelände einer ehemaligen Klinik in den Kellerräumen der dort leer stehenden Gebäude Aktenordner, die u. a. personenbezogene Unterlagen zu Patienten enthielten. Darunter waren OP-Berichte, gynäkologische Gutachten, die Informationen zu Erwerbsminderungen, Vaterschaften, Kunstfehlern und Geschlechtsumwandlungen enthielten, sowie andere Untersuchungs- und Arztberichte zu Schwangerschaften (z. T. zu Schwangerschaftsverläufen von drogenabhängigen Frauen), Geburten und Aborten. Die stark verwahrlosten Gebäude waren offen zugänglich und wurden offensichtlich von Menschen genutzt. Jedenfalls waren die Aktenordner bewegt worden und lagen z. T. aufgeschlagen auf dem Boden. Soweit uns das bei der Sichtung vor Ort möglich war, stellten wir fest, dass die Unterlagen größtenteils aus den 1960er bis 1990er Jahren stammten. Die Klinik, die 1995 in den Räumlichkeiten ansässig war, existierte als solche nicht mehr. Rechtsnachfolgerin dieser Klinik sowie Rechtsnachfolgerin der Krankenhäuser, die z. T. als aktenführende Stellen aus den Akten hervorgingen, ist die Charité. Nachdem wir den Aktenfund dort mitgeteilt hatten, veranlasste das Krankenhaus unverzüglich die Räumung der Kellerräume und die Vernichtung der Patientenakten. Eine Benachrichtigung der Betroffenen erfolgte nicht.

Gerade im Gesundheitsbereich wiederholen sich solche Aktenfunde mit erschreckender Regelmäßigkeit.²²⁵ Die Charité hatte die Benachrichtigung der Betroffenen aus verschiedenen Gründen abgelehnt. Neben nicht tragfähigen Argumenten (z. B. dass Papierakten keine „Datenträger“ seien) teilte das Krankenhaus mit, dass keine schwerwiegenden Beeinträchtigungen für die Betroffenen drohten, da die Vorgänge z. T. 30 bis 40 Jahre alt und aufgrund des schlechten Aktenzustandes Namen und Wohnorte nur schwer lesbar gewesen seien. Diese Gefahrenprognose wurde von dem Krankenhaus jedoch insbesondere im Hinblick auf Daten zu Drogenabhängigkeiten, Erwerbsminderungen und Geschlechtsumwandlungen nicht ausreichend

225 JB 2007, 7.3.6; JB 2008, 8.2.4

belegt. Zudem war es problematisch, dass das Krankenhaus sämtliche Patientenunterlagen aus den Kellerräumen vernichtet hatte, obwohl nicht ausgeschlossen werden konnte, dass auch Akten anderer verantwortlicher Stellen betroffen waren. Durch die Vernichtung der Akten war eine Benachrichtigung einzelner Betroffener nicht mehr möglich. Wir haben die Charité auf diese Missstände aufmerksam gemacht und darauf hingewiesen, dass zukünftig vor der Räumung von Standorten der Aktenbestand erfasst werden und nach der Räumung überprüft werden sollte, ob die Akten tatsächlich entfernt wurden. Auch sind Akten nach der Aufbewahrungsfrist erst zu vernichten, wenn feststeht, dass keine Benachrichtigungspflicht besteht. Akten anderer verantwortlicher Stellen dürfen keinesfalls vernichtet, sondern müssen der anderen Stelle übergeben werden.

Bei einem Datenverlust muss anhand der Art der Daten, der möglichen Verwendungsszenarien und der Gesamtumstände des Falles eine differenzierte Prognose erstellt werden, ob für die Betroffenen schwerwiegende Beeinträchtigungen drohen.

Verlust von Tourenplänen in der Hauskrankenpflege

Aus der Praxis

Ein Unternehmen für Hauskrankenpflege informierte uns gleich in zwei Fällen, dass Tourenpläne der mobilen Pflegekräfte abhandengekommen waren. Wie und wo dies geschehen war, konnte nicht mehr nachvollzogen werden. Auf den Tourenplänen waren nicht nur die Namen und Adressen der zu pflegenden Personen vermerkt. Die Pläne enthielten auch Angaben zu den Pflegemaßnahmen (z. B. „Darm-/Blasenentleerung“, „große Körperpflege“) sowie Bemerkungen dazu, wann und in welcher Höhe die Gepflegten Taschengeld erhalten und wie die Pflegekräfte Zugang zur Wohnung erhalten („3x klingeln“, „Zugang über die Terrasse“, „Tür steht immer offen“). Da die meisten Betroffenen unter rechtlicher Betreuung standen, wurden in diesen Fällen nicht die Betroffenen selbst, sondern ihre Betreuer über den Vorfall benachrichtigt.

Durch den Verlust der Tourenpläne drohten schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen: Bei den

Angaben zu den Pflegemaßnahmen handelt es sich um sensitive Daten, die vertraulich zu behandeln sind und der Schweigepflicht unterliegen können. Zudem ergibt sich aus den Tourenplänen, dass die Personen auf fremde Hilfe angewiesen sind. Im Zusammenhang mit den Hinweisen, wie der Zugang zu den Wohnungen möglich ist, können diese Informationen z. B. für Einbrüche genutzt werden, sodass ein besonders hohes Missbrauchsrisiko besteht. Wir haben das Unternehmen darauf hingewiesen, dass nicht in jedem Fall der Betreuung zwingend der Betreuer anstelle der betreuten Person zu benachrichtigen ist. Vielmehr muss die verantwortliche Stelle im Einzelfall prüfen, ob die Person einsichtsfähig ist und daher selbst informiert werden kann. Das Unternehmen hat die Beschäftigten erneut belehrt und auf die sorgsame Behandlung der Tourenpläne hingewiesen. Künftig werden alle Beschäftigten regelmäßig zu Verhaltensmaßnahmen im Datenschutz geschult.

Die Tourenpläne in der Pflege, die den Arbeitsablauf der Pflegekräfte festlegen, können sensitive Daten über die Betreuten enthalten. Wenn eine betroffene Person einsichtsfähig ist, muss sie auch bei einer Betreuung selbst über Datenpannen informiert werden.

Fehlendung per Fax mit unangenehmen Folgen

Bei der Bearbeitung einer Datenschutzbeschwerde erfuhren wir, dass eine Personalvermittlungsfirma Daten zu Leiharbeitnehmern (u. a. zu deren Bankverbindungsdaten) versehentlich an eine falsche Faxnummer gesendet hatte. Als das bemerkt wurde, schickte das Unternehmen ein Fax mit der Bitte um Vernichtung der fehlgeleiteten Unterlagen hinterher. Bei dem Empfänger der Daten handelte es sich um einen Rechtsanwalt, der einen ehemaligen Mitarbeiter in einem arbeitsgerichtlichen Prozess gegen das Unternehmen vertrat.

Die Personalvermittlungsfirma hatte die Betroffenen zunächst nicht benachrichtigt. Sie hatte mit der Stellung des fälschlichen Datenempfängers argumentiert und erklärt, dass keine schwerwiegenden Beeinträchtigungen drohen würden, da der Rechtsanwalt als Organ der Rechtspflege die Daten weisungsgemäß vernichten würde. Gleichzeitig räumte die Personalvermittlungsfirma

allerdings ein, der Anwalt habe telefonisch mitgeteilt, dass er die empfangenen Unterlagen zur Handakte genommen und seinen Mandanten über den Irrläufer informiert hatte. Die Rechtsanwaltskammer hat hierin keinen Verstoß gegen anwaltliches Berufsrecht gesehen. Nachdem wir das Unternehmen darauf hingewiesen hatten, dass nicht absehbar sei, wie der Mandant mit den Daten weiter verfährt, benachrichtigte die Personalvermittlungsfirma alle Betroffenen schriftlich.

Im Rahmen der Prognose, ob schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen, spielt es auch eine Rolle, wer Empfänger von fehlgeleiteten Daten ist. Dabei ist nicht nur die Stellung der Person, z. B. als Rechtsanwalt, sondern auch das konkrete Verhalten – soweit bekannt – zu berücksichtigen.

Diebstahl von Laptop und Papierakten aus dem PKW

Der Mitarbeiterin eines Unternehmens, das arbeitsmedizinische Untersuchungen durchführt, wurden ein Laptop und zehn Papierakten aus dem Fahrzeug entwendet. Betroffen waren Daten von Probanden, d. h. von Beschäftigten des Auftraggebers des Unternehmens. Die Papierakten enthielten ärztliche Befunde. Auf dem Notebook waren ärztliche Stellungnahmen zu der Frage der Eignung der Probanden für bestimmte berufliche Tätigkeiten gespeichert. Das Gerät verfügte über eine Festplattenverschlüsselung mit einem aus acht Zeichen bestehenden Passwort.

Das Unternehmen informierte zwar die Betroffenen. Die Benachrichtigung enthielt allerdings Ungenauigkeiten und objektive Unrichtigkeiten (wie das falsche Datum des Vorfalls), sodass wir die Korrektur des Schreibens gefordert haben. Technische und organisatorische Maßnahmen werden grundsätzlich nicht eingehalten, wenn Akten und Notebooks mit sensiblen Daten im geparkten PKW hinterlassen werden. Außerdem kann auch der Verlust oder Diebstahl von Papierakten eine Informationspflicht auslösen. Eine Festplattenverschlüsselung ist nur dann wirksam, wenn das Gerät zum Zeitpunkt des Verlusts auch tatsächlich ausgeschaltet ist. Trotz Verschlüsselung ist zu berücksichtigen, dass ein möglicher Angreifer das Gerät in seiner Gewalt hat und folglich unbeschränkt verschiedene Passwörter durchprobieren kann. Dement-

sprechend muss das Passwort für die Verschlüsselung von Laptops eine ausreichende Länge haben.²²⁶

Eine Festplattenverschlüsselung eines Notebooks bietet nur dann ausreichende Sicherheit, wenn es zum Zeitpunkt des Verlusts ausgeschaltet ist, das Passwort eine ausreichende Länge aufweist und nicht oder nicht so notiert wird, dass es einem potenziellen Angreifer in die Hände gelangen kann.

Versand von Befundmustern ohne ausreichende Schwärzung

Zur Beschaffung eines neuen Laborinformationssystems führte ein Labor ein Vergabeverfahren durch. Dabei waren exemplarisch Befundmuster an Bieterunternehmen übermittelt worden. Die Muster waren allerdings z. T. nicht oder nicht ausreichend geschwärzt, und die Namen waren durch die Schwärzung hindurch erkennbar. Das Labor hat daraufhin die Bieterunternehmen zur Vernichtung der Befundmuster aufgefordert und darüber von sämtlichen Bieterunternehmen eine Bestätigung erhalten. Die Betroffenen wurden nicht benachrichtigt.

Das Labor begründete das damit, dass die Bieterunternehmen im Rahmen des Vergabeverfahrens zur vertraulichen Behandlung der Befundmuster verpflichtet waren. Auch hätten sämtliche Bieterunternehmen die Vernichtung der Unterlagen bestätigt, sodass keine schwerwiegende Beeinträchtigung für die Betroffenen drohte. Wir hatten keine Anhaltspunkte, die Einschätzung des Labors in Frage zu stellen.

Bei der Weitergabe von Musterformularen muss darauf geachtet werden, dass sie entweder keine personenbezogenen Daten enthalten oder anonymisiert wurden.

²²⁶ Laut Empfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI) sollten hierfür nicht nur 8, sondern 20 Zeichen verwendet werden; siehe www.bsi-fuer-buerger.de

15.2.2 Datenpannen in der Verwaltung

Beschäftigtendaten im Intranet der BVG

Ein Petent (ehemaliger Mitarbeiter der BVG) beschwerte sich bei uns über Datenschutzverstöße bei der BVG und übergab uns eine CD mit Daten zu BVG-Beschäftigten. Es handelte sich um Excel-Tabellen mit Abwesenheitszeiten innerhalb von zwei Jahren und taggenauer Zuordnung der An- und Abwesenheitsgründe (z. B. krankheitsbedingter Ausfall) sowie um leistungs- oder verhaltensbezogene Vermerke.

Die BVG stellte sich zunächst auf den Standpunkt, dass der Petent schon während seiner Dienstzeit Kenntnis von den Daten erhalten habe und daher eine unrechtmäßige Kenntnisnahme durch einen „Dritten“ nicht gegeben sei. Diese Auffassung war unzutreffend, denn die personenbezogenen Informationen stammten aus einer Zeit, in der der Petent nicht mehr Mitarbeiter gewesen war, mithin ein (weiterer) Dritter die Daten zur Kenntnis genommen und kopiert haben musste. Nachdem die BVG den Sachverhalt weiter aufgeklärt hatte, stellte sich heraus, dass aufgrund einer Änderung der Verzeichnisstruktur versehentlich alle Beschäftigten einer Abteilung auf bestimmte Daten zugreifen konnten.

Unabhängig davon, dass das Führen von Listen mit krankheitsbedingten Ausfällen zu Personalplanungszwecken nicht erforderlich und damit unzulässig ist und die BVG diese Praxis nach unserer Intervention einstellte, stand hier die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Dritten nach § 18 a BlnDSG im Raum. Diese Pflicht wird ausgelöst, wenn personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Auch Beschäftigte können „Dritte“ sein, wenn sie personenbezogene Daten zur Kenntnis nehmen, auf die sie nach ihren dienstrechtlich festgelegten Befugnissen nicht zugreifen dürfen. Die Beschäftigten werden dann zu Empfängern, die außerhalb der datenverarbeitenden Stelle stehen, mithin „Dritte“ sind.

So lag der Fall hier: Sowohl der Petent als auch alle in der Abteilung Tätigen konnten für eine bestimmte Zeit auf Personaldaten zugreifen, obwohl dies nach

dem Berechtigungskonzept der BVG nur Personalverantwortlichen erlaubt war. Auch bestand kein Zweifel daran, dass schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohten: Informationen zu krankheitsbedingten Fehlzeiten sind Gesundheitsdaten und werden von den Datenschutzgesetzen als sensitiv eingestuft. Die leistungs- und verhaltensbezogenen Vermerke können das Ansehen der Betroffenen im Kollegenkreis nachhaltig beschädigen. Die BVG musste von uns mehrmals aufgefordert werden, bis sie ihrer Informationspflicht gegenüber den Betroffenen schließlich nachkam.

Ein wirksames und funktionierendes Zugriffs- und Berechtigungskonzept ist bei der personenbezogenen Datenverarbeitung in Organisationen unabdingbar. Insbesondere müssen Personaldaten vertraulich behandelt werden. Es muss sichergestellt sein, dass Beschäftigte, die keine Personalverwaltungsaufgaben haben, solche Daten nicht zur Kenntnis nehmen können. Auch der unberechtigte Zugriff von Beschäftigten auf Personaldaten kann eine informationspflichtige Datenpanne sein.

Ungeschwärzte Angaben zu ärztlichen Fachrichtungen

Das Bezirksamt Charlottenburg-Wilmersdorf teilte uns mit, dass es zu einer unzulässigen Datenübermittlung an die Personalvertretungen gekommen war: Es hatte ihnen im Rahmen ihrer Beteiligungsrechte Wiedereingliederungspläne von Beschäftigten vorgelegt. Dabei waren die Informationen zu ärztlichen Fachrichtungen der ausstellenden Ärzte nicht geschwärzt worden, sodass es möglich war, auf Krankheitsbilder der Betroffenen zu schließen.

Informationen zu möglichen Krankheitsbildern von Personen in der Wiedereingliederung sind für die Aufgabenerfüllung der Personalvertretungen im Rahmen ihrer Beteiligung nicht erforderlich. Eine Übermittlung dieser sensitiven Daten ist grundsätzlich nur mit Einwilligung der Betroffenen zulässig. Wie der Fall zeigt, ist eine Pflicht zur Benachrichtigung der Betroffenen nicht nur denkbar, wenn die Daten versehentlich (aufgrund eines „Datenlecks“) abhandengekommen sind, sondern auch, wenn sie wissentlich – jedoch unzulässigerweise – von der verantwortlichen Stelle weitergegeben

wurden. In jedem Fall muss geprüft werden, ob schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Die Daten verarbeitende Stelle muss die Gefahr für die Betroffenen unter Berücksichtigung der Datenarten, der Verwendungsszenarien sowie der Datenempfänger prognostizieren. Hier waren zwar einerseits sensitive Daten betroffen. Andererseits war die Gefahr, die von den Datenempfängern ausging, als gering zu bewerten, da die Mitglieder der Personalvertretungen generell zur Verschwiegenheit verpflichtet sind. Das Bezirksamt hat gleichwohl die Betroffenen über die fehlerhaften Datenübermittlungen informiert und wird künftig keine Informationen über ärztliche Fachrichtungen an die Personalvertretungen weiterleiten.

Eine Informationspflicht kann auch dann in Betracht kommen, wenn die Daten verarbeitende Stelle eine bewusste Datenübermittlung vorgenommen hat, die unzulässig war.

Schülerakten verschwunden!

Aus der Praxis

Eine Grundschule informierte uns, dass aus dem Sekretariat Schülerbögen verschwunden waren. Dabei handelte es sich um neu angelegte Schülerakten, die neben den Stammdaten (Name des Kindes, Name der Erziehungsberechtigten, Anschrift und Telefonnummer) auch Kopien von Geburtsurkunden der Kinder sowie Untersuchungsbögen des Schularztes enthielten. Wie die Akten abhandengekommen waren, konnte nicht geklärt werden. Die Grundschule informierte die Schulaufsicht und den Schuldatenschutzbeauftragten und erstattete Strafanzeige bei der Polizei. Zwei Wochen nach dem Vorfall benachrichtigte die Grundschule die Eltern der betroffenen Kinder schriftlich.

Zwar konnte die Grundschule in diesem Fall nicht positiv feststellen, ob ein Dritter die Unterlagen mitgenommen und zur Kenntnis genommen hatte. Da sie trotz intensiver Suche aber nicht gefunden werden konnten, war dies jedenfalls nicht unwahrscheinlich. Gerade wenn wie hier auch besondere Arten personenbezogener Daten (Untersuchung beim Schularzt) eine Rolle spielen, ist eine Benachrichtigung unumgänglich. In den Fällen der Informationspflicht muss die Benachrichtigung unverzüglich, d. h. ohne schuldhaftes

Zögern erfolgen. Dabei steht der datenverarbeitenden Stelle grundsätzlich eine angemessene Frist zu, den Sachverhalt auch im Hinblick auf eine mögliche Informationspflicht zu prüfen. In der Regel ist eine zweiwöchige Prüffrist der datenverarbeitenden Stelle nur bei komplexen Sachverhalten angemessen. Da die Grundschule zunächst eine intensive Suche durchgeführt hatte, war die Benachrichtigung der Eltern trotz des Ablaufs von zwei Wochen noch vertretbar.

Bei der Prüfung, ob eine Informationspflicht besteht, muss nicht positiv festgestellt werden, ob Dritte von den Daten Kenntnis erlangt haben. Wenn anhand von tatsächlichen Anhaltspunkten mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann, ist zu benachrichtigen.

Verlust eines Laptops in der S-Bahn

Die Schwerbehindertenvertretung eines Bezirksamtes sicherte Informationen zu Beschäftigten auf ihrem privaten Notebook, um Arbeit zu Hause zu erledigen. Bei den Daten handelte es sich um Widerspruchsschreiben der Beschäftigten, die einen Antrag auf Feststellung der Behinderung gestellt hatten. Die Bemühungen der Schwerbehindertenvertretung, das Notebook wiederzuerlangen, waren erfolglos: Weder bei der S-Bahn-Aufsicht noch in den Fundbüros war das Notebook abgegeben worden. Die Schwerbehindertenvertretung stellte zudem Strafantrag wegen Fundsachenunterschlagung. Das Ermittlungsverfahren wurde eingestellt. Die Schwerbehindertenvertretung benachrichtigte die Betroffenen jeweils im persönlichen Gespräch über den Vorfall. Sie informierte zudem die Dienststellenleitung und den behördlichen Datenschutzbeauftragten, der wiederum uns in Kenntnis setzte.

Die Nutzung von privater Hardware war nach den technisch-organisatorischen Anweisungen des Bezirksamtes nicht erlaubt.²²⁷ Das Notebook war folglich als dienstliches Arbeitsmittel nicht zugelassen. Es verfügte auch nicht über eine Verschlüsselung, sodass Dritten der Zugriff auf die Daten unproblematisch

²²⁷ Der Einsatz von privaten Geräten im dienstlichen Gebrauch ist generell problematisch, siehe hierzu 2.3.

möglich war. Der datenverarbeitenden Stelle steht es nach den gesetzlichen Vorgaben grundsätzlich frei, mündlich, schriftlich oder elektronisch zu informieren. Da sie im Zweifel nachweisen können muss, dass sie die Betroffenen benachrichtigt hat, ist es allerdings ratsam, schriftlich zu informieren. Aufgrund des besonderen Vertrauensverhältnisses hielt es die Schwerbehindertenvertretung in diesem Fall für sinnvoller, die Betroffenen persönlich zu informieren. Sie hat uns später schriftlich über den Gesprächsinhalt informiert, sodass wir feststellen konnten, dass die Mitteilung an die Betroffenen inhaltlich richtig und vollständig war.

Unabhängig davon, wie die Betroffenen benachrichtigt werden (schriftlich, elektronisch oder mündlich), muss die Daten verarbeitende Stelle uns über den Inhalt der Information aufklären. Ansonsten können wir nicht überprüfen, ob die Mitteilung an die Betroffenen korrekt war.

15.3 Datenschutzfreundliche Verfahrensgestaltung: Behandlungsleitlinien für Schmerzpatienten

Um auf die datenschutzfreundliche Gestaltung von Verfahren der personenbezogenen Datenverarbeitung hinzuwirken, beraten wir insbesondere bei der Erstellung von Datenschutzkonzepten und in Fragen des Datenschutzmanagements. So stellte uns eine Schmerztherapieeinrichtung ein Verfahren vor, mit dem Behandlungsleitpfade von Schmerzpatienten kontinuierlich entwickelt und verbessert werden sollen. Die an dem Modell teilnehmenden Schmerztherapieeinrichtungen und Arztpraxen sollen den an bestimmten Leitlinien orientierten Behandlungsverlauf mit einem Behandlungspfad-Tool standardisiert dokumentieren. Diese Dokumentationen werden zentral in einer Forschungsdatenbank ausgewertet und in Form von Behandlungsempfehlungen an die teilnehmenden Einrichtungen zurückgegeben.

Zunächst legte uns die Einrichtung den Entwurf eines Datenschutz- und Sicherheitskonzepts vor, das vorsah, die Daten personenbezogen, einrichtungsübergreifend und zentral in einer elektronischen Patientenakte zu erfassen und zu dokumentieren. Die Verfahrensabläufe waren allerdings unvollständig, sodass

eine abschließende rechtliche Prüfung nicht möglich war. Auch genügten die beschriebenen Maßnahmen nicht den Anforderungen an ein datenschutzgerechtes Verfahren.

Wir stellten einen umfangreichen Katalog zur Nachbesserung zusammen. Daraufhin entwickelte die Einrichtung ein datenschutzfreundlicheres Verfahren: Das neue Konzept sah keine zentrale Dokumentation personenbezogener Patientendaten mehr vor. Die Daten sollen nunmehr in den lokalen Systemen der teilnehmenden Einrichtungen anonymisiert und in dieser Form an die Forschungsdatenbank gemeldet werden. Auf der Grundlage der anonymisierten Daten sollen Behandlungsempfehlungen erstellt und an die Teilnehmer zurückgemeldet werden. Auf dieser Basis hatten wir gegen das Verfahren keine Einwände. Wir wiesen allerdings darauf hin, dass wir einzubeziehen sind, wenn das anonymisierte in ein personenbezogenes Verfahren umgewandelt werden soll.

Patientenbezogene Daten sollten auch dann dezentral gespeichert werden, wenn sie Forschungszwecken dienen.

15.4 Stiftung Datenschutz

Nachdem es lange Zeit ruhig war um die „Stiftung Datenschutz“, hat der Bundestag im Juni auf Antrag der Koalitionsfraktionen²²⁸ die Bundesregierung aufgefordert, die Stiftung bis Oktober in Leipzig zu errichten. Die aktuelle Satzung sieht eine Beteiligung der Datenschutzbehörden im Beirat der Stiftung vor. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im November beschlossen, von der Möglichkeit der Mitwirkung derzeit keinen Gebrauch zu machen, weil frühere Forderungen der Datenschutzbeauftragten²²⁹ in dem aktuellen Stiftungskonzept nicht berücksichtigt wurden. So entsprechen die vorgesehenen Mitwirkungsmöglichkeiten über den Beirat

228 BT-Drucksache 17/10092

229 Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010: „Förderung des Datenschutzes durch Bundesstiftung“, Dokumentenband 2010, S. 21

der Stiftung nicht den Vorstellungen, die die Datenschutzbeauftragten von einer engen Kooperation zwischen Stiftung und Datenschutzbehörden haben. Dazu sind die Möglichkeiten, z. B. auf die Ausgestaltung von Standards in Zertifizierungsverfahren Einfluss zu nehmen, zu gering. Außerdem steht die erforderliche Unabhängigkeit der Stiftung von den datenverarbeitenden Stellen und der IT-Wirtschaft angesichts des Konzepts der Stiftung und ihrer finanziellen Ausstattung in Frage. Die Datenschutzbeauftragten haben dem Bundesministerium des Innern die Entscheidung über ihre derzeitige Nichtbeteiligung mitgeteilt.

16 Telekommunikation und Medien

16.1 Die neue Google-Datenschutzerklärung – ein Rückschritt für den Datenschutz

Die Google Inc., die neben einer Suchmaschine noch eine Vielzahl anderer Anwendungen einschließlich eines E-Mail-Dienstes, eines sozialen Netzwerks und eines Betriebssystems für Smartphones anbietet, hat im März ihre Datenschutzbestimmungen geändert und bisher produktspezifisch getroffene Regelungen für mehrere Dutzend Einzelprodukte in einer einzigen Datenschutzerklärung zusammengefasst. Hinter dieser vordergründig kundenfreundlich erscheinenden Neuerung verbirgt sich eine grundlegende Änderung der Datenverarbeitung bei Google zulasten der Nutzenden. In der Vergangenheit hatte das Unternehmen stets erklärt, keine umfassenden Nutzerprofile anlegen zu wollen. Das Unternehmen behält sich jetzt vor, solche auch produktübergreifend zu erstellen, also z. B. Daten aus der Nutzung des E-Mail-Programms „Gmail“ mit solchen aus dem sozialen Netzwerk „Google+“, der Suchmaschine und dem „Android“-Betriebssystem für Smartphones miteinander zu kombinieren.

Zwar ist für bestimmte Dienstleistungen (etwa die Berücksichtigung von Daten aus dem sozialen Netzwerk bei der Zusammenstellung von Suchergebnissen in der Suchmaschine – „Search Plus Your World“) die Kombination von Daten aus verschiedenen Diensten erforderlich. Auch können viele dieser umsonst angebotenen Dienste des Unternehmens unter einem Pseudonym genutzt werden, einige sogar ohne vorherige Registrierung. Jedoch will das Unternehmen offenbar Anreize dafür setzen, dass möglichst viele Nutzende sich bei Google mit einem sog. „Google-Account“ registrieren. Über den Einsatz von Cookies werden dann die verschiedenen Nutzungsdaten zu einem Nutzerprofil zusammengeführt. Je mehr Detailinformationen diese möglicherweise zunächst pseudonymen Profile enthalten, umso mehr steigt die Möglichkeit zur De-Pseudonymisierung. Allein aus der Kombination von Profil- und Nutzungsdaten des sozialen Netzwerks „Google+“ mit Angaben über die Nutzung der Suchmaschine lassen sich detaillierte Informationen über die Interessen, Wünsche und Befindlichkeiten der oder des Nutzenden ableiten.

Die französische Datenschutzbehörde hat im Auftrag der Art. 29-Datenschutzgruppe eine Untersuchung der neuen Datenschutzerklärung des Unternehmens durchgeführt. Die Ergebnisse wurden im Oktober veröffentlicht. In einer gemeinsamen Erklärung stellen die Datenschutzbeauftragten Europas fest, dass Google seine Nutzerinnen und -nutzer unzureichend über die Verarbeitung ihrer personenbezogenen Daten informiert: Für eine Nutzerin oder einen Nutzer ist es gegenwärtig nicht möglich, aus der Datenschutzerklärung zu ersehen, welche Kategorien von personenbezogenen Daten für einen Dienst verarbeitet werden und für welche Zwecke dies genau erfolgt. Die Datenschutzbeauftragten haben Google aufgefordert, klarere und umfassendere Informationen über die verarbeiteten Daten und die Zwecke der jeweiligen Datenverarbeitung zu geben. Sie kritisieren auch, dass Google den Nutzenden keine Kontrolle über die Kombination ihrer Daten aus den verschiedenen Diensten ermöglicht. Praktisch jede Online-Aktivität mit Bezug zu Google könne erhoben und für verschiedene Zwecke kombiniert werden. Die Datenschutzbeauftragten Europas fordern Google auf, die Einwilligung der Nutzenden in die Kombination von Daten für den Zweck der Optimierung von Diensten, der Entwicklung neuer Dienste, der Werbung und der Reichweitenmessung zu verbessern, z. B. indem den Nutzenden eine Wahlmöglichkeit zum Zeitpunkt der Kombination der Daten eingeräumt wird, etwa mit besonderen Schaltflächen innerhalb der Dienste. Die Möglichkeiten zur Kontrolle der Kombination von Daten soll dadurch verbessert werden, dass Widerspruchsmöglichkeiten vereinfacht und zentralisiert werden und indem den Nutzenden die Möglichkeit gegeben wird zu bestimmen, für welche Dienste ihre Daten kombiniert werden. Die Datenschutzbehörden kritisieren auch Umfang und Dauer der Speicherung.

Zwar ist eine Kombination personenbezogener Daten über verschiedene Dienste hinweg aufgrund einer informierten Einwilligung der Nutzenden nach deutschem Recht grundsätzlich möglich. Die Betroffenen sollten sich jedoch genau überlegen, welche Dienste der Google Inc. sie unter den neuen Bedingungen nutzen wollen. Für viele der von Google angebotenen Dienste stehen datenschutzfreundlichere Alternativen zur Verfügung. Wer auf einzelne Dienste des Unternehmens nicht verzichten will, sollte erwägen, Google und den damit verbundenen Unternehmen, z. B. Doubleclick, das Setzen von Cookies durch entsprechende Browser-Einstellungen zu untersagen.²³⁰ Von der kombinierten

230 Siehe 16.4.1

Nutzung von Diensten unter einem Google-Account ist abzuraten. Dort wo die Registrierung eines Accounts Voraussetzung für die Nutzung eines Dienstes ist, empfehlen wir die Registrierung verschiedener Accounts für die verschiedenen Dienste.²³¹ Schließlich sollten die für die einzelnen Dienste existierenden Widerspruchsmöglichkeiten gegen die Verarbeitung personenbezogener Daten umfassend genutzt werden.

Die geänderte Datenschutzerklärung der Google Inc. macht nochmals deutlich, dass die Betroffenen scheinbar kostenlos angebotene Dienste mit der Nutzung ihrer personenbezogenen Daten bezahlen. Ähnlich wie bei sozialen Netzwerken gilt auch hier der Grundsatz, dass „umsonst“ nicht unbedingt auch „gratis“ ist.

Die produktübergreifende Profilbildung führt zu neuen Risiken für den Schutz der Privatsphäre. Google wird hier Verbesserungen vornehmen müssen. Nutzerinnen und Nutzer sollten aber auch selbst Maßnahmen treffen, um eine umfassende Profilbildung durch das Unternehmen zu verhindern.

16.2 Soziale Netzwerke

16.2.1 Social Plugins

Bereits 2011²³² haben wir darauf hingewiesen, dass der Einsatz sog. „Social Plugins“, mit denen die Nutzung von Webseiten mit der Nutzung sozialer Netzwerke verknüpft werden kann, dem geltenden Datenschutzrecht nur dann genügt, wenn die Übertragung personenbezogener Daten (einschließlich IP-Adressen und Browser-Einstellungen) von Nutzenden durch den Anbieter der Webseite an den Betreiber des sozialen Netzwerks erst dann erfolgt, wenn Nutzende die entsprechende Schaltfläche des Social Plugins betätigt haben (sog. „Zwei-Klick-Lösung“). Besondere Risiken für

231 Vor einem Account-Wechsel sollten immer auch die Cookies gelöscht werden, um Verknüpfungsmöglichkeiten zu reduzieren.

232 JB 2011, 2.3

die Privatsphäre können entstehen, wenn mit der Übermittlung der Nutzungsdaten dem Betreiber des sozialen Netzwerks implizit sensitive Daten offenbart werden (wie z. B. ein Interesse an Informationen zu bestimmten Erkrankungen). Inzwischen entscheiden sich immer mehr Unternehmen für die „Zwei-Klick-Lösung“. Besonders erfreulich ist, dass aufgrund unserer Hinweise auch einige der großen Berliner Medienunternehmen dazu übergegangen sind, Social Plugins in ihren Angeboten unter Nutzung dieser Möglichkeit auszugestalten.

Einige Anbieter großer sozialer Netzwerke haben es bisher unterlassen, selbst entsprechende datenschutzkonforme Lösungen bereitzustellen. Dies ist unverständlich, weil durch solche Lösungen sowohl den Interessen der Nutzenden am Schutz ihrer Privatsphäre als auch den Interessen der Anbieter von Webseiten an der Vermeidung aufsichtsbehördlicher Maßnahmen am besten entsprochen werden könnte.

Anbieter von Webseiten können Social Plugins in ihre Angebote unter Nutzung der „Zwei-Klick-Lösung“ datenschutzkonform einbinden. Anbieter sozialer Netzwerke bleiben aufgefordert, ihren Kunden auch selbst entsprechende Lösungen zur Verfügung zu stellen.

16.2.2 Anschluss- und Benutzungszwang bei Facebook?

Einige Anbieter sozialer Netzwerke geben anderen Anbietern von Telemedien die Möglichkeit, für eine Registrierung bei diesen Telemedien auf die Registrierungsdaten aus dem sozialen Netzwerk zurückzugreifen. Nutzende können sich dann mit ihren Registrierungsdaten aus dem sozialen Netzwerk auch für das betreffende Telemedium anmelden. Dies hat aus Sicht der Nutzenden den Vorteil, dass sie für das Telemedium nicht noch einen weiteren Satz von Registrierungsdaten (Nutzerkennung, Passwort) verwalten müssen. Allerdings besteht je nach Ausgestaltung u. U. auch die Möglichkeit, dass der Betreiber des sozialen Netzwerks nicht nur Kenntnis von der Tatsache der Registrierung bei dem jeweiligen Telemedium erhält, sondern auch Einzelheiten über dessen Nutzung erfährt.

Solche Ausgestaltungen sind grundsätzlich zulässig, wenn sie mit Wissen und Willen der Betroffenen erfolgen. Voraussetzung ist allerdings, dass das jeweilige soziale Netzwerk selbst die im Telemediengesetz (TMG) festgelegten Rechte der Nutzenden berücksichtigt.

Unzulässig ist es dagegen, wenn der Anbieter eines Telemediums die Registrierung für seinen Dienst ausschließlich über ein soziales Netzwerk anbietet, das – entgegen der im TMG enthaltenen Verpflichtung zum Angebot anonymer bzw. pseudonymer Nutzung²³³ – auf einer Registrierung in dem sozialen Netzwerk ausschließlich unter dem Klarnamen besteht. Dies ist bisher z. B. bei Facebook der Fall. Das US-Unternehmen hat sich trotz mehrfacher Hinweise der deutschen Datenschutzbehörden bisher geweigert, von dieser Praxis abzurücken. Da Anbieter von Telemedien nach deutschem Recht ihrer gesetzlichen Verpflichtung zum Angebot anonymer bzw. pseudonymer Nutzung nachkommen müssen, können sie also eine Registrierung über Facebook lediglich als eine mögliche Alternative anbieten, wenn sie gleichzeitig selbst eine anonyme bzw. pseudonyme Nutzung ermöglichen. Die Nutzenden sind über die zur Verfügung stehenden Möglichkeiten und die daraus jeweils resultierende Verarbeitung ihrer personenbezogenen Daten zu informieren, damit sie entscheiden können, welche Zugangsart sie bevorzugen. Einen – wenn auch nur indirekten – Anschluss- und Benutzungszwang bei Facebook kann es nicht geben.

Diensteanbieter sind nach dem in Deutschland geltenden Telemediengesetz verpflichtet, den Nutzenden die Möglichkeit zur anonymen bzw. pseudonymen Nutzung einzuräumen. Die ausschließliche Eröffnung der Nutzung eines Telemediums über ein soziales Netzwerk, das eine anonyme bzw. pseudonyme Nutzung nicht zulässt, ist rechtswidrig.

233 § 13 Abs. 6 TMG

16.2.3 Leitfaden für den Einsatz von sozialen Medien in der Berliner Verwaltung

Bereits 2011²³⁴ haben wir auf Probleme bei der Nutzung von sozialen Medien – insbesondere in Bezug auf Social Plugins und auf Profile von Organisationen – hingewiesen. Im selben Jahr hat die Senatsverwaltung für Inneres und Sport eine Arbeitsgruppe „Social Media“ eingerichtet, die einen Leitfaden für die Nutzung von sozialen Netzwerken in der Berliner Verwaltung erarbeitet hat. An dieser Arbeitsgruppe haben wir uns beteiligt. Die Senatsverwaltung für Inneres und Sport hat unsere Bewertungen im Leitfaden berücksichtigt.

Ob und ggf. unter welchen Voraussetzungen der Einsatz von sog. „Fanpages“ zulässig ist, wird derzeit von den Verwaltungsgerichten in Schleswig-Holstein geprüft.

Öffentliche und private Stellen sollten bei der Einrichtung von Profilen ihrer Organisation in sozialen Netzwerken darauf achten, ob der Anbieter des sozialen Netzwerks es ihnen ermöglicht, ihre Verpflichtungen nach dem TMG einzuhalten. Wo dies nicht der Fall ist, sollte auf die Anlage solcher Profile jedenfalls gewährt werden.

16.3 Liquid Feedback mit Klarnamen?

Wir haben im letzten Jahr über das „Liquid Feedback“-System (LQFB) der Piratenpartei berichtet.²³⁵ Der Landesverband Pankow beabsichtigt, für alle Formen der Beteiligung am LQFB das Klarnamenprinzip einzuführen. Das Pankower Modell soll Pilotcharakter auch für andere LQFB-Systeme innerhalb der Piratenpartei haben. Die Daten sollen unbefristet gespeichert werden, im Fall der Beendigung der LQFB-Teilnahme oder der Parteimitgliedschaft soll der Klarnamen durch ein Pseudonym ersetzt werden. Das Klar-

234 JB 2011, 2.3

235 JB 2011, 1.2.1 (S. 30 ff.)

namenprinzip soll insbesondere das Risiko einer Verfälschung des Willensbildungsprozesses durch die Schaffung von virtuellen Nutzern ohne dahinterstehende Parteimitglieder („Sockenpuppen“) verringern. Die wachsende Bedeutung des LQFB auch für parlamentarische Entscheidungen der Partei erfordere außerdem die Änderung des Systems, das bisher eine pseudonyme Nutzungsmöglichkeit für Teilnehmende und Parteimitglieder vorsieht.

Ob die Verarbeitung der Angaben über politische Meinungen im LQFB für die Tätigkeit der Partei „erforderlich“ ist,²³⁶ ist unter Berücksichtigung der verfassungsrechtlichen Grundsätze des Parteienrechts zu ermitteln. Dazu gehört insbesondere das Recht jeder Partei, ihre interne Willensbildung selbst zu regeln,²³⁷ sowie der Grundsatz der parteiinternen Öffentlichkeit als „Demokratiebedingung“.²³⁸ Bezüglich der konkreten Verfahren und Formen, in denen parteiinterne Öffentlichkeit hergestellt wird, bestehen von Verfassungs wegen Gestaltungsspielräume. Aber aus dem demokratischen Selbstbestimmungsrecht einer Partei ergibt sich nicht, dass jede Art elektronischer parteiinterner Willensbildung zulässig sein muss.

Die Einführung des Klarnamenprinzips im LQFB führt dazu, dass Aktivitäten (Initiativen, Anregungen und Abstimmungsverhalten) der Mitglieder dauerhaft nachvollziehbar sind. Ein umfassendes Archiv, das auf unbestimmte Zeit alle LQFB-Aktivitäten der Mitglieder in personenbezogener Form erfasst, kann nicht als erforderlich angesehen werden.

Auch der demokratische Grundsatz der parteiinternen Öffentlichkeit spricht nicht für die Erforderlichkeit des Klarnamenprinzips. Der demokratische Willensbildungsprozess einer Partei setzt verfassungsrechtlich keineswegs eine generelle Kenntnis des Abstimmungsverhaltens der Mitglieder voraus; im Gegenteil ist gerade die Möglichkeit geheimer Abstimmungen eine Minderheiten schützende demokratische Vorkehrung. Wenn durch das Klarnamenprinzip im LQFB also Abstimmungen generell namentlich nachvollziehbar wer-

236 § 28 Abs. 9 BDSG

237 Art. 21 Abs. 1 Satz 3 Grundgesetz (GG)

238 Klein in Maunz/Dürig, GG-Kommentar, Art. 21, Rn. 320

den sollen, läuft das den verfassungsrechtlichen Vorgaben einer demokratischen Parteistruktur zuwider.

Die Erforderlichkeit der Einführung von Klarnamen aller Mitglieder kann auch nicht damit begründet werden, dass in einer basisdemokratischen politischen Partei größtmögliche Kenntnisse über (mögliche) Vorstandsmitglieder geboten seien. Denn bereits im bestehenden LQFB dürfen Kandidatinnen und Kandidaten für Ämter zur Gewinnung von Unterstützern ihre Namen freiwillig offenlegen; jedenfalls wäre insoweit eine Abstufung möglich, ohne von vornherein alle LQFB-Nutzenden zur Offenbarung ihres Klarnamens zu zwingen. Es gibt datenschutzfreundlichere Möglichkeiten, Missbräuche zu verhindern. Hier kommt insbesondere ein mehrstufiges dokumentiertes und überwacht Akkreditierungsverfahren für das LQFB in Betracht.

Die Einführung des Klarnamenprinzips kann auch nicht auf eine Einwilligung der LQFB-Teilnehmenden gestützt werden. Angesichts der zentralen Bedeutung, die dem LQFB satzungsmäßig zukommt,²³⁹ müssen Mitglieder de facto teilnehmen, wenn sie effektiv Einfluss nehmen wollen. Für die sogar noch zunehmende Bedeutung von LQFB spricht in Berlin etwa die informelle Verpflichtung von Abgeordneten, ihr Mandat im Abgeordnetenhaus entsprechend den Ergebnissen von LQFB-Abstimmungen auszuüben. Eine entsprechende formelle Verpflichtung würde allerdings der Verfassung von Berlin widersprechen.²⁴⁰

Gegen die Einführung eines beschränkten Klarnamenprinzips bestehen demgegenüber keine Bedenken. Es können als Ausnahmen Fallgruppen gebildet werden, bei denen vom Grundsatz der pseudonymen Datenverarbeitung abgewichen werden kann. In Frage kommt etwa, die Klarnamenpflicht bei der Einbringung von Initiativen einzuführen. Hier besteht ein Interesse zu wissen, ob die Initiative von einer entsprechenden Lobby herrührt. Die Klarnamenpflicht für bloße Stimmabgaben oder Delegationen der Mitglieder sollte sich allerdings auf noch zu definierende Ausnahmefälle beschränken.

239 Siehe nur § 11 Abs. 4 und 5 Satzung der Piratenpartei

240 Art. 38 Abs. 4 VvB

Teilnehmende an Online-Plattformen zur Meinungsbildung in politischen Parteien oder Gremien sollten keinem generellen Zwang zur Identifizierung mit Klarnamen unterliegen.

16.4 Selbsthilfe im Internet

Im Internet kann jeder prinzipiell auch uneingeschränkt Dienste anbieten. Durch deren weltweite Verfügbarkeit ist die Durchsetzung nationaler oder regionaler rechtlicher Regelungen nur eingeschränkt möglich. Die so entstehenden Schutzlücken können jedoch durch Selbstschutzmaßnahmen zumindest teilweise geschlossen werden. Hier sollen insbesondere Maßnahmen zur Einschränkung der Überwachung der Aktivitäten der Internetnutzenden aufgezeigt werden. Weitere Maßnahmen zur IT-Sicherheit finden sich z. B. unter <http://www.verbraucher-sicher-online.de>.

16.4.1 Selbstschutz gegen Tracking

Unter (Web-) Tracking versteht man im Allgemeinen die Bildung von Profilen über Internetnutzende, in denen personenbezogene Eigenschaften wie z. B. ihre demografischen Daten (Wohnort, Alter, Geschlecht), Lebensumstände (z. B. ledig / geschieden, Anzahl der Kinder, Höhe des Einkommens, Gesundheitsstatus), Konflikte und insbesondere die konsumrelevanten Interessen erfasst sein können. Die Daten werden derzeit in erster Linie dazu genutzt, möglichst passende Werbung anzuzeigen, da die Werbetreibenden und Werbevermarkter sich so höhere Erfolgchancen ausrechnen.

Diese derzeit vorherrschende Nutzung zu Werbezwecken könnte man als unproblematisch ansehen, wenn sichergestellt wäre, dass dieses Profil stets unter einem Pseudonym statt unter dem Namen der Person geführt wird, ein direkter Personenbezug niemals hergestellt wird und die umfassende Kontrolle über

die Profilinhalte beim Betroffenen selbst liegt.²⁴¹ Tatsächlich erstellen große Anbieter wie Facebook und Google aber diese Profile zumeist mit vollem Personenbezug. Andererseits sind auch die Nutzungsmöglichkeiten grundsätzlich unbegrenzt: Technisch ist es möglich, Informationen über die jeweiligen Nutzenden auch zur Einschränkung von Angeboten zu nutzen, z. B. die angebotenen Warenpreise abhängig von der Kundenbonität zu gestalten oder Betroffene von (Versicherungs-) Angeboten auszuschließen, wenn aufgrund der vorliegenden (meist ungenauen) Daten Risiken angenommen werden. Denkbar ist auf diese Weise jedwede **informationelle und reale Diskriminierung**. Nicht zuletzt könnten staatliche Stellen so auf persönlichste Daten zugreifen, die anderweitig niemals verfügbar wären. Man denke nur an die in sozialen Netzwerken verfügbaren Daten, z. B. über Beziehungen zwischen Personen sowie das dort vorhandene Foto- und Videomaterial, welches zunehmend automatisiert mit anderen Quellen abgeglichen werden kann.

Tracking wird dadurch möglich, dass Nutzende von allgegenwärtigen Webdiensten (wie z. B. sozialen Netzen, bei denen sie sich freiwillig immer wieder anmelden, oder bei verborgen arbeitenden Werbe- oder Webanalysediensten) auf vielen (externen) Webangeboten wiedererkannt werden. Technisch wird dies durch sog. Cookies und vergleichbare Techniken möglich, die im Wesentlichen Identifikationsnummern immer dann an diese Dienste übermitteln, wenn die gerade besuchte Webseite – oder die benutzte Smartphone-App – einen Vertrag mit dem jeweiligen Dienst eingegangen ist (z. B. zur Anzeige von Werbung und von Social Plugins oder zur statistischen Erfassung der Nutzenden).

Folgende Möglichkeiten zum Selbstschutz gibt es:

- Die bei den Anbietern hinterlassene Datenmenge sollte beschränkt werden. Insbesondere sollten unterschiedliche Dienste (wie E-Mail, Websuche, Networking) bei verschiedenen (Universal-) Anbietern oder zumindest mit mehreren verschiedenen pseudonymen Accounts genutzt werden.
- Der Cookie-Mechanismus sollte bewusst eingesetzt werden. Mittlerweile bieten alle Browser ausgefeilte Cookie-Konfigurationsmöglichkeiten, meist unter „(Internet-) Einstellungen/Datenschutz“. Cookies sollten grund-

241 Testen Sie, was der Internetdienst Google über Sie weiß: www.google.com/ads/preferences. Falls Sie einen Account haben, auch www.google.com/dashboard.

sätzlich nur für die jeweilige Sitzung akzeptiert werden („Cookies löschen, wenn der Browser geschlossen wird“). Außerdem sollten Cookie-Daten nur dann zurückgesendet werden, wenn das betreffende Webangebot willentlich besucht wird („Drittanbieter-“ bzw. „Third-Party-Cookies“ sollte man deaktivieren).

- Außerdem bieten Webbrowser die Möglichkeit, weitere lokale Daten wie Chronik/Verlauf, Cache und Webseiten-Einstellungen zu löschen bzw. automatisch löschen zu lassen. Diese Daten ermöglichen, dass die Internet-Aktivitäten am lokalen Gerät (z. B. auch in einem Internet-Café oder an einem Internet-Zugang in einer öffentlichen Bibliothek) nachvollzogen werden können. Zudem nutzen einige Webseiten diese Mechanismen, um eine mit Cookies vergleichbare Tracking-Funktionalität zu erzielen, die die Nutzenden nicht so leicht kontrollieren können. Über derartige Speichermöglichkeiten verfügen teilweise auch Browser-Erweiterungen wie z. B. das Flash-Plugin.
- Grundsätzlich sollte man nicht dauerhaft bei einem Webdienst eingeloggt bleiben. Nach jedem Logout sollte man zudem die erstellten Cookies löschen.
- Es gibt für einige Browser (Firefox, Chrome, Safari) empfehlenswerte Browser-Erweiterungen gegen Web-Tracking:
 - **BetterPrivacy** ermöglicht automatisches gründliches Löschen von Cookies, Flash-Daten u. a..
 - **Ghostery** verhindert die Datenweitergabe an Trackingdienste, indem deren Objekte (Werbebanner, Webbugs, Social Plugins) nicht oder erst nach dem Anklicken abgerufen werden.
 - **Flashblock**: Flash-Elemente wie Werbebanner oder Videos werden nur auf Wunsch (beim Anklicken) geladen und gestartet.
 - **Adblock plus** stoppt das Laden von Werbebannern und damit die Datenerhebung durch die jeweiligen Werbedienste. Diese Dienste arbeiten oft sehr arbeitsteilig. Aus Datenschutzsicht bedeutet dies, dass der Aufruf eines einzelnen Webangebotes dazu führen kann, dass Daten wie z. B. die Internet-Adresse an eine zweistellige Anzahl von weltweit verteilten Firmen versendet werden, die entsprechend viele Tracking-Cookies setzen.

Der Microsoft-Browser Internet Explorer hat mit den sog. „**Tracking Protection Lists**“ bereits einen integrierten Schutz gegen Tracking, den die Nutzenden jedoch erst manuell aktivieren müssen. Technisch soll dieser Filter Webdienste automatisch identifizieren, die auf vielen anderen Webseiten Objekte einbinden und damit potenziell Tracking durchführen könnten. Man kann aber auch vorgefertigte Listen²⁴² mit den bereits bekannten Trackingdiensten herunterladen.

Derzeit wird im World Wide Web Consortium (W3C) über die Standardisierung eines Verfahrens namens „**Do Not Track (DNT)**“ diskutiert. Dieses ist bereits in mehreren Browsern integriert und ermöglicht, die jeweiligen Server zu informieren, ob man Tracking gestattet oder verbietet. Die Einstellungen dafür finden sich in der Regel in den Datenschutzeinstellungen. In den noch laufenden Standardisierungsbestrebungen soll erreicht werden, dass jeder Webdienst diese von den Nutzenden übermittelte Vorgabe auch beachtet. Allerdings werden sich Anbieter nur dann danach richten, wenn bei Missachtung empfindliche rechtliche Konsequenzen drohen. Zudem ist noch unklar, wie es zu werten ist, wenn keine Vorgabe gesendet wird. Nur wenn in diesem Fall kein Tracking stattfindet, wäre ein künftiger „Do Not Track“-Standard mit der europäischen E-Privacy-Richtlinie²⁴³ vereinbar, die Cookies nur bei ausdrücklicher Einwilligung der Betroffenen erlaubt. Allerdings leisten die Online-Werbeindustrie und große Internet-Unternehmen dem Vernehmen nach massiven Widerstand gegen einen solchen „Do Not Track“-Standard.

Aufgrund unzureichender internationaler Durchsetzungsmöglichkeiten für rechtliche Rahmenbedingungen ist es empfehlenswert, auch auf Selbstschutzmaßnahmen zu setzen. Neben einigen technischen Maßnahmen ist das Verhalten der Einzelnen mitentscheidend für den Umfang der Personenprofile, die von Dritten erstellt werden können.

242 Z. B. vom Fraunhofer Institut für Informationstechnik: www.sit.fraunhofer.de/de/tpl.html

243 Art. 5 Abs. 3; siehe dazu JB 2011, 12.1

16.4.2 Wie kann ich eigene Daten löschen?

Ein weiteres Problem stellen personenbezogene Daten dar, die mit oder ohne ursprüngliche Einwilligung der Betroffenen im Internet veröffentlicht sind. Uns erreichen insbesondere Beschwerden zu Veröffentlichungen in sozialen Netzwerken, in Foren und auf Portalen, die Adressen von Gewerbetreibenden veröffentlichen, sowie zu beleidigenden bzw. diskriminierenden Äußerungen in privaten Blogs oder auf dubiosen Webseiten.

Oft ist der Ausgangspunkt einer Beschwerde, dass bei Eingabe des eigenen Namens in eine Suchmaschine ein unerwünschter Treffer angezeigt wird. Die erste Forderung der Betroffenen ist meist, dass dieser Inhalt aus der jeweiligen Suchmaschine – meist Google – gelöscht werden soll. Übersehen wird dabei jedoch, dass der beanstandete Inhalt in der Regel nicht von der Suchmaschine selbst veröffentlicht wird, sondern diese nur auf die eigentliche Quelle auf einer anderen Internetseite verweist. In diesen Fällen kann der Betreiber der Suchmaschine auf das Bundesdatenschutzgesetz verweisen, nach dem das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten zulässig ist, wenn die Daten allgemein zugänglich sind, es sei denn, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Veröffentlichung offensichtlich überwiegen.²⁴⁴

Betroffene sollten jedoch zuerst versuchen, die Daten an der Quelle zu entfernen. Dazu sollten sie den Betreiber des jeweiligen Webangebotes anschreiben und zur Löschung der jeweiligen Daten auffordern. Diese Aufforderung sollte eine Begründung enthalten, weshalb die Veröffentlichung als unzulässig angesehen wird, und die zu entfernenden Passagen sollten konkret benannt werden, auch indem der Link auf die betreffenden Webseiten angegeben wird. Gründe für die Löschaufforderung könnten z. B. sein, dass die Veröffentlichung das Recht am eigenen Bild²⁴⁵ oder andere Persönlichkeitsrechte verletzt. Soll ein von Betroffenen selbst erstellter und auf der jeweiligen Plattform veröffentlichter Inhalt wieder entfernt werden, muss gegenüber dem Betreiber der Plattform eine ursprünglich erteilte Einwilligung zur Veröffentlichung widerrufen werden.

244 § 28 Abs. 1 Satz 1 Nr. 3 BDSG

245 § 22 Kunsturhebergesetz

Zu berücksichtigen ist auch, dass das Bundesdatenschutzgesetz nur auf personenbezogene Daten anwendbar ist. Oft kann daher nicht die Löschung eines Inhaltes gefordert werden, sondern nur die Entfernung des Personenbezuges. In Diskussionsforen kann dies z. B. dadurch erreicht werden, dass der Name der Verfasserin oder des Verfassers aus dem Beitrag entfernt oder durch ein nicht zur Identität der oder des Betroffenen auflösbares Pseudonym ersetzt wird. Betroffene sollten daher um Löschung, alternativ um Pseudonymisierung bitten.

Sollte der direkte Kontakt zum Betreiber zu keinem Erfolg führen, kann die für den Hauptsitz des Unternehmens zuständige Aufsichtsbehörde um Unterstützung gebeten werden.

Da Suchmaschinen einen kurzen Ausschnitt des Inhaltes der eigentlichen Webseite darstellen und außerdem oft eine Möglichkeit gegeben wird, das gesamte Dokument als Kopie anzuzeigen, muss das oben genannte „offensichtlich überwiegende schutzwürdige Interesse“ der Betroffenen auch von Suchmaschinen berücksichtigt werden. Insbesondere kann dies zutreffen, wenn die Inhalte auf den Originalwebseiten entfernt worden sind. Viele Suchmaschinen bieten eine technische Schnittstelle zur Meldung von „veralteten“ Suchergebnissen an.²⁴⁶ Oft besteht auch die Möglichkeit, Verweise auf rechtswidrige Inhalte anzuzeigen. Die Nutzung dieser Schnittstellen ist zu empfehlen, da auf diese Weise Anträge schneller bearbeitet werden. Die Aktualisierung veralteter Verweise auf Webseiten erfolgt in der Regel automatisiert innerhalb weniger Stunden.

Insbesondere bei eigenen Inhalten wie z. B. der in letzter Zeit diskutierten „Auto-Vervollständigungs“-Funktion der Suchmaschine Google kann sich der Betreiber jedoch nicht seiner Verantwortung entziehen. Die Argumentation, die Funktion schlage nur die häufigsten Suchanfragen der Nutzenden als Eingabehilfe vor, sodass es sich um Inhalte Dritter handele, für die der Betreiber keine Verantwortung trägt, geht fehl, da die Nutzenden diese Daten gerade nicht veröffentlichen. Der Deutsche Juristentag hat deshalb im September den Gesetz-

246 Für die Suchmaschine Google: <https://www.google.com/webmasters/tool/removals>. Für die Nutzung ist das Anlegen eines Accounts erforderlich, der jedoch nach Ende des Verfahrens wieder gelöscht werden kann. Betroffene sollten dafür eine gesonderte E-Mail-Adresse verwenden.

geber aufgefordert, die datenschutzrechtliche Verantwortung der Betreiber von Suchmaschinen klarzustellen.²⁴⁷

Bei unzulässigen Veröffentlichungen personenbezogener Daten sollten zuerst die Betreiber der jeweiligen Webangebote kontaktiert werden, bei Misserfolg die zuständige Aufsichtsbehörde. Suchmaschinen müssen in der Regel nur Verweise auf nicht mehr existierende Daten löschen, sind aber für eigene Inhalte verantwortlich.

16.5 Smartphones und Apps

2010²⁴⁸ haben wir ausführlich über die Datenschutzfragen bei Smartphones und sog. Smartphone-Apps berichtet. Problematisch ist dabei, dass die Apps aus unbekanntem Quellen stammen können und grundsätzlich Zugriff auf die im Gerät gespeicherten Daten haben bzw. über die Sensoren Daten erheben können.

In der Zwischenzeit führten mehrere Organisationen, insbesondere aus den Bereichen Presse und Verbraucherschutz, Tests der gebräuchlichsten Apps durch. Gefunden wurden erhebliche Mängel: Vielfach werden mehr Daten als nötig weitergegeben und IT-Sicherheitsmaßnahmen unzureichend dokumentiert. Wir waren an der grundsätzlichen Bewertung der Ergebnisse mehrerer Vergleichstests der Stiftung Warentest beteiligt.

Das häufigste Problem ist die Übermittlung von Geräte-Identifikationsnummern (UDIDs) an die Hersteller der jeweiligen App, den Hersteller des Betriebssystems oder gar an Dritte. Der übliche Zweck der Übermittlung ist die Profilerstellung über das Nutzerverhalten,²⁴⁹ um z. B. personalisierte Wer-

247 Beschlüsse des 69. Deutschen Juristentags, Abt. IT- und Kommunikationsrecht, Nr. 28

248 JB 2010, 2.5; Smartphone-Apps sind kleine Programme unterschiedlicher Hersteller, die speziell für Smartphones bzw. Tablet-Computer erstellt werden und direkt online über sog. App-Stores, die oft vom Hersteller des Betriebssystems bereitgestellt werden, verkauft werden.

249 Einzelne ggf. anonyme Daten, wie z. B. ermittelte Aufenthaltsorte, können durch die UDID immer wieder einem Gerät und damit der oder dem Nutzenden zugeordnet werden.

bung zu ermöglichen oder Statistiken über die App-Nutzung zu erstellen. In der Regel werden die Nutzenden darüber nicht aufgeklärt, und insbesondere steht keine Möglichkeit zur Verfügung, dieser Art der Datennutzung zu widersprechen.

Andere Apps übermitteln z. B. ohne Einwilligung das gesamte Adressbuch zu einem Server des Anbieters. In vielen Fällen kann der Zweck der Übermittlung mit bestimmten Aspekten der zu erbringenden Dienstleistung begründet werden. So ist ein Adressbuchabgleich bei Diensten sinnvoll, die SMS-ähnliche Chatfunktionen anbieten und zur Adressierung die Mobiltelefonnummer verwenden. So kann den Nutzenden sofort mitgeteilt werden, wer über den jeweiligen Dienst erreichbar ist. Dennoch muss der Anbieter vor Einsatz dieser Funktion eine Einwilligung einholen und Maßnahmen ergreifen, die die Datenübermittlung soweit wie möglich begrenzen. Im obigen Beispiel genügt es dazu, allein die Telefonnummer zu übermitteln. In anderen Fällen kann auch der Einsatz bestimmter kryptografischer Techniken, wie z. B. Hashfunktionen, angezeigt sein, die den Missbrauch von Daten durch den Anbieter selbst verhindern oder zumindest wesentlich erschweren.

Es gibt zudem Unternehmen, wie z. B. *flurry.com*, die sich darauf spezialisiert haben, ausführliche Daten über die oder den jeweiligen Nutzenden zu sammeln und den App-Anbietern zu verkaufen. Diese Informationen werden durch Langzeitprotokollierung des Verhaltens von Smartphone-Nutzenden aufgrund genutzter Apps und auf der Basis von Sensordaten wie der GPS-Aufenthaltsorte erhoben. Bei dem Umfang der erhobenen Daten muss man davon ausgehen, dass diese eine persönliche Identifizierung ermöglichen. Die Erhebung und Weiterleitung an Dritte erfordert die Einwilligung der Nutzenden. Die derzeit übliche Umsetzung, bei der keine wirksame Einwilligung eingeholt wird, keine ausreichende Information der Nutzenden erfolgt und im besten Fall ein Widerspruch ermöglicht wird, ist in Deutschland und dem Europäischen Wirtschaftsraum unzulässig.²⁵⁰

250 Siehe Art. 5 Abs. 3 E-Privacy-Richtlinie 2002/58/EG, geändert durch die Richtlinie 2009/136/EG; Stellungnahme 2/2010 der Art. 29-Datenschutzgruppe vom 22. Juni 2010 zur Werbung auf Basis von Behavioural Targeting (WP 171), siehe Dokumentenband 2010, S. 92 ff.

Wir haben begonnen, Anbieter von Smartphone-Apps zu prüfen. Insbesondere haben wir Anbieter mit anscheinend unnötigen Datenübermittlungen um Stellungnahme gebeten. In einzelnen Fällen konnte die Notwendigkeit überzeugend dargelegt werden. Einige Anbieter haben die jeweiligen Funktionen geändert. Die Prüfungen werden wir fortsetzen.

2010²⁵¹ haben wir zudem die Hersteller von Smartphone-Betriebssystemen aufgefordert, Datenschutzfunktionalitäten zu entwickeln bzw. zu verbessern, die den Zugriff von App-Entwicklern auf im Gerät gespeicherte Daten bzw. Gerätesensoren beschränken oder zumindest unter Kontrolle der Nutzenden stellen. Zumindest ein bekannter Hersteller hat in der Zwischenzeit die Nutzerkontrolle wesentlich verbessert. So muss in der aktuellen Version des Apple Betriebssystems iOS²⁵² jede App die Nutzenden um Einwilligung bitten, bevor z. B. der Zugriff auf das Adressbuch, die Fotosammlung oder den Kalender gestattet wird. Im Gegensatz zum weitverbreiteten Google-Produkt Android²⁵³ müssen Nutzende nicht zwangsläufig alle erbetenen Zugriffsrechte gewähren, um die App nutzen zu können. Die Nutzenden können einzeln und je nach Situation entscheiden, ob und welche Zugriffe gestattet werden sollen. Diese Entscheidungen sind zudem nachträglich korrigierbar. Auch beim Microsoft Windows Phone 8²⁵⁴ können Zugriffsrechte einzeln vergeben werden.

Die Zweckbindung der erhobenen Daten wird bisher – auch aus Gründen der technischen Realisierbarkeit – nur beschränkt umgesetzt: Entwickler von iOS-Apps können nun Gründe dafür angeben, weswegen bestimmte Rechte erbeten werden. Allerdings ist die Angabe der Gründe, woraus sich eine Zweckbindung ableiten ließe, bisher noch optional und nicht formalisiert. Zudem fehlt eine Dokumentation der Datenflüsse, die eine Prüfung auf Einhaltung der Zweckbindung durch die Nutzenden oder eine Prüfinstanz ermöglichen würde.

Auch in Bezug auf Tracking-Techniken wurden zumindest erste technische Änderungen eingeführt. So soll der Zugriff auf die Geräte-Identifikationsnum-

251 JB 2010, 2.5

252 iOS ist das Standard-Betriebssystem der Apple-Produkte iPhone und iPad.

253 Android ist ein herstellerunabhängiges Betriebssystem für mobile Geräte wie Smartphones, Mobiltelefone, Netbook und Tablets.

254 Windows Phone 8 ist die derzeit aktuelle Version des Windows Phone-Betriebssystems für Mobiltelefone.

mer zukünftig in iOS unterbunden werden. Als Ersatz wird eine Werbe-ID bereitgestellt, die prinzipiell änderbar ist und deren Nutzung von den Nutzenden deaktiviert werden kann. Allerdings handelt es sich hierbei um eine sog. Opt-Out-Lösung. Dies bedeutet, dass Nutzende selbst aktiv werden und eine Systemeinstellung – über die sie nicht ausreichend informiert werden – ändern müssen. Auch die möglichen Optionen sind sehr eingeschränkt: Es besteht derzeit nur durch Rücksetzen des Systems (verbunden mit dem Löschen aller Daten) die Möglichkeit, die ID und damit das Pseudonym zu wechseln. Hier sollte eine einfachere Möglichkeit und ein automatischer Wechsel in Zeitintervallen geschaffen werden. Zudem sollten App-spezifisch verschiedene Werbe-IDs zum Einsatz kommen.²⁵⁵

Befürchtungen über mögliche Datenschutzverstöße von Smartphone-Apps haben sich bewahrheitet. Wir haben und werden weiterhin Anbieter zur Einhaltung der Datenschutzbestimmungen anhalten. Hersteller von Smartphone-Betriebssystemen entwickeln erste technische Lösungen gegen unzulässige Datennutzung.

16.6 Intelligente Werbeflächen

Seit einigen Jahren sind große digitale Werbetafeln an Bushaltestellen, in Fußgängerzonen, auf Verkehrsinseln, an Magistralen oder an Gebäuden ein gewohntes Bild in deutschen Städten. Die Tafeln sind werbewirksamer als die mittlerweile antik anmutenden Litfaßsäulen und erregen mit ihrer Art der Informationsvermittlung durch LED-Displays oder interaktive Grafiken größere Aufmerksamkeit bei den Konsumenten.

Um diese Aufmerksamkeit weiter zu steigern, experimentieren Hersteller von digitalen Werbeflächen auch mit Videotechnik. Ein Hersteller hat uns sein Produkt vorgestellt und um unsere Einschätzung hinsichtlich des Einsatzes von

255 Weitere Details zu Datenschutz-Funktionalitäten sowie möglichen Systemeinstellungen sind nachlesbar unter <http://www.macwelt.de/ratgeber/iOS-6-Datenschutz-mit-iOS-6-6783237.html>.

Videokameras im öffentlich zugänglichen Raum gebeten. Mithilfe einer in der Werbefläche integrierten Kamera werden Live-Bilder gezeigt, die sich hinter der Werbefläche befinden; man kann also durch die Werbefläche hindurchsehen wie durch eine Glasscheibe. In das Live-Bild auf der Werbefläche werden Grafiken, Animationen oder 3D-Modelle des zu bewerbenden Produkts eingeblendet und direkt über ein passierendes Objekt gelegt. Beim Hindurchsehen durch die Werbefläche werden z. B. alle vorbeifahrenden PKW mit einem Bild der zu bewerbenden Automarke verfremdet. Mithilfe dieser Technik könnten auch vorbeigehende Passanten mit der zu bewerbenden Kleidung eines Bekleidungs Herstellers „angezogen“ werden.

Da ausschließlich Live-Bilder erzeugt und weder Bilddaten gespeichert noch ins Internet übertragen werden, ist das Projekt unter diesen Voraussetzungen solange nicht zu beanstanden, wie lediglich Gegenstände (Autos) zu Werbezwecken verfremdet werden. Sollten allerdings identifizierbare Personen ohne ihre Einwilligung in ihrem äußeren Erscheinungsbild technisch manipuliert werden, wäre dies eine Verletzung ihres Persönlichkeitsrechts.

16.7 Aus der Arbeit der „Berlin Group“

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. „Berlin Group“) hat auf ihrer 51. Sitzung in Sopot (Polen) ein viel beachtetes Arbeitspapier zu Fragen des Datenschutzes und der Privatsphäre beim Cloud Computing („Sopot Memorandum“)²⁵⁶ verabschiedet. Darin untersucht die Arbeitsgruppe die Verarbeitung personenbezogener Daten beim Cloud Computing, benennt die sich daraus ergebenden Risiken und gibt Empfehlungen zu deren Verringerung. Insbesondere dürfen durch Cloud Computing Datenschutzstandards im Vergleich zur herkömmlichen Datenverarbeitung nicht abgesenkt werden.²⁵⁷

²⁵⁶ Dokumentenband 2012, S. 171

²⁵⁷ Zur Situation in Deutschland siehe JB 2011, 2.1.1

Basierend auf dem Arbeitspapier der „Berlin Group“ hat die Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre im Oktober in Punta del Este (Uruguay) eine Entschließung zum Cloud Computing gefasst, in der Kernforderungen zur Sicherung des Schutzes der Privatsphäre bei der Anwendung dieser Technologie zusammengefasst sind.²⁵⁸

258 Dokumentenband 2012, S. 168

17 Technik und Organisation

17.1 Kontrolle bei den Bäder-Betrieben

Die Berliner Bäder-Betriebe betreiben als Anstalt des öffentlichen Rechts die meisten städtischen Bäder. Mehrere Eingaben des Personalrats veranlassten uns zu einer Kontrolle.

Die vorher angeforderten Dokumente waren ausnahmslos unvollständig, widersprüchlich und in den meisten Fällen veraltet. Sie waren teilweise in Eile erarbeitet worden und entsprachen nicht den Vorgaben der IT-Standards des Landes. Für die Vorbereitung der Kontrolle waren sie deshalb nur bedingt verwendbar.

Die Unterlagen sollen im Wesentlichen die nach dem Berliner Datenschutzgesetz²⁵⁹ gebotene Transparenz der Datenverarbeitung gegenüber interessierten Nutzenden der Bäder gewährleisten. Ein wichtiger Bestandteil sind die Dateibesreibungen, deren Gestaltung in § 19 BlnDSG geregelt ist. Danach hat jede Person das Recht, ohne Angabe von Gründen in den ersten Teil der Dateibesreibung Einsicht zu nehmen. Wir haben einen repräsentativen Ausschnitt untersucht und festgestellt, dass keine einzige Dateibesreibung ohne Mängel war. Deshalb haben wir Hinweise für die Korrektur aller Dateibesreibungen gegeben.

Während der Kontrolle wurde ferner festgestellt, dass der Stellvertreter des behördlichen Datenschutzbeauftragten auch als Regionalleiter tätig ist. Durch diese Leitungsfunktion ergab sich ein Interessenkonflikt, sodass eine objektive Amtsausführung zweifelhaft erschien. Durch die inzwischen erfolgte Bestellung eines neuen Stellvertreters wurde dieser Mangel behoben.

Der Einsatz der betriebswirtschaftlichen Standardsoftware ERP der Firma SAP erforderte aufgrund der hohen Komplexität eine gesonderte Betrachtung. Auch hier fielen die Inkonsistenz und die fehlende Aktualität der Unterlagen auf. Die konsequente Umsetzung eines Sicherheitsprozesses und ein stets aktuelles

²⁵⁹ § 5 Abs. 2 Nr. 6 BlnDSG

Berechtigungskonzept hätten viele der von uns festgestellten Mängel verhindern können. Als Beispiel ist die Vermengung von administrativen Funktionen mit Funktionen nicht privilegierter Anwender zu nennen. Besonders problematisch war die unzulässige Nutzung von Echtdaten im SAP-Testsystem. Um förmliche Beanstandungen wegen rechtswidriger Verarbeitung personenbezogener Daten zu vermeiden, empfehlen wir, aus Echtdatenbeständen durch Anonymisierung Testdatenbestände zu generieren und zum Testen zu verwenden. Hauptkritikpunkt war das Fehlen eines Informationssicherheitskonzepts, das den Anforderungen des § 5 Abs. 3 BlnDSG entspricht. Es gab lediglich Teilkonzepte, die nicht nach den IT-Standards des Bundesamts für Sicherheit in der Informationstechnik²⁶⁰ gefertigt waren. Insbesondere die fehlende Aktualität der Konzepte und Pläne war auffallend.

Obwohl die festgestellten Mängel stellenweise so gravierend waren, dass eine förmliche Beanstandung²⁶¹ hätte ausgesprochen werden können, sahen wir zunächst davon ab. Uns wurde glaubhaft versichert, dass mit einer gründlichen Aufarbeitung der festgestellten Mängel unverzüglich begonnen wird.

Um die informationstechnische Sicherheit zu gewährleisten, ist die Erstellung eines Sicherheitskonzepts eine wichtige Voraussetzung. Die Einbindung des Konzepts in einen Sicherheitsprozess garantiert seine unverzichtbare Aktualität.

17.2 Organisation des Datenschutzes in den Bezirken

Der behördliche Datenschutzbeauftragte eines Bezirksamtes hat sich an uns gewandt, weil er bei der Prüfung der Meldungen zur Dateienüber-sicht²⁶² auf Vollständigkeit die notwendige Unterstützung der Fachabteilungen vermisste.

260 BSI-Standards 100-2 und 100-3

261 § 26 Abs. 1 BlnDSG

262 § 19 a Abs. 1 i.V.m. § 19 Abs. 2 BlnDSG

Die Daten verarbeitende Stelle hat den behördlichen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben, zu denen die Führung der Beschreibungen und Verzeichnisse nach § 19 Abs. 2 BlnDSG gehört, zu unterstützen.²⁶³ Wir haben den Bezirksbürgermeister gebeten, sich dafür einzusetzen, dass dem behördlichen Datenschutzbeauftragten die erforderlichen Unterlagen zeitnah zur Verfügung gestellt werden.

Auch im regelmäßig bei uns tagenden Gesprächskreis der behördlichen Datenschutzbeauftragten der Bezirke waren die fehlende Unterstützung durch die Fachabteilungen und zusätzlich wahrzunehmende Aufgaben wiederholt Thema. Wir haben dies zum Anlass genommen, die behördlichen Datenschutzbeauftragten der Bezirke um die Beantwortung eines Fragenkataloges zu bitten, um einen Überblick über die Organisation des Datenschutzes in den Bezirken zu erhalten.

Hier einige Ergebnisse: Zwei behördliche Datenschutzbeauftragte nehmen zusätzlich die Funktion des Antikorruptionsbeauftragten wahr. Den Interessenkonflikt bei der gleichzeitigen Wahrnehmung dieser Aufgaben haben wir gegenüber dem Bezirksamt Pankow beanstandet,²⁶⁴ ohne dass sich nach Ablauf von mehr als zwei Jahren daran etwas geändert hat. Auch der Bezirk Lichtenberg handelt entsprechend rechtswidrig.

Das zur Verfügung stehende Zeitkontingent in den Bezirken reicht von 25 – 100 % der regelmäßigen wöchentlichen Arbeitszeit. Die Mehrheit hält mindestens die Hälfte der regelmäßigen wöchentlichen Arbeitszeit für erforderlich, um die Aufgabe wirkungsvoll erfüllen zu können. Anlassunabhängige Kontrollen wurden überwiegend nicht durchgeführt. Bezirkliche Datenschutzbeauftragte sollten in einigen Bezirken von anderen Arbeiten entlastet werden.

Die Umsetzung der gesetzlichen Pflicht, die Festlegungen zu automatisierten Verarbeitungen den behördlichen Datenschutzbeauftragten für die Dateienübersicht zu melden, ist ein generelles Problem in den Bezirken. Die Festlegungen erfolgen teilweise spät oder gar nicht. Damit wird nicht nur die Dokumentationspflicht nicht in der gebotenen Form erfüllt. Es werden auch die

263 § 19 a Abs. 3 BlnDSG

264 JB 2010,12.4

Rechte der Menschen verkürzt, die diese Unterlagen einsehen können.²⁶⁵ Ferner wird uns die Wahrnehmung unserer Aufgabe erschwert, die Einhaltung der Vorschriften zum Datenschutz zu kontrollieren.

Alle Dienststellen haben die behördlichen Datenschutzbeauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. In einigen Bezirken sind strukturelle Verbesserungen überfällig.

265 § 7 Satz 1 Nr. 4 BlnDSG

18 Informationsfreiheit

18.1 Informationsfreiheit in Deutschland

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) tagte in diesem Jahr unter dem Vorsitz des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, der seit 2012 beide Aufgaben wahrnimmt. Mit einer Entschließung appellierte die IFK an die Bundesregierung, sich im Europäischen Rat für mehr Transparenz einzusetzen und den freien Zugang zu Dokumenten der EU²⁶⁶ nicht zu beschneiden.²⁶⁷ Die IFK hat sich außerdem dafür ausgesprochen, dass Kooperationsverträge zwischen Wissenschaft und Unternehmen grundsätzlich offengelegt werden. Das betrifft auch die Finanzierung von Forschungsprojekten. Da reine Selbstverpflichtungen der Universitäten und Forschungseinrichtungen hierfür nicht ausreichen, sollten die Informationsfreiheitsgesetze des Bundes und der Länder auch hierfür eine grundsätzliche Offenlegungspflicht vorsehen.²⁶⁸ Anlässlich von Infektionsfällen auf Neugeborenen-Stationen sollten nach Ansicht der IFK in den Krankenhäusern bundesweit verpflichtende Hygienestandards festgelegt werden, die über das Infektionsschutzgesetz und landesrechtliche Hygienebestimmungen²⁶⁹ hinausgehen und deren Veröffentlichung verpflichtend ist.²⁷⁰ Schließlich appellierte die IFK an die Parlamente von Bund und Ländern, selbst Vorreiter in Sachen Transparenz zu werden, und zwar nicht nur in Bezug auf die Einkünfte von Abgeordneten, sondern z. B. auch in Bezug auf Unterlagen der Ausschüsse und Plenarsitzungen.²⁷¹ Im nächsten Jahr wird die IFK unter dem Vorsitz des Thüringischen Landesbeauftragten für den Datenschutz und die

266 EU-Verordnung 1049/2001

267 Entschließung vom 12. Juni 2012: Informationsfreiheit auf europäischer Ebene ausbauen, nicht einschränken!, siehe Dokumentenband 2012, S. 185

268 Entschließung vom 12. Juni 2012: Mehr Transparenz bei der Wissenschaft – Offenlegung von Kooperationsverträgen –, siehe Dokumentenband 2012, S. 186

269 Siehe 9.1

270 Entschließung vom 27. November 2012: Mehr Transparenz bei Krankenhaushygienedaten, siehe Dokumentenband 2012, S. 187

271 Entschließung vom 27. November 2012: Parlamente sollen in eigener Sache für mehr Transparenz sorgen!, siehe Dokumentenband 2012, S. 187. In Berlin könnten die Forderungen umgesetzt werden in einem Parlamentsinformationsgesetz, siehe hierzu JB 2011, Einleitung (S. 12).

Informationsfreiheit stattfinden, dem mit der Änderung des Thüringer Informationsfreiheitsgesetzes zum Jahresende die Funktion des Informationsfreiheitsbeauftragten übertragen wurde. Damit nehmen in allen elf Bundesländern mit Informationsfreiheitsgesetzen ebenso wie im Bund die Datenschutzbeauftragten zugleich die Aufgaben eines Beauftragten für Informationsfreiheit wahr.

Als ein Meilenstein der Informationsfreiheit kann das im Juni beschlossene **Hamburgische Transparenzgesetz** bezeichnet werden, das im Oktober in Kraft getreten ist.²⁷² Es ist das Ergebnis der Volksinitiative „Transparenz schafft Vertrauen“ und wurde in der Hamburgischen Bürgerschaft von allen Fraktionen unterstützt. Zu den wesentlichen Neuerungen gehört die proaktive Veröffentlichung zahlreicher Dokumente von öffentlichem Interesse in einem Informationsregister. Für die Bereitstellung dieses Registers wurde der hamburgischen Verwaltung eine Frist bis Herbst 2014 eingeräumt. Insbesondere durch die grundsätzliche Abkehr von der sog. Holschuld hin zur sog. Bringschuld ist das Hamburgische Transparenzgesetz als das fortschrittlichste in der Bundesrepublik zu bezeichnen: Die Menschen müssen sich nun nicht mehr als „Bittsteller“ in Bezug auf Informationen des Staates fühlen, sondern dieser muss künftig eine Vielzahl von für die Öffentlichkeit interessanten Informationen von sich aus allgemein zugänglich machen. Daneben bleibt das Recht des Einzelnen, Zugang zu bestimmten weiteren Informationen zu verlangen, erhalten.

18.2 Informationsfreiheit in Berlin

Die Entwicklung in Hamburg blieb in Berlin nicht folgenlos: So hat die Fraktion Bündnis 90/Die Grünen den **Entwurf eines Berliner Transparenz- und Informationsfreiheitsgesetzes** in das Abgeordnetenhaus eingebracht.²⁷³ Es soll die Vorzüge des bislang geltenden IFG²⁷⁴ zusammenführen mit den fortschrittlichen Regelungen des hamburgischen Modells, damit auch in Berlin der grund-

272 Hmb GVBl. S. 271

273 Drs. 17/0456

274 Z. B. den Katalog der nicht schutzbedürftigen personenbezogenen Daten nach § 6 Abs. 2 IFG; siehe auch Einleitung

legende Paradigmenwechsel zu einem Informationszugang vollzogen werden kann, der grundsätzlich von Amts wegen und nicht erst auf Antrag zu gewährleisten ist. Da sämtliche Verwaltungsbereiche von der proaktiven Informationspflicht betroffen sein werden, wurde der Gesetzentwurf an 14 Fachausschüsse zur Beratung überwiesen. Ob der Gesetzentwurf deshalb bis zum Ende der Legislaturperiode abschließend beraten wird, bleibt abzuwarten.

Die gesetzgeberischen Aktivitäten zeigen, dass der Stellenwert der Informationsfreiheit auch in der Politik in den letzten Jahren deutlich zugenommen hat. Eine **verfassungsrechtliche Verankerung des Anspruchs auf Informationszugang** könnte dies zusätzlich fördern.²⁷⁵ Das Recht, von öffentlichen Stellen Informationen zu erhalten, hat bislang allein in Brandenburg Verfassungsrang. Der Berliner Beauftragte für Informationsfreiheit hat bei allen Fraktionen dafür geworben, sich dem Beispiel Brandenburgs folgend für die Aufnahme eines Grundrechts auf Informationsfreiheit in die Verfassung von Berlin einzusetzen.²⁷⁶ Damit würde die Bundeshauptstadt ein bedeutsames Signal für noch mehr Transparenz staatlichen Handelns aussenden.

In der Vergangenheit haben wir kontinuierlich über **Hygienesiegel im Gaststättenbereich** berichtet.²⁷⁷ Die meisten Bezirke bezweifeln zu Unrecht nach wie vor, dass sie die Ergebnisse von Restaurantüberprüfungen ins Internet stellen dürfen. Daran hat auch das neugefasste Verbraucherinformationsgesetz nichts geändert.²⁷⁸ Während das für den Verbraucherschutz zuständige Bundesministerium seit langem davon ausging, dass jedes Bundesland eine verpflichtende Kennzeichnung von Gastronomiebetrieben einführen darf, hat das für die Wirtschaft zuständige Bundesministerium eine entsprechende gesetzliche Klarstellung gestoppt. Berlin sollte sich nun für eine einheitliche Lösung für alle Bezirke stark machen und ggf. die Erfahrungen auswerten, die mit den derzeit verfügbaren Internet-Plattformen gemacht

275 Siehe bereits die Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 28. November 2011: Informationsfreiheit ins Grundgesetz und in die Landesverfassungen, Dokumentenband 2011, S. 139

276 Die Fraktion Bündnis 90/Die Grünen im Bundestag spricht sich ebenfalls für ein Informationszugangsgrundrecht als Art. 5 Abs. 2a GG aus, siehe BT-Drs 17/9724.

277 Zuletzt JB 2011, 13.2 (S. 190)

278 Siehe die Bekanntmachung der Neufassung des Verbraucherinformationsgesetzes vom 17. Oktober 2012, BGBl. I, S. 2166

wurden.²⁷⁹ Ggf. müssen rechtlich verpflichtende Bestimmungen einheitlich für alle Bezirke geschaffen werden.²⁸⁰

Auch für die **Forschung** sind die Erkenntnisse aus dem **Smiley-Projekt Pankow** von Interesse. So hat sich die Martin-Luther-Universität Halle-Wittenberg an das Bezirksamt Pankow mit der Frage gewandt, ob sie die veröffentlichten Daten für ein Forschungsprojekt²⁸¹ nutzen dürfe. Wir haben dem Bezirksamt auf dessen Bitte um Prüfung mitgeteilt, dass die im Internet veröffentlichten Daten den Forschenden wie jedermann frei zur Verfügung stehen und daher ohne datenschutzrechtliche Einwände von diesen verwendet werden können. Die Forschenden können also sowohl für die Erhebung von Primärdaten (bei den Betrieben) als auch von Sekundärdaten (beim Bezirksamt) die Angaben in der Liste (z. B. Adressdaten) frei verwenden. Allerdings war zu bedenken, dass ein vollständiger Zugriff auf die Datenbestände der Lebensmittelaufsicht mehr Angaben über die Betriebe und die bei ihnen durchgeführten Lebensmittelkontrollen beinhaltet. Für den Fall, dass die Einsichtnahme der Unterlagen des Bezirksamtes in personenbeziehbarer Form geplant war, musste den Betroffenen nach bisheriger Rechtslage die Gelegenheit zur Stellungnahme eingeräumt werden.²⁸² Nach neuer Rechtslage kann von der Anhörung des Betriebes abgesehen werden; stattdessen ist ihm der beabsichtigte Informationszugang bekanntzugeben und ein ausreichender Zeitraum zur Einlegung von Rechtsbehelfen einzuräumen.²⁸³ Bei der Entscheidung des Bezirksamtes konnte zugunsten des Informationszugangs die Verwendung der Daten zu reinen Forschungszwecken und die im weiteren Verarbeitungsprozess angestrebte Anonymisierung der Daten berücksichtigt werden.

279 Smiley-Projekt im Bezirksamt Pankow sowie „Sicher essen“ der Senatsverwaltung für Justiz und Verbraucherschutz

280 Dabei sollten auch die Anforderungen berücksichtigt werden, die das Verwaltungsgericht Berlin an die „Sicher essen“-Liste der Senatsverwaltung für Justiz und Verbraucherschutz gestellt hat (VG 14 K 79.11).

281 „Verhaltensökonomische Analyse moralischer Risiken in der Lebensmittelproduktion“

282 § 4 Abs. 1 Satz 2 Nr. 1 Verbraucherinformationsgesetz –VIG (a. F.)

283 Bis zu 14 Tage, siehe § 5 Abs. 1 und 4 Verbraucherinformationsgesetz –VIG (n. F.)

18.3 Einzelfälle

Viel Ärger um Senatsbeschlüsse

Ein Petent begehrte bei der Senatskanzlei Auskunft über die Rechtsgrundlage für die Einführung des sog. „berlinpasses“, nachdem die Senatsverwaltung für Gesundheit und Soziales mitgeteilt hatte, dass der „berlinpass“ auf einen Senatsbeschluss aus dem Jahr 2008 zurückgehe. Die Senatskanzlei teilte ihm mit, dass Senatsbeschlüsse generell nicht veröffentlicht würden, und verwies ihn auf eine Pressemitteilung der (damaligen) Senatsverwaltung für Integration, Arbeit und Soziales zur Einführung des „berlinpasses“. Die Senatskanzlei begründete dies uns gegenüber damit, dass dem Informationszugang einerseits der Schutz des behördlichen Entscheidungsprozesses entgegenstünde,²⁸⁴ da zu den Beratungen auch deren Ergebnisse bzw. Beschlüsse gehörten, andererseits Senatsbeschlüsse nach der Geschäftsordnung des Senats (GO Sen) nicht herausgegeben werden dürften, wenn die Herausgabe nicht ausdrücklich im Senatsbeschluss vorgesehen sei,²⁸⁵ dies sei beim Senatsbeschluss zum „berlinpass“ jedoch nicht der Fall. Im Übrigen würden Senatsbeschlüsse dem Bürger ohnehin nicht weiterhelfen, die Pressemitteilungen seien in dieser Hinsicht viel informativer.

Die Auffassung der Senatskanzlei war in mehrfacher Hinsicht rechtsirrig. Der Schutz des behördlichen Entscheidungsprozesses²⁸⁶ umfasst nur den sog. Kernbereich exekutiver Eigenverantwortung, d. h. nur die Beratungen des Senats selbst, nicht jedoch deren Ergebnisse wie etwa Senatsbeschlüsse, soweit hierdurch auch künftig die freie Willensbildung nicht beeinträchtigt werden kann. Auch kann die GO Sen als untergesetzliche Regelung allenfalls ausfüllen, was vom Berliner Informationsfreiheitsgesetz (IFG) vorgegeben wird, nicht aber das IFG außer Kraft setzen. Wir baten die Senatskanzlei, den Petenten unter Berücksichtigung dieser Rechtslage erneut zu bescheiden und die GO Sen an die geltende Rechtslage anzupassen: Danach ist der Informationszugang die Regel und nicht – wie in der GO Sen – die Ausnahme.

284 § 10 Abs. 3 Nr. 1 IFG

285 § 14 Abs. 2 Satz 2 GO Sen

286 § 10 Abs. 3 Nr. 1 IFG

Die Senatskanzlei hielt jedoch an ihrer unzutreffenden Rechtsauffassung fest und verweigerte die Herausgabe des Senatsbeschlusses nun mit der Begründung, dass Beschlüsse in vielen Fällen neben dem Beratungsergebnis auch die ggf. kontrovers diskutierten Auffassungen der Senatsmitglieder wiedergeben würden. Darüber hinaus sei es in vielen Fällen, darunter auch dem vorliegenden, ohnehin nicht möglich, den Beschluss ohne die ihn vorbereitenden Besprechungsunterlagen und Senatsvorlagen inhaltlich zu verstehen. Der betreffende Senatsbeschluss enthielt jedoch gerade keine unterschiedlichen Auffassungen, sondern nur das eigentliche Beratungsergebnis. Darüber hinaus war er auch ohne die ihn vorbereitenden Vorlagen jedenfalls im Hinblick auf das weitere Verfahren äußerst aufschlussreich, da beschlossen wurde, dass eine Vorlage an das Abgeordnetenhaus nicht erforderlich sei und der Beschluss von der Senatsverwaltung für Integration, Arbeit und Soziales bearbeitet werden solle. Wir haben dem Petenten, der an der Umsetzung des Senatsbeschlusses interessiert war, daher empfohlen, bei der zuständigen Senatsverwaltung einen neuen Antrag auf Akteneinsicht hinsichtlich der Vorgänge zu stellen, die auf Grundlage des Senatsbeschlusses angelegt wurden.

Die Senatskanzlei teilte uns erst nach mehreren Monaten und nach mehrmaliger Aufforderung sowie Androhung einer Beanstandung²⁸⁷ wegen Verletzung der Unterstützungspflicht²⁸⁸ mit, dass eine Anpassung der GO Sen weder geboten noch geplant sei.

Senatsbeschlüsse unterliegen als Ergebnis eines Willensbildungsprozesses in der Regel nicht dem Schutz des behördlichen Entscheidungsprozesses. Die Geschäftsordnung des Senats widerspricht der geltenden Rechtslage. Der Senat sollte eine pro-aktive Veröffentlichungspflicht für alle Senatsbeschlüsse einführen.

287 § 26 Abs. 1 BlnDSG

288 § 28 Abs. 1 BlnDSG

Privatisierungsverträge der Wohnungsbaugesellschaft GSW

Mehrere Petenten beehrten bei der Senatsverwaltung für Finanzen Einsicht in die Privatisierungsverträge der GSW. Die Senatsverwaltung lehnte dies mit der Begründung ab, dass dem Informationszugang der Schutz von Betriebs- und Geschäftsgeheimnissen entgegenstünde.²⁸⁹ Der Vertrag beinhalte detaillierte Ausführungen zur Wohnungspolitik und zu geplanten Entwicklungen sowie sonstige Verpflichtungen mit erheblicher Wettbewerbsrelevanz. Darüber hinaus könne auch kein beschränkter Informationszugang erteilt werden,²⁹⁰ da eine sinnvolle Trennung in zu schützende und zu veröffentliche Teile nicht möglich sei. Mit den verbleibenden Aktenteilen könne daher der Zweck des Informationszugangs, nämlich die Kontrolle staatlichen Handelns,²⁹¹ nicht mehr erreicht werden. Schließlich enthalte der Vertrag eine Vertraulichkeitsvereinbarung.

Wir baten die Senatsverwaltung zunächst darum, uns vor der Bescheidung des zwischenzeitlich erhobenen Widerspruchs kurzfristig die Einsichtnahme des Vertrages zu ermöglichen. Nach zwei Wochen ohne Reaktion wurde uns auf telefonische Nachfrage mitgeteilt, dass wir keine Befugnis dazu hätten, auf die Entscheidung der Widerspruchsstelle Einfluss zu nehmen, und daher vor Abschluss des Widerspruchsverfahrens eine Akteneinsicht durch uns nicht in Betracht käme. Eine Nachfrage bei der Widerspruchsstelle ergab, dass rechtliche Zweifel daran bestünden, ob wir überhaupt ein Recht auf Akteneinsicht in den streitgegenständlichen Vertrag hätten. Erst nach Einschaltung des Finanzsenators selbst wurde uns die erbetene Akteneinsicht ermöglicht.

In diesem Fall stand der einzig in Betracht kommende Ausschlussgrund des Schutzes von Betriebs- und Geschäftsgeheimnissen dem Informationszugang nicht entgegen, da der Vertrag – wie sich zwischenzeitlich herausgestellt hatte – bereits im Internet „geleaked“ worden war. Damit war er nicht mehr nur einem begrenzten Personenkreis zugänglich, sondern offenkundig.²⁹² Auch konnte die Vertraulichkeitsabrede dem Informationszugang nicht entgegenste-

289 § 7 IFG

290 § 12 IFG

291 § 1 IFG

292 Zu den Voraussetzungen von Betriebs- und Geschäftsgeheimnissen siehe BVerfG, Beschluss vom 14. März 2006 – 1 BvR 2087/03, Absatz-Nr. 87; siehe bereits JB 2003, 4.9.3

hen, da sie nur gelten sollte, „soweit nicht aufgrund gesetzlicher [...] Vorschriften [...] eine Verpflichtung zur Offenlegung besteht“; der Informationszugang nach dem IFG stellt jedoch gerade eine solche gesetzliche Vorschrift dar. Eine den Informationszugang einschränkende Vertraulichkeitsabrede wäre ohnehin wegen Verstoßes gegen ein gesetzliches Verbot nichtig gewesen.²⁹³

Rund zweieinhalb Monate nachdem wir dies dem Senator mitgeteilt hatten, wies die Senatsverwaltung den Widerspruch der Petenten zurück und blieb – ohne sich mit unseren Argumenten auseinandergesetzt zu haben – bei ihrer unzutreffenden Rechtsauffassung. Wir übersandten den Petenten unsere Stellungnahme an den Senator als Argumentationshilfe für ein gerichtliches Verfahren.

Behörden gehen mit dem Ausschlussgrund des Schutzes von Betriebs- und Geschäftsgeheimnissen noch immer zu großzügig um.

Mühsame Akteneinsicht bei der Senatsverwaltung für Stadtentwicklung und Umwelt

Aus der Praxis

Ein Petent beehrte bei der Senatsverwaltung für Stadtentwicklung und Umwelt die Übersendung von Kopien des Antrags sowie des Genehmigungsbescheids nebst Anlagen in einem wasserrechtlichen Genehmigungsverfahren Dritter. Nachdem wir vermittelnd tätig geworden waren, erhielt der Petent einige der begehrten Unterlagen. Die Herausgabe der übrigen Umweltinformationen, bei denen es sich um zeichnerische Unterlagen, statische Berechnungen, Prüfberichte und Baubeschreibungen handelte, lehnte die Senatsverwaltung jedoch mit der Begründung ab, dass dadurch Urheberrechte verletzt werden könnten.²⁹⁴

Wir baten die Senatsverwaltung um Stellungnahme, inwieweit durch die Herausgabe dieser Unterlagen jeweils konkret Urheberrechte verletzt werden würden, und wiesen darauf hin, dass eine abstrakt geäußerte Vermutung eine Ablehnung nicht rechtfertigen kann. Auf mehrmalige Nachfragen wurde uns zwar

293 § 134 BGB

294 § 18a Abs. 1 IFG i.V.m. § 9 Abs. 1 Satz 1 Nr. 2 UIG

stets eine kurzfristige Erledigung in Aussicht gestellt, die erbetene Stellungnahme erhielten wir jedoch nicht. Erst nach einem Anruf beim Senator und einer weiteren schriftlichen Erinnerung endete die Angelegenheit mit einem zufriedenstellenden Ergebnis: Der Petent erhielt alle beantragten Unterlagen, da die Senatsverwaltung nunmehr zum Ergebnis gekommen war, dass dem Informationszugang doch keine Urheberrechte entgegenstehen. Interessant war die Begründung der Senatsverwaltung vor allem deswegen, weil diese nun ausführte, dass eine urheberrechtliche Schutzfähigkeit der Unterlagen nicht gegeben sei. Einerseits würden sich die Pläne nicht durch Originalität und Form von dem Üblichen abheben, andererseits handele es sich bei den Berichten nicht um schöpferische Leistungen, da die Ingenieure keinen Freiraum bei der Darstellung hätten.

Zwar kam der Petent letztlich zu seinem Recht, zwischen der Antragstellung und der vollständigen Übersendung der Unterlagen lag jedoch ein Dreivierteljahr. Zwischen unserer Bitte um Stellungnahme zu den Urheberrechten und der Erkenntnis der Senatsverwaltung, dass Urheberrechte nicht verletzt sein können, lagen sieben Monate. Derart lange Verfahrensdauern sind unter keinen Umständen hinnehmbar.²⁹⁵

Eine Behörde darf der Herausgabe von Kopien nicht pauschal Urheberrechte entgegenhalten. Vielmehr hat sie im Einzelfall zu prüfen, ob tatsächlich Urheberrechte entgegenstehen.

Einsicht in eine Vereinbarung zum baurechtlichen Sozialplanverfahren

Zwei Petenten begehrten bei der Senatsverwaltung für Stadtentwicklung und Umwelt Einsicht in eine Vereinbarung zum Sozialplanverfahren²⁹⁶ für ein Grundstück in Mitte. Zwar wurde den Petenten die Vereinbarung übersandt, jedoch war ein Paragraf samt Überschrift komplett geschwärzt. Das begründete die Senatsverwaltung mit privaten und unternehmensinternen Informationen und Abstimmungen.

²⁹⁵ Eine sog. Untätigkeitsklage kann gegen eine Behörde bereits nach drei Monaten erhoben werden, siehe § 75 VwGO.

²⁹⁶ §§ 180, 181 BauGB

Selbst bei geheimhaltungsbedürftigen Angaben hätte keinesfalls der komplette Paragraf mit Überschrift geschwärzt werden dürfen, sondern nur die schutzwürdigen Angaben selbst.²⁹⁷ Jedenfalls hätten die Petenten einen Auskunftsanspruch in Bezug auf den Regelungsgehalt der geschwärzten Passagen gehabt. Eine Durchsicht der Vereinbarung, die uns die Senatsverwaltung zur Prüfung übersandt hatte, ergab, dass der Akteneinsicht keine Ausschlussgründe entgegenstanden und insbesondere keine Betriebs- oder Geschäftsgeheimnisse²⁹⁸ enthalten waren. Nach Mitteilung dieses Ergebnisses übersandte die Senatsverwaltung den Petenten das ungeschwärzte Dokument.

Kurz darauf wandte sich die Senatsverwaltung mit der Bitte um Unterstützung an uns, da der Rechtsanwalt des Vertragspartners gerügt habe, dass seine Mandantin vor der Herausgabe nicht angehört worden sei²⁹⁹ und darüber hinaus die Petenten das Dokument im Internet veröffentlicht hätten. Die Vertragspartei musste jedoch nicht angehört werden, da durch die Akteneinsicht weder personenbezogene Daten noch Betriebs- oder Geschäftsgeheimnisse betroffen waren.³⁰⁰ Auch durften die Petenten das ungeschwärzte Dokument im Internet veröffentlichen, da es keine entsprechende Verwendungsbeschränkung der erlangten Informationen gibt.

Die Behörde muss im Einzelfall prüfen, ob es sich bei bestimmten Informationen um schutzwürdige Betriebs- oder Geschäftsgeheimnisse handelt. Eine Anhörung der Betroffenen ist nur dann erforderlich, wenn sich die Behörde trotz des Vorliegens von Betriebs- oder Geschäftsgeheimnissen für die Herausgabe entscheiden würde, weil entweder der Offenbarung keine schutzwürdigen Belange der Betroffenen entgegenstehen oder das Informationsinteresse das Interesse der Betroffenen an der Geheimhaltung überwiegt.³⁰¹

297 § 12 IFG

298 § 7 IFG

299 § 14 Abs. 2 IFG

300 § 14 Abs. 2 Satz 1 IFG

301 § 14 Abs. 2 Satz 1 IFG

Trinkwasseruntersuchungen in Mitte

Eine Petentin wandte sich mit der Bitte um Unterstützung ihres Informationszugangsbegehrens an uns und teilte Folgendes mit: Sie sei schwer erkrankt und habe beim Gesundheitsamt Mitte um Auskunft gebeten, womit das Wasser in einem bestimmten Gebäudekomplex belastet war. Da hierauf keine Reaktion erfolgte, habe sie sich telefonisch an das Gesundheitsamt gewandt. Im Telefonat habe sie auf die Frage, wofür sie die Information benötigt, mitgeteilt, dass sie sich in ärztlicher Behandlung befindet. Ihr sei erklärt worden, dass der Offenbarung der Prüfergebnisse datenschutzrechtliche Belange entgegenstünden und die Ergebnisse nur an die behandelnde Ärztin weitergegeben werden dürften. Deshalb habe die Petentin ihre Ärztin benannt, der dann telefonisch eine Belastung des Wassers mit Legionellen mitgeteilt worden ist. Die Petentin habe daraufhin beim Gesundheitsamt die Übersendung der Messergebnisse zu den Trinkwasseruntersuchungen beantragt. Nach nochmaliger Erinnerung wurden ihr zwar Unterlagen übersandt, ausweislich dieser Prüfberichte waren jedoch keine Legionellen festgestellt worden. Auf weitere Schreiben in dieser Sache erhielt sie vom Gesundheitsamt keine Antwort mehr.

Da der Fall in mehrfacher Hinsicht brisant war, baten wir den Bezirksbürgermeister, zugleich Leiter der zuständigen Abteilung Gesundheit, Personal und Finanzen, um Stellungnahme, aus welchen Gründen der Petentin der beantragte Informationszugang nicht gewährt wird, welche datenschutzrechtlichen Belange gegen eine Mitteilung an die Petentin sprechen sowie auf welcher Rechtsgrundlage das Gesundheitsamt sie nach ihrer behandelnden Ärztin befragt und sodann Kontakt mit dieser aufgenommen hat.

Das Gesundheitsamt erwiderte, man habe prüfen wollen, auf welcher Grundlage bzw. mit welcher Motivation die Petentin die Informationen begehre. Die Petentin habe sich damit einverstanden erklärt, dass das Gesundheitsamt bei ihrer behandelnden Ärztin Informationen einhole. Eine Nachfrage durch das Gesundheitsamt beim Vermieter des Gebäudekomplexes habe ergeben, dass die Petentin dort nicht gewohnt habe, daher seien in den Befunden wohnungsspezifische Angaben geschwärzt worden. Auch sei lediglich vereinbart worden, dass die Petentin Nachbeprobungsbefunde erhalten solle.

Die Petentin hatte jedoch nicht nur die Übersendung der Nachbeprobungsbefunde beantragt, sondern die Übersendung aller Prüfberichte. Sie musste auch kein Informationsinteresse darlegen, da der Anspruch auf Informationszugang voraussetzungslos ist und auch nicht begründet werden muss. Das Gesundheitsamt sagte uns zu, der Petentin nunmehr Kopien der übrigen Befunde zu übersenden. Da wir jedoch Anhaltspunkte dafür hatten, dass auch diese Kopien unvollständig waren, haben wir vor Ort die Prüfberichte eingesehen. Erst drei Monate nach Antragstellung erhielt die schwer erkrankte Petentin daraufhin schließlich die begehrten Prüfberichte, auf deren Grundlage die ärztliche Behandlung fortgesetzt werden konnte.

Der Fall war aber nicht nur im Hinblick auf den Informationszugang zu den Prüfberichten bedeutsam. Datenschutzrechtlich war sowohl die Erhebung der Daten der Ärztin als auch die Kontaktaufnahme mit dem Vermieter unzulässig. Das Gesundheitsamt hat der Petentin die Information über die derzeitige ärztliche Behandlung regelrecht abgerungen. Der Petentin wurde darüber hinaus fälschlicherweise mitgeteilt, dass die Angaben zu den Untersuchungsergebnissen aus datenschutzrechtlichen Gründen nicht an sie selbst, sondern nur an ihre Ärztin hätten übermittelt werden dürfen. Da der Antrag auf Informationszugang voraussetzungslos ist und insbesondere nicht von berechtigten oder rechtlichen Interessen der Antragstellerin abhängt, war auch die Kontaktaufnahme zum Vermieter, um zu erfahren, ob sich die Petentin im Objekt aufgehalten hatte, datenschutzrechtlich unzulässig. Um solche Datenschutzverstöße zu vermeiden, wird das Gesundheitsamt künftig Auskunftsanträge zunächst rechtlich unter Einbeziehung datenschutzrechtlicher Regelungen prüfen. Es versprach auch, die Beschäftigten nochmals auf die datenschutzrechtlichen Regelungen hinzuweisen.

Der Anspruch auf Informationszugang nach dem IFG ist voraussetzungslos und muss nicht begründet werden. Die aktenführende Stelle ist nicht befugt, bei der antragstellenden Person die Motive zu erfragen oder Dritte zur Klärung der Motive zu kontaktieren.

Fehlerhafte Rechtsfortbildung im Rechtsamt Reinickendorf

Ein Petent beschwerte sich bei uns darüber, dass das Bezirksamt Reinickendorf seinen Antrag auf Einsicht in einen Prüfbericht der Prüfgruppe zur Korruptionsbekämpfung mit der Begründung abgelehnt habe, dass deren Prüfungsvorgänge bislang nicht für Einsichtnahmen zur Verfügung gestellt worden seien – weder für interne Zwecke und insbesondere nicht für Außenstehende – und dieser Standpunkt auch weiterhin aufrecht erhalten würde. Auf unsere Bitte um Stellungnahme, aus welchen rechtlichen Gründen die Akteneinsicht verweigert wird, teilte uns das bezirkliche Rechtsamt mit, dass Prüfverfahren vertraulich durchgeführt werden und die Mitarbeiter der Prüfgruppe zu strenger Verschwiegenheit verpflichtet seien. Diese Verschwiegenheitsverpflichtung sei auch in den gerade neu gefassten „Richtlinien für die Arbeit der Prüfgruppen zur Korruptionsbekämpfung in der Hauptverwaltung“ festgeschrieben. Auch müsse es immer Bereiche geben, die einer Einsichtnahme wegen der besonderen Materie der Akten von vornherein entzogen seien.

Diese rechtsirrigte Argumentation erstaunte auch im weiteren Verlauf schon deshalb, weil sie vom bezirklichen Rechtsamt stammte. Der Informationszugang ist in dem beantragten Umfang zu gewähren, wenn keine der im Gesetz geregelten Ausnahmen Anwendung findet.³⁰² Dafür, dass der gesamte Bereich der Korruptionsbekämpfung im Bezirksamt ausgenommen, d. h. auch kein teilweiser Informationszugang möglich sein soll, gibt es im IFG keine Anhaltspunkte. Zudem konnten die genannten Richtlinien als Verwaltungsvorschriften das gesetzliche Recht auf Akteneinsicht nicht einschränken (diese trafen ohnehin keine Regelungen in Bezug auf Akteneinsichten). Die Verpflichtung der Mitarbeiter zu strenger Verschwiegenheit kann dem Recht auf Akteneinsicht nicht entgegenstehen, da mit der Entscheidung, Informationszugang zu gewähren, zugleich eine Aussagegenehmigung zu erteilen ist.³⁰³ Wir baten das Rechtsamt daher, unter Beachtung dieser Rechtslage erneut über den Antrag des Petenten zu entscheiden.

302 § 4 Abs. 1 IFG

303 § 5 Satz 1 IFG i.V.m. § 37 Abs. 3 BeamStG

Das Rechtsamt entsprach dem nicht: Es wolle zunächst den Ausgang eines vergleichbaren Rechtsstreits eines anderen Bezirksamts vor dem Verwaltungsgericht Berlin abwarten. Wir erklärten dem Rechtsamt, dass das Ergebnis eines Rechtsstreits in anderer Sache keine Wirkung für dieses Verfahren entfalten kann, und baten darum, zur Klärung der Angelegenheit kurzfristig selbst Einsicht in den streitbefangenen Prüfbericht nehmen zu können. Als trotz unseres Hinweises auf die Unterstützungspflicht³⁰⁴ nach zwei Wochen keine Reaktion erfolgt war, erklärte das Rechtsamt auf telefonische Nachfrage, dass zunächst die Neukonstituierung der Prüfgruppe abgewartet werden müsse und vorher über unser Anliegen nicht entschieden werden könne. Auch wurden Zweifel geäußert, ob wir den Prüfbericht überhaupt einsehen dürften. Erst nach Einschaltung des Bezirksbürgermeisters wurde uns die begehrte Einsichtnahme ermöglicht.

Die Durchsicht des gesamten Prüfungsvorgangs ergab keine Anhaltspunkte auf schutzwürdige Angaben oder sonst geheimhaltungsbedürftige Aktenteile. Auf unseren erneuten Hinweis, dass keiner der im IFG genannten Ausnahmetatbestände erfüllt sei, erklärte das Rechtsamt nun, dass man dies ebenfalls so sehe. Man gehe jedoch weiterhin davon aus, dass alle Prüfungsvorgänge und Verfahrensakten zur Korruptionsbekämpfung dem Anwendungsbereich des IFG von vornherein entzogen seien. Dem Petenten stellten wir den Schriftwechsel mit dem Rechtsamt als Argumentationshilfe für eine mögliche Klage beim Verwaltungsgericht zur Verfügung.

Das IFG enthält keine Ausnahmen für ganze Verwaltungsbereiche oder -aufgaben. Auch die Annahme, dass die Korruptionsbekämpfung als solche vom Informationszugang nach dem IFG ausgenommen ist, findet im Gesetz keine Stütze.

304 § 28 Abs. 1 BlnDSG

Aktenpläne im Bezirksamt Treptow-Köpenick – und deren Zweck

Ein Petent wollte bei der Zentralen Revision zur Korruptionsbekämpfung (ZRK) beim Bezirksamt Treptow-Köpenick die allgemein zugänglichen Register, Aktenpläne, Aktenordnungen, Aktenverzeichnisse, Einsenderverzeichnisse und Tagebücher einsehen.³⁰⁵ Das Bezirksamt lehnte das ab mit der Begründung, dass das Aktenverzeichnis der ZRK bereits von ihrer Aufgabenstellung her nicht diesen Verzeichnissen zuzuordnen sei. Weiter führte das Bezirksamt – ohne Begründung – aus, dass der Akteneinsicht der Schutz personenbezogener Daten³⁰⁶ sowie der Schutz besonderer öffentlicher Belange, der Rechtsdurchsetzung und der Strafverfolgung³⁰⁷ entgegenstünden.

Wir baten das Bezirksamt um Stellungnahme, weshalb erstens bei der ZRK kein Verzeichnis geführt wird, das geeignet ist, die Aktenordnung und den Aktenbestand sowie den Zweck der geführten Akten erkennen zu lassen,³⁰⁸ zweitens die Register, Aktenpläne, Aktenordnungen, Aktenverzeichnisse, Einsenderverzeichnisse, Tagebücher sowie die vorgenannten Verzeichnisse entgegen der gesetzlichen Vorgabe nicht allgemein zugänglich gemacht werden³⁰⁹ sowie drittens einer Einsichtnahme in das Aktenverzeichnis die genannten Ausnahmetatbestände konkret entgegenstehen sollen. Daneben baten wir zur weiteren Aufklärung des Sachverhalts um eine Kopie des derzeit bei der ZRK geführten Aktenverzeichnisses.

Kurz darauf wandte sich die behördliche Informationsfreiheitsbeauftragte des Bezirksamts mit einem Beratungersuchen an uns, da sie den Auftrag erhalten habe, allen Organisationseinheiten im Bezirksamt beratende Unterstützung für die Führung von gesetzeskonformen Aktenplänen anzubieten. Diesem Wunsch kamen wir gerne nach und erläuterten die Anforderungen unter Hinweis auf unseren eigenen Aktenplan.³¹⁰

305 § 17 Abs. 5 Satz 2 IFG

306 § 6 IFG

307 § 9 IFG

308 § 17 Abs. 5 Satz 1 IFG

309 § 17 Abs. 5 Satz 2 IFG

310 Abrufbar unter www.datenschutz-berlin.de/content/berlin/berliner-beauftragter/aktenordnung

Das Bezirksamt teilte uns später mit, dass der bisherige auf Personendaten basierende Aktenplan nun auf ein den Anforderungen des IFG genügendes numerisches System umgestellt worden sei. Wir haben festgestellt, dass er nun den gesetzlichen Anforderungen genügt.

Auch 13 Jahre nach Inkrafttreten des IFG verfügen nur wenige öffentliche Stellen über allgemein zugängliche Aktenpläne. Die Nichterfüllung dieser Pflicht ist ein klarer Gesetzesverstoß.

Allgemein zugängliche Aktenpläne sind die Grundvoraussetzung für eine spätere detaillierte Informationsanfrage, wie der Fall im weiteren für den Petenten unglücklichen Verlauf zeigte.

Der Petent beehrte bei der ZRK nun Einsicht in insgesamt 22 Aktenordner, die im Aktenplan mit „Gesetze, Verordnungen und Rechtsvorschriften“, „Korruptionsprävention und -bekämpfung“ sowie „Gefährdungsatlas“ bezeichnet waren. Das Bezirksamt gewährte die Akteneinsicht hinsichtlich einiger Aktenordner vollumfänglich, bei den übrigen Ordnern trennte es teilweise Unterlagen komplett ab, teilweise schwärzte es einzelne Angaben. Das Bezirksamt erteilte zudem einen Gebührenbescheid i. H. v. 500 € – der Höchstgebühr³¹¹ –, wobei sich dem Bescheid nicht entnehmen ließ, wie sich die Gebühr zusammensetzte.

Eine Prüfung des umfangreichen Bescheids ergab, dass die Akteneinsicht bei 18 der vorgenommenen 19 Einschränkungen nicht bzw. nicht vollständig hätte abgelehnt werden dürfen. So rügte das Bezirksamt mehrfach, dass der Petent sein Informationsinteresse nicht dargelegt habe und daher sein Informationsinteresse das Interesse der Betroffenen an der Geheimhaltung nicht überwiege.³¹² Die antragstellende Person muss ihr Informationsinteresse aber nicht darlegen. Ferner trennte das Bezirksamt unter Verweis auf den Schutz des behördlichen Entscheidungsprozesses³¹³ mehrfach komplette Unterlagen ab, ohne zu begründen, weshalb hier keine beschränkte Akteneinsicht gewährt werden konnte.³¹⁴

311 Siehe Tarifstelle 1004 b) Nr. 3 des Gebührenverzeichnisses zur Verwaltungsgebührenordnung

312 § 6 Abs. 1 IFG

313 § 10 IFG

314 § 15 Abs. 3 IFG i. V. m. § 12 IFG

Zudem hätte der Petent hinsichtlich der Hälfte der 22 Aktenordner nach den Beschreibungen im Aktenplan nicht damit rechnen müssen, dass sich dort überhaupt potentiell geheimhaltungsbedürftige Unterlagen befanden. Laut Aktenplan sollten sich etwa in dem mit „Gesetze, Verordnungen und Rechtsvorschriften“ beschriebenen Aktenordner nur „Amtsblatt für Berlin, Gesetz- und Verordnungsblatt für Berlin, Aufsätze, Urteile und Kommentare“ befinden. Tatsächlich war dort auch eine „Kassensicherheitsbestimmung“ vorhanden, deren Herausgabe mit der Begründung abgelehnt wurde, dass das Bekanntwerden die Sicherheit der in diesem Bereich Beschäftigten gefährden und zu schwerwiegenden Nachteilen für das Land Berlin führen könne.³¹⁵ Insbesondere dann, wenn anhand des Aktenplans ein schutzbedürftiger Inhalt nicht erwartet werden muss, ist jedoch ein vorheriger Hinweis an die antragstellende Person über die u. U. gebührenpflichtige Abtrennung dieses Inhalts erforderlich.

Nach unserer Intervention hat das Bezirksamt dem zwischenzeitlich erhobenen Widerspruch des Petenten teilweise abgeholfen. Im Gebührenbescheid schlüsselte es zwar den Verwaltungsaufwand nunmehr nachvollziehbar pro Aktenordner auf, ging jedoch nicht auf unsere Argumente ein und rückte auch nicht von der Höchstgebühr ab. Dem Petenten blieb daher nur die Klageerhebung. Hierzu stellten wir ihm unsere Stellungnahme an das Bezirksamt als Argumentationshilfe zur Verfügung.

Die Gebühren für Informationszugang nach dem IFG dürfen keinesfalls abschreckend wirken. Zumindest wenn eine öffentliche Stelle beabsichtigt, eine außergewöhnlich hohe Gebühr oder die Höchstgebühr zu erheben, sollte sie hierauf vorab hinweisen.

Vier weitere Einzelfälle mit positivem Ausgang werden im Kapitel 19 dargestellt.

315 § 11 IFG

19 Was die Menschen sonst noch von unserer Tätigkeit haben ...

Ein Bürger informierte uns darüber, dass er von einem Krankenhaus irrtümlich einen **Entlassungsbericht** mit Gesundheitsdaten eines anderen Patienten **per Fax erhalten** habe. Die Klinik teilte uns mit, dass ärztliche Mitteilungen nur bei Dringlichkeit oder auf Patientenwunsch veranlasst würden. Hier sei die Übermittlung per Fax auf Wunsch des Patienten erfolgt, und er habe die Faxnummer hierfür telefonisch mitgeteilt. Es konnte jedoch nicht mehr nachvollzogen werden, ob die Faxnummer falsch angegeben, falsch notiert oder falsch ins Sendegerät eingegeben wurde. Die Klinik hat versichert, dass bereits ein Merkblatt zum Datenschutz bei Einsatz und Nutzung von Faxgeräten genutzt wird. Künftig wird zur Versendung personenbezogener Daten per Fax die schriftliche Zustimmung der Patientin oder des Patienten (oder der Betreuungsperson) eingeholt, und personenbezogene Mitteilungen werden per Fax nur noch über einen besonders geschützten Faxbereich mit Dokumentation des Sendevorgangs verschickt. Der Datenschutzbeauftragte des Krankenhauses hat das medizinische Personal der Abteilung erneut über die Datenschutzvorgaben belehrt.

Um eine lückenlose Anschlussmedikation zu gewährleisten, bat ein Hausarzt das Krankenhaus des Maßregelvollzugs um Übersendung eines medizinischen **Entlassungsberichts** in Bezug auf seinen Patienten. Das Krankenhaus schickte neben dem Bericht einen **vollständigen Verlauf des Strafvollzugs** des Betroffenen. Diese Informationen waren für die Weiterbehandlung durch den Hausarzt nicht erforderlich, die Übermittlung war also rechtswidrig. Das Krankenhaus räumte den Datenschutzverstoß ein und bat den Hausarzt um unverzügliche Löschung der Daten bzw. Vernichtung der Unterlagen. In einer Mitarbeiterkonferenz hat das Krankenhaus die Beschäftigten erneut für den bewussten Umgang mit Patientendaten sensibilisiert.

Wir haben erreicht, dass ein von der Senatsverwaltung für Gesundheit und Soziales entwickelter Vordruck für die **Beantragung von Grundsicherung im Alter und bei Erwerbsminderung** überarbeitet wurde. Bisher wurden die Bedürftigen aufgefordert, **Kontoauszüge** einzureichen, obwohl das Gesetz nur

die Vorlage sog. Beweisurkunden fordert.³¹⁶ Deshalb sind Kontoauszüge weder im Original noch in Kopie einzureichen. Unsere Anregung, den in Rede stehenden Passus umzuformulieren und lediglich die Vorlage der Kontoauszüge der letzten drei Monate zu verlangen, wurde aufgegriffen. Darüber hinaus wird auf die Möglichkeit hingewiesen, dass bei Abbuchungen geringer Beträge (in der Regel bis zu 50 Euro) die zu den Einzelbuchungen aufgeführten Texte (nicht die Beträge) geschwärzt werden können.

Ein Gast eines Hotels bat um **Prüfung** des dort gebräuchlichen **Hotelmeldescheins**. Er enthielt u. a. Datenfelder zu der E-Mail-Adresse, der Telefonnummer, der Ausweisnummer und dem Geburtstag des Gastes. Nach § 21 a Berliner Meldegesetz müssen Meldescheine außer dem Namen und der Anschrift der Beherbergungsstätte Angaben über den Tag der Ankunft und den der voraussichtlichen Abreise, den Familiennamen, den gebräuchlichen Vornamen (Rufnamen), die Anschrift und die Staatsangehörigkeit des Gastes enthalten. Weitere Daten wie Geburtstag, E-Mail-Adresse, Telefonnummer und Personalausweis-/Passnummer sind dagegen mit dem Hinweis auf Freiwilligkeit zu kennzeichnen. Andernfalls ist ihre Erhebung unzulässig. Insbesondere sollte der Meldeschein eine optisch eindeutige und transparente Abgrenzung zwischen den vom Gesetz geforderten Angaben (Pflichtfelder) und denjenigen Daten aufweisen, die auf freiwilliger Basis erhoben werden. Das Hotel sagte zu, dies umzusetzen.

Ein Bürger bestellte ein **Zeitschriften-Abonnement**. Auf dem Bestellformular kreuzte er „Zahlung per Rechnung“ an und füllte die Felder nicht aus, die für die **Bankverbindungsdaten** vorgesehen waren. Trotzdem buchte das Unternehmen den Rechnungsbetrag vom Konto des Betroffenen ab. Das Unternehmen griff dabei auf Bankverbindungsdaten zurück, die ihm bereits aus einem Jahre zurückliegenden gekündigten Abonnement des Betroffenen bekannt waren. Diese Daten hatte das Unternehmen noch nicht gelöscht, weil es verpflichtet war, diese Daten aufgrund handels- und steuerrechtlicher Vorschriften weiter aufzubewahren. Allerdings hätten die Daten gesperrt werden müssen. Die Nutzung dieser Daten zum Einzug von Forderungen aus dem neuen Abonnement war nicht zulässig. Wir haben festgestellt, dass in dem Unternehmen keine Vorgaben für die Sperrung von Daten bestanden, sodass Daten aus Alt-Verträgen ungehindert rechtswidrig im operativen Geschäft verwendet

316 Siehe § 60 Abs. 1 Satz 1 Nr. 3 SGB I

werden konnten. Aufgrund unserer Intervention hat das Unternehmen nunmehr ein **Sperrkonzept** entwickelt und umgesetzt.

Ein Bürger beehrte bei der **Ärztammer Berlin** Auskunft über **berufsrechtliche und berufsgerichtliche Verfahrensregeln** und machte schon bei Antragstellung deutlich, dass es ihm nicht um Einzelfälle geht. Die Ärztekammer teilte ihm mit, dass nach dem Berliner Informationsfreiheitsgesetz (IFG) kein allgemeiner Auskunftsanspruch bestehe, sondern sich dieser nur bezogen auf bestimmte Verfahrensakten ergeben könne. Eine Einsicht in diese Akten sei jedoch nur mit Zustimmung des betroffenen Arztes möglich. Auch werde pro Akte eine Gebühr zwischen 5 und 500 € erhoben.³¹⁷ Wir teilten der Ärztekammer mit, dass grundsätzlich alle Akten dem IFG unterliegen, der Bürger eindeutig keine Auskunft zu konkreten Verfahren beehrte und die Gebühr nicht etwa pro Akte, sondern grundsätzlich pro Antrag erhoben wird. Nach unserer Intervention erhielt der Bürger gebührenfreie Auskünfte.

Eine Bürgerin bat nach dem IFG beim **Bezirksamt Charlottenburg-Wilmersdorf** um Übersendung dreier **Rechtsgutachten zu einem Bebauungsplan**. Ein Gutachten wurde ihr zwar zur Verfügung gestellt, die Herausgabe der beiden übrigen Gutachten jedoch unter Verweis auf den Schutz des behördlichen Entscheidungsprozesses³¹⁸ abgelehnt: Diese dienen der Beratung und Willensbildung innerhalb des Bezirksamts, und der entsprechende Verfahrensschritt sei noch nicht abgeschlossen. Wir wiesen das Bezirksamt darauf hin, dass Akten zur Vorbereitung und Durchführung der Bauleitplanung einsehbar sind, sobald (wie hier) der Beschluss, einen Bauleitplan aufzustellen, gefasst ist.³¹⁹ Aufgrund unserer Intervention erhielt die Bürgerin vom Bezirksamt auch die übrigen Gutachten.

Ein Bürger wollte beim **Bezirksamt Treptow-Köpenick** den **Aktenplan des Büros des Bezirksbürgermeisters** einsehen. Das Bezirksamt teilte ihm mit, dass der Informationszugang nach dem IFG gebührenpflichtig sei und man ihm erst nach Entrichtung einer Verwaltungsgebühr von 50 € den Termin und Ort für die Einsichtnahme mitteilen werde. Wir wiesen das Bezirksamt darauf

317 Siehe Tarifstelle 1004 des Gebührenverzeichnisses zur Verwaltungsgebührenordnung

318 § 10 IFG

319 § 10 Abs. 2 Satz 1 IFG

hin, dass Aktenpläne, Aktenordnungen und ähnliche Verzeichnisse allgemein zugänglich zu machen sind³²⁰ und deshalb die Einsicht in diese Verzeichnisse nicht gebührenpflichtig ist.³²¹ Das Bezirksamt hob daraufhin den Gebührenbescheid auf und ermöglichte dem Bürger die gebührenfreie Einsicht in den Aktenplan.

Ein Bürger beantragte nach dem IFG beim **Bezirksamt Treptow-Köpenick** die Übersendung aller **internen Weisungen, Anordnungen und Richtlinien** zur Wohnaufwendungsverordnung (WAV) 2012. Eine Mitarbeiterin des Bezirksamts habe ihm mitgeteilt, dass interne Weisungen hierzu nicht herausgegeben würden. Uns teilte sie jedoch mit, dass zur WAV 2012 keine Anordnungen, Weisungen o. Ä. existieren. Eine Nachfrage beim Petenten ergab, dass die Rechts- und Widerspruchsstelle des Bezirksamts erklärt habe, dass dort eine entsprechende Weisung der Senatsverwaltung für Gesundheit und Soziales vorhanden sei. Das bestätigte uns die bezirkliche Stelle, die zusagte, dem Bürger die Weisung zu übersenden.

320 § 17 Abs. 5 Satz 2 IFG

321 Allenfalls können für die Anfertigung von Kopien Gebühren nach Tarifstelle 1001 c) des Gebührenverzeichnisses zur Verwaltungsgebührenordnung erhoben werden.

20 Aus der Dienststelle

20.1 Entwicklungen

Der langjährige Stellvertreter des Berliner Beauftragten für Datenschutz und Informationsfreiheit, Diplominformatiker Hanns-Wilhelm Heibey, trat am 30. September in den Ruhestand. Er hat unsere Dienststelle mit aufgebaut und 31 Jahre lang wesentlich mitgestaltet. Insbesondere war er maßgeblich beteiligt an wegweisenden Stellungnahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in deren Arbeitskreis Technik er zuletzt an der Formulierung der Orientierungshilfe Cloud Computing³²² mitgewirkt hat. Sein Verdienst ist es, dass der Stellenwert der Informatik bei der Gestaltung und Durchsetzung des Datenschutzes nicht allein in Berlin, sondern auch in Deutschland und darüber hinaus sehr früh erkannt worden ist.

20.2 Zusammenarbeit mit dem Abgeordnetenhaus, dem Deutschen Bundestag und dem Europäischen Parlament

Im Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit sind der Jahresbericht 2010 und die Stellungnahme des Senats³²³ beraten worden. Der nach der Neuwahl des Parlaments neu gebildete Ausschuss hat nach der Geschäftsordnung keine Möglichkeit, selbst Beschlussempfehlungen zu beschließen. Allerdings können Anträge zu den Jahresberichten des Berliner Beauftragten für Datenschutz und Informationsfreiheit und den Stellungnahmen des Senats im Plenum gestellt werden, was bisher noch nicht erfolgt ist. In dem neuen Ausschuss sind „Datenschutz und Informationsfreiheit“ zwar nicht mehr die einzigen Themen wie im früheren Unterausschuss, sie werden aber bei der Diskussion von Fragen der Netzpolitik oder der Digitalisierung der Verwaltung häufig mit thematisiert, was von der Sache her auch geboten ist.³²⁴

322 JB 2011, 2.1.1

323 Abgh.-Drs. 16/4334

324 Siehe 1

Im Dezember erläuterte der Berliner Beauftragte für Datenschutz und Informationsfreiheit seine Haltung zur Open-Data-Strategie der Bundesregierung im Unterausschuss Neue Medien des Deutschen Bundestages. Thema der jährlichen Interparlamentarischen Tagung der Ausschüsse des Europäischen Parlaments und der nationalen Parlamente war im Oktober der neue europäische Rechtsrahmen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit erhielt dabei Gelegenheit, zu den Vorschlägen der Kommission³²⁵ Stellung zu nehmen.

20.3 Zusammenarbeit mit anderen Stellen

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** tagte am 21./22. März in Potsdam und am 7./8. November in Frankfurt/Oder unter dem Vorsitz der brandenburgischen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht und fasste zahlreiche Entschlüsse zu aktuellen Fragen des Datenschutzes.³²⁶ Für 2013 hat die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen den Vorsitz in der Konferenz übernommen.

Der bisher als selbständiges Koordinationsgremium der **Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich** arbeitende **Düsseldorfer Kreis** unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen wurde in die Konferenz der Datenschutzbeauftragten des Bundes und der Länder integriert, was der Zusammenlegung der Datenschutzkontrolle im öffentlichen und nicht-öffentlichen Bereich in allen Bundesländern außer im Freistaat Bayern Rechnung trägt. Der Düsseldorfer Kreis fasste zwei Beschlüsse zum Datenschutz im Unternehmensbereich.³²⁷

Die **Konferenz der Informationsfreiheitsbeauftragten in Deutschland** tagte am 12. Juni und 27. November unter dem Vorsitz des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz in Mainz und

325 Siehe Einleitung und 14.1

326 Dokumentenband 2012, S. 9 ff.

327 Dokumentenband 2012, S. 25, 61

fasste mehrere Entschlößungen zu aktuellen Fragen des Informationszugangs und der Transparenz.³²⁸ 2013 wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit diese Konferenz leiten.

Die **Arbeitsgruppe nach Art. 29 der Europäischen Datenschutzrichtlinie**, in der Berlin traditionell die Bundesländer im Auftrag der deutschen Datenschutzbehörden vertritt, gewinnt gerade im gegenwärtigen Prozess der Formulierung eines neuen europäischen Rechtsrahmens an Bedeutung. An ihre Stelle soll nach dem Vorschlag der Kommission der in gleicher Weise zusammengesetzte Europäische Datenschutzausschuss treten. Die Art. 29-Gruppe hat zwei umfangreiche Stellungnahmen zum europäischen Datenschutzpaket und darüber hinaus weitere Stellungnahmen u. a. zum Cloud Computing verfasst, die teilweise in unserem Dokumentenband abgedruckt sind.³²⁹

Auf Einladung der Datenschutzbehörde von Uruguay fand die **34. Internationale Konferenz der Datenschutzbeauftragten** am 25./26. Oktober in Punta del Este statt, die sich u. a. ebenfalls zum zentralen Thema des Cloud Computing geäußert hat.³³⁰ Die hierzu gefasste Entschlößung der Konferenz beruht wesentlich auf dem Arbeitspapier der **Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“)**, das bei deren Sitzung in Sopot am 22./23. April als „Sopot-Memorandum“ verabschiedet wurde.³³¹ Die Arbeitsgruppe tagte erneut am 10./11. September in Berlin und beriet über weitere Fragen insbesondere der Internetnutzung, zu denen Arbeitspapiere in Vorbereitung sind.

Außerdem besuchten wieder mehrere ausländische Delegationen die Dienststelle des Berliner Beauftragten für Datenschutz und Informationsfreiheit, um mit uns praktische Fragen der Datenschutzkontrolle und des Informationszugangs zu erörtern. Neben Vertretern der mosambikanischen Zentralbank stattete uns auch die parlamentarische Beauftragte für Menschenrechte der Ukraine einen Besuch ab und informierte sich über unsere Arbeit.

328 Dokumentenband 2012, S. 185 ff.

329 Siehe 14.2 und Dokumentenband 2012, S. 63 ff.

330 Dokumentenband 2012, S. 167 f.

331 Dokumentenband 2012, S. 171 ff.

20.4 Öffentlichkeitsarbeit

Am 27. Januar fand auf Einladung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Thema „Vorratsdatenspeicherung“ eine zentrale Veranstaltung in der Vertretung des Freistaates Bayern beim Bund in Berlin aus Anlass des 6. Europäischen Datenschutztages statt.

Am 27. September haben wir zusammen mit der Europäischen Akademie für Informationsfreiheit und Datenschutz anlässlich des zehnten Jubiläums der Akademie und des elften internationalen Tages der Informationsfreiheit ein Symposium zum Thema „Transparenz und Privatsphäre“ durchgeführt. Dabei referierten u.a. der Vorsitzende des Ausschusses für Digitale Verwaltung, Datenschutz und Informationsfreiheit, Alexander Morlang, und der ehemalige Vizepräsident des Bundesverfassungsgerichts und frühere Hessische Datenschutzbeauftragte, Prof. Dr. Winfried Hassemer.

Außerdem beteiligten wir uns an folgenden öffentlichen Veranstaltungen:

- Gemeinsamer Tag der offenen Tür des Abgeordnetenhauses und des Bundesrates am 12. Mai
- Jugendmesse YOU unter dem Motto „Online, offline: Mach die Welt, wie sie dir gefällt.“ am 8./9. Juni in den Messehallen am Funkturm.

Berlin, den 27. März 2013

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit



Stichwortverzeichnis

A

Abfragegrund 52
 Abiturzeugnis 118
 Adresshandel 132
 Aktenplan 201, 206
 Anliegen-/ Beschwerdedatenbank 18
 Anonymisierung 31, 39
 Antiterrordatei 48
 Apothekenrechenzentren 38
 App 66, 115, 177
 Archivakten 72
 Art. 29-Datenschutzgruppe 144
 Aufbewahrungsfristen 119, 152
 Auftragsdatenverarbeitung 19, 21, 32, 43, 79
 Auskunfteien 30
 Auskunftsanspruch 196, 206

B

Bäder-Betriebe 183
 Bankrecht 127
 Bauakte 106
 Bebauungsplan 206
 Berichtspflicht 26
 Berliner Datenportal 17
 Berliner Mietspiegel 104
 Berliner Schulen 20, 124
 Berlin Group 181
 Beschäftigtendatenschutz 98
 Bestellpflicht 29

Bewegungsdaten 67
 Bibliothek 112
 Bilddaten 120, 125, 138
 Bodenbelastungskataster 105
 Bonitätsprüfung 131
 Bundesmeldegesetz 57
 BVG 156
 BYOD 32

C / D

Cloud Computing 145
 Datenaustausch 122
 Datengeheimnis 46
 Datenlecks 149
 Datenpannen 151, 156
 Datenschutzbeauftragte 29, 44, 184
 Datenschutzverstoß 28, 42, 139
 De-Mail 14
 Dienstvereinbarung 98
 Digitale Verwaltung 13
 digitale Werbeflächen 180
 Dokumentationspflicht 26
 Drittstaatentransfer 146

E

e-Akte 14
 ec-cash-Verfahren 129
 E-Government-Gesetz 13
 eGovernment@School 20
 Einbürgerungsantrag 61

Einsichtsrecht 71, 74, 106, 195, 199
Einwilligung 29, 31, 34, 109, 110, 116,
121, 131, 164, 178
elektronisches Klassenbuch 20
elektronisches Ticketing 66
Elterninterviews 109
Endoprothesenregister 92
Entlassungsbericht 204
E-Postbrief 15
Ethik-Kommission 111
EU-Datenschutz-Grundverordnung
28, 141

F

Facebook 166
Fernmeldegeheimnis 114
Festplatten-Crash 136
Finanzamt 75
Fluggastdaten 143
Forschung 108, 160, 190
fragdenstaat.de 135
Funkzellenabfrage 23, 24

G

Gebührenbescheid 203
Geräte-Identifikationsnummer 177
Gesundheitsamt 89, 96, 197
Gesundheitsdaten 85
Google-Datenschutzerklärung 163
Grundstücksdaten 106

H

Handyparken 67
HandyTicket Deutschland 66
Hinweispflicht 31
Hotelmeldeschein 205

Hygienesiegel 189
Hygieneverordnung 87

I

IHK 132
Informationsfreiheit 187
Informationspflicht 87, 149, 154, 158
IT-Sicherheit 37, 95, 171, 177
IT-Standards 183

J / K

Jugendamt 78, 81
Kennzeichenerfassung 63, 65
Kennzeichnungspflicht 25
Kinderschutz 79, 81
Kinderschutzgesetz 88
Klarnamenprinzip 168
Krankenhaus 95
Krankenhausinformationssysteme 93
Krebsregistrierung 91
Kundendaten 67
Kuvertierung 130

L

LABO 59
Landesarchiv 61
Landeskrankenhausgesetz 91
Liquid Feedback 168
Löschkonzept 45
Löschpflicht 25, 54

M

Melddaten 59
Melderegister 58
Musterformular 155

O

Online-Befragung 108
 Open Data 16
 Ordnungsamt 18
 Orientierungshilfe 93, 103

P

Patientendaten 91, 95, 151, 161
 Personaldaten 34, 99, 101, 156
 Personalvermittlung 153
 Personalvertretung 157
 Plagiatssoftware 113
 POLIKS 55
 Präqualifikationsverfahren 100
 Privatisierungsverträge 193
 Probandendaten 111
 Protokollierung 93, 98
 Prüfungsakten 71
 Pseudonymisierung 31, 40, 78,
 91, 176

R

Rechtsamt 199
 Rechtsextremismus-Datei 49
 RFID-Technik 112

S

Sanktionsstelle 139
 Schadsoftware 36, 95
 Schulcomputer 113
 Schülerdaten 115, 116
 Schulgesetz 117, 121, 123
 Schul-IT 20
 Schulschwänzer-SMS 21
 Schultrojaner 113

Schweigepflichtentbindungs-
 erklärung 90
 Schwerbehindertenakte 85
 Scoring 30
 Selbstschutz 172
 Senatsbeschlüsse 191
 sensitive Daten 97, 99, 110, 153, 158
 sicheres Berliner Schulintranet 20
 Smart Meter 103
 Smartphone 35, 65, 66, 115, 177
 Social Plugins 165, 168
 Sozialamt 83
 Sozialdaten 78, 83
 Staatsanwaltschaft 26
 Steuerakten 74
 Steuerprüfung 75
 Stiftung Datenschutz 161
 Stille SMS 51
 Strafverfolgungsbehörden 23
 Suchmaschine 175

T

Tablet-Computer 95, 115
 Telearbeit 99
 Tourenpläne 152
 Tracking 171
 Transparenz 87, 90
 Transparenzgesetz 188
 Trinkwasseruntersuchungen 197

U

Umweltinformationen 194
 unabhängige Datenschutzkontrolle 27
 unbefugter Abruf 53
 Urheberrecht 101, 113, 194

V

Verbindungsdaten 23
Verbrauchsdaten 103
Verfahrensverzeichnis 43
Verhaltenskodex 147
Verkehrsdatenerhebung 24, 63
Verordnungsdaten 38
Verschlüsselung 38, 64, 97, 155
Versicherungswirtschaft 147
Videoüberwachung 62, 124, 137

W

Wahlvorschlag 133
Werbefilm 120
Werbung 31

Widerspruchsrecht 133
WIMES 78
Wohnungsunternehmen 81

Z

Zeitschriften-Abonnement 205
zentrale Auskunftsstelle 70
zentrale Serverinfrastruktur 19
Zweckbindungsgrundsatz 26

Veröffentlichungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit

Tätigkeitsberichte:

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Senat von Berlin jährlich einen Bericht über seine 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 Falblätter 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.

Digitale Verwaltung • **Funkzellenabfragen** – von der Ausnahme zur Regel? • Zehn Vorschläge zur Verbesserung der **EU-Datenschutz-Grundverordnung** • **BYOD** – „Bring your own device“: Arbeiten mit privaten Endgeräten • Wann dürfen **Apothekenrechenzentren** Verordnungsdaten weitergeben? • Wenn die Aufsichtsbehörde klingelt – vermeidbare Fehler von Unternehmen bei Prüfungen • **Antiterrordatei** auf dem Prüfstand • **Videoüberwachung** im Straßenverkehr • Bezirksamt lädt Vermieter zur Schnüffelei ein • **Tablets** in der Charité • Private Nutzung von Internet und E-Mail • **Schultrojaner** • Wer darf in die Bauakte schauen? • Datenpannen in Wirtschaft und Verwaltung • Selbstschutz gegen Tracking • **Smartphones und Apps** • Hygienesiegel im Gaststättenbereich • Entwurf eines Berliner Transparenz- und Informationsfreiheitsgesetzes