Abgeordnetenhaus BERLIN

Drucksache 17/1103
12.08.2013

17. Wahlperiode

Vorlage – zur Kenntnisnahme –

Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2012

Der Senat von Berlin
SenInnSport – I AbtL 1
Tel. (9223) 2066

An das
Abgeordnetenhaus von Berlin

über Senatskanzlei G Sen

V o r l a g e
- zur Kenntnisnahme -

über Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2012

Der Senat legt nachstehende Vorlage dem Abgeordnetenhaus zur Besprechung vor:

Nach § 29 Abs. 2 Berliner Datenschutzgesetz sowie § 18 Abs. 3 Berliner Informationsfreiheitsgesetz erstattet der Beauftragte für Datenschutz und Informationsfreiheit dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis seiner Tätigkeit. Der Senat hat dazu nach § 29 Abs. 2 des Berliner Datenschutzgesetzes eine Stellungnahme herbeizuführen und legt diese hiermit dem Abgeordnetenhaus vor.

Berlin, den 30. Juli 2013

Der Senat von Berlin

Michael Müller	Sandra Scheeres
---	---
Bürgermeister für den Regierenden Bürgermeister	Senatorin für den Senator für Inneres und Sport

Stellungnahme des Senats

zum Bericht des

Berliner Beauftragten für

Datenschutz und

Informationsfreiheit

für das

Jahr 2012

(nach § 29 Abs.2 Berliner Datenschutzgesetz)

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats

Inhaltsverzeichnis

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats

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 Kom-

mission, 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 Regie-

---

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

rungen betrieben.

Dabei wird zu Unrecht davon ausgegangen, dass der Datenschutz per se innovationshemmend 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

[4] Siehe 15.1

schwächen würde.

Die Entwicklung des Informationsfreiheitsrechts tritt mit dem neuen Hamburgischen Transparenzgesetz in eine neue Phase.[5] Während es immer noch fünf Bundesländer[6] 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.

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- Gouvernment

[5] Siehe 18.1, 18.2

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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
Das Bundesministerium des Innern veröffentlichte im März den Referentenentwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (**{**XE "E-Government-Gesetz"**}E-Govern-ment-Gesetz**). Ziel des Gesetzes ist es, durch den Abbau bundesrechtlicher Hindernisse die elektro-nische 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 Datenschutzgesetz[7] sind die wesentlichen Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit 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 (**„{XE "e-Akte"}e-Ak-te“**) muss genauso gewährleistet sein wie bei einer Papierakte. Die elektronische Aktenführung sollte daher den gegenwärtigen Standard verbessern und nicht hinter diesem zurückbleiben.	Die ordnungsgemäße Aktenführung ist behördenübergreifend die gemeinsame Basis des Verwaltungshandelns und betrifft nahezu jeden Büroarbeitsplatz der Berliner Verwaltung. Der für das Land Berlin konzipierte eAkten-Basisdienst beinhaltet die Kernfunktionalitäten einer GGO-konformen Aktenführung, so dass damit Papierakten abgelöst werden können und landesweit auf eine elektronische Aktenführung umgestellt werden kann. Der eAkten-Basisdienst kann mit vergleichsweise einfachen Mitteln - die ordnungsgemäße Aktenführung wesentlich erleichtern, - die Bearbeitungs-, Durchlauf- und Suchzeiten von Vorgängen und Dokumenten wesentlich reduzieren und - den Raumbedarf für die Aktenhaltung und Archivierung deutlich senken.
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	

[7] § 5 Abs. 2 Nr. 1 – 6 BlnDSG

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
Länder und Kommunen. In seiner Stellungnahme[8] 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 2011[10] 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.	Der Senat strebt weiter an, ein E-Government-Gesetz Berlin noch in diesem Jahr in das Abgeordnetenhaus einzubringen, unabhängig davon, ob das Bundesgesetzgebungsverfahren zum E-Government-Gesetz des Bundes in dieser Legislaturperiode erfolgreich abgeschlossen werden kann oder nicht. Es wäre wünschenswert und vorteilhaft für die Berliner Verwaltung, wenn auch die wesentlichen Änderungen des E-Government-Gesetz des Bundes zum Tragen kämen. Ein im Vergleich zum Referentenentwurf 2011 überarbeiteter Entwurf des Berliner E-Government-Gesetzes befindet sich derzeit in der internen Abstimmung bei der Senatsverwaltung für Inneres und Sport.
Im Rahmen der Kommunikation von Bürgerinnen und Bürgern mit öffentlichen Stellen des Bundes oder der Länder stellt **{**XE "De-Mail"**}De-Mail** eine wichtige Kom-ponente dar, soll sie doch die sichere, vertrauliche und nachweisbare Kommunikation über das Inter-net gewährleisten. Im Berichtszeitraum wurden die ersten De-Mail-Anbieter beim Bundesamt für Sicherheit in der Informationstechnik akkreditiert. Im Gegensatz zum **{**XE "E-Postbrief"**}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 Dienste-Anbieter (DMDA) eine Ende-zu-Ende-Verschlüsselung	

8 BR-Drs. 557/12(B)
9 BT-Drs. 17/11473, S. 93
10 JB 2011, 1.2.1

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 BSI[14] und den Datenschutz-Kriterienkatalog[15] 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 {XE "Open Data"}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,

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

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

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

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.
Kurzfristig soll der Gedanke der offenen Daten in den Berliner Verwaltungsvorschriften verankert und das **{**XE "Berliner Datenportal"**}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

[17] Both/Schieferdecker (Hrsg.), Berliner Open Data-Strategie, Organisatorische, rechtliche und technische Aspekte offener Daten in Berlin – Konzept, Pilotsystem und Handlungsempfehlungen
[18] Siehe Kurzfassung der Studie „Berliner Open Data-Strategie“, S. 6
[19] A. a. O., S. 17

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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, Bildung), 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.	Der Senat ist seinen gesetzlichen Verpflichtungen zur vollständigen Offenlegung der Verträge zur Teilprivatisierung der Berliner Wasserbetriebe voll umfänglich nachgekommen. Die Konsortialverträge samt sämtlicher Anlagen und die sechs Änderungsvereinbarungen sowie das Closing-Protokoll wurden auf der Homepage der Senatsverwaltung für Finanzen, auf der Homepage des Berliner Beauftragten für Datenschutz und Informationsfreiheit und im Amtsblatt für Berlin veröffentlicht. Zum Zwecke der Veröffentlichung wurden die Unterlagen im pdf-Format eingescannt. Die Überführung der pdf-Dokumente in maschinenlesbarer Form wäre nur mit erheblichem Kosten- und Zeitaufwand möglich gewesen.
1.3 Weitere Berliner IT-Projekte Im Rahmen des Projektes **{**XE "Anliegen-/ Beschwerdedatenbank"**}Anliegen-/ Beschwer-**	

[20] A. a. O., S. 20

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
dedatenbank im **{**XE "Ordnungsamt"**}**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 Anliegendatenbank 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 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 **{**XE "zentrale Serverinfrastruktur"**}zentrale Serverinfrastruktur** den Behörden erhebliches Einsparpotential bietet. Der Senat griff die Empfehlung des Rechnungshofes auf und legte eine Strategie für einen einheitlichen Serverbetrieb	Ausgehend von dem Beschluss des Senats aus dem Jahr 2011 zum weiteren Vorgehen hat der Senat am 26. März 2013 Kennzahlen zur Konsolidierung der Server-Infrastrukturen in der Berliner Landesverwaltung beschlossen. Mittels dieser Kennzahlen soll die Effizienz und Servicequalität des dezentralen und zentralen Serverbetriebs ermittelt und bewertet werden. Die Kennzahlen werden ab Mitte 2013 von allen Behörden erfasst und nach einem Jahr in einem

[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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
vor.	landesweiten Vergleich ausgewertet. Die Senatsverwaltung für Inneres und Sport wird dem Senat in der zweiten Jahreshälfte 2014 das Ergebnis der Kennzahlerfassung - verbunden mit einem Vorschlag zu weiteren Schritten zur Konsolidierung des Serverbetriebs der Berliner Verwaltung - vorlegen.
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.	Das Projekt VITBL ist nach Einschätzung des Senats von landesweiter Bedeutung. Es zeigt einen Weg auf, wie Behörden der Berliner Verwaltung ihre IT-Dienstleistungen in einem gleitenden Verfahren in das ITDZ verlagern können und der IT-Betrieb auch vor dem Hintergrund aktueller und zukünftiger Herausforderungen (z. B. demografischer Wandel) in der benötigten Qualität gewährleistet werden kann.
Nach dem BlnDSG[23] 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.	Der Senat unterstützt die notwendige Anpassung vorhandener Sicherheitskonzepte im Rahmen eines entsprechenden Auftrags an das ITDZ.
Auch wird eine umfangreiche vertragliche Regelung der **{**XE "Auftragsdatenverarbeitung"**}**Auftragsdatenverarbeitung nach § 3 Abs. 1 und 2 BlnDSG durch das ITDZ notwendig, die alle verlagerten IT-Verfahren betrifft. Pro-blematisch erscheint hier die gesetzliche Forde-rung,[24] dass die Angaben zu den verarbeiteten Datenarten hinreichend genau sein müssen und vor allem die besonderen Kategorien von personenbe-zogenen Daten[25] 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 Dateibe-	

[23] § 5 Abs. 3 Satz 1 BlnDSG
[24] § 3 Abs. 1 Satz 3 Nr. 2 BlnDSG
[25] § 6 a BlnDSG

schreibungen[26] 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 **{**XE "eGovernment@School"**}eGovernment@School** in allen Berliner Schulen ein. Zweck der Maßnahme ist eine Vereinheit-lichung der bisher heterogenen **{**XE "Schul-IT"**}**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 **{**XE "Berliner Schulen"**}**Berliner Schulen über ein sog. **{**XE "sicheres Berliner Schulintranet"**}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 **{**XE "elektronisches Klassenbuch"**}elektronischen Klas-senbuches** (eKlassenbuch) an einigen Schulen getestet. Dieses Projekt ermöglicht u. a., die **Erziehungsberechtigten unentschuldigt 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 Datenverarbeitung erfolgt durch die Datacenterbox – mit Ausnahme des eKlassenbuchs

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

– 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 **{**XE "Auftragsdatenverarbeitung"**}**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 „**{**XE "Schulschwänzer-SMS"**}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,

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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 personenbezo-gene 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.	Aus pädagogischen Erwägungen und aus Fürsorge für die Erziehungsberechtigten, die durch einen nicht näher bestimmten Grund für den Rückruf verunsichert werden könnten, ist bezüglich des SMS-Textes in Absprache mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit eine Variante festgelegt worden, die eine Information über den Anlaß des Rückrufes zulässt.

2 Schwerpunkte

2.1 Funkzellenabfragen – von der Ausnahme zur Regel?

Die Strafprozessordnung gibt den Strafverfolgungsbehörden die Möglichekit, 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.	Die Staatsanwaltschaft hat im Rahmen der stichprobenartigen Überprüfung von Funkzellenabfragen im Zusammenhang mit Brandanschlägen auf Kraftfahrzeuge festgestellte Defizite durch Nachholung der erforderlichen Benachrichtigungen und Löschungen entsprechend den gesetzlichen Vorschriften beseitigt. Um zukünftig eine höhere Sensibilität der Dezernentinnen und Dezernenten zu erreichen, hat die Staatsanwaltschaft die einschlägige interne Handlungsanweisung (Generalienverfügung) vorläufig ergänzt. In einer Arbeitsgruppe bestehend aus Mitgliedern der Generalstaatsanwaltschaft, der Staatsanwaltschaft, der Amtsanwaltschaft und der Polizei wird ein Konzept zur Speicherung der bei Funkzellenabfragen gewonnenen personenbezogenen Daten und deren Löschung erarbeitet. Sobald dieses Konzept vorliegt, erfolgt eine Einbindung des Berliner Beauftragten für Datenschutz und Informationsfreiheit.
Der Gesetzgeber hat die Maßnahme unter den Vorbehalt der richterlichen Anordnung gestellt. Diese darf erst dann von den Strafverfolgungsbehörden beantragt werden, wenn die Erforschung	Eine Kontrollbefugnis des Berliner Beauftragten für Datenschutz und Informationsfreiheit gegenüber der Staatsanwaltschaft im Zusammenhang mit der richterlichen Anordnung unterliegenden

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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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 **{**XE "Strafverfolgungsbehörden"**}**Strafverfolgungsbehörden weitere Vorgaben beachten: Die erhobenen Ver-kehrsdaten 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.	strafprozessualen Maßnahmen, wie z. B. Funkzellenabfragen, besteht hinsichtlich des Umgangs mit den gewonnenen Daten. Da der Berliner Beauftragten für Datenschutz und Informationsfreiheit abgesehen von Verwaltungsangelegenheiten nach § 24 Abs. 2 Satz 1 des Berliner Datenschutzgesetzes jedoch nicht für gerichtliche Entscheidungen zuständig ist, unterliegt seiner Kontrolle nicht die Anordnung selbst. Alle im Rahmen von strafrechtlichen Ermittlungsverfahren ergehenden richterlichen Maßnahmen gehören zu dem Kernbereich der richterlichen Unabhängigkeit und sind daher der Überprüfung durch andere Staatsgewalten - auch durch die Datenschutzbeauftragten - von vornherein entzogen. Dies gilt wegen des untrennbaren Zusammenhangs auch für die staatsanwaltliche Antragstellung der vom Gericht angeordneten Maßnahme.
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 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]	Das Abgeordnetenhaus hat in seinem Beschluss vom 7. März 2013 (Drs. 17/0796) festgestellt, dass die Funkzellenabfrage als eine Ermittlungsmethode zur Ergreifung von Tätern, z. B. bei gemeingefährlichen Straftaten wie Brandstiftungen, notwendig ist. Zu dem Beschluss wird der Senat einen gesonderten Bericht vorlegen.
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 **{**XE "Verkehrsdatenerhebung"**}**Verkehrsdatenerhebung	

[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

in den Bun-destag ein.[31] Beide Initiativen wurden bislang jedoch nicht verabschiedet.

Anfang 2012 berichteten die Medien über die Durchführung einer {XE "Funkzellenabfrage"}**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 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 Verwal-

31 BT-Drs. 17/7033

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

tung 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 **{**XE "Kennzeichnungspflicht"**}**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 **{**XE "Löschpflicht"**}**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 **{**XE "Zweckbindungsgrundsatz"**}**Zweckbindungsgrundsatz zu konkreti-sieren und enger zu fassen.
- Es ist eine **{**XE "Dokumentationspflicht"**}**Dokumentationspflicht für die Begründung des Einsatzes von Funkzellenabfragen sowie die Durch-führung der Benachrichtigungs- und Löschpflichten einzuführen.

- Der Anwendungsbereich für Funkzellenabfragen ist zumindest auf konkret benannte Straftaten[33] 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 **{**XE "Berichtspflicht"**}**Berichts-pflicht 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 **{**XE "Staatsanwaltschaft"**}**Staatsanwaltschaft rechtsirrig. Das Berliner Datenschutzgesetz[34] 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.
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 **{**XE "unabhängige Datenschutzkontrolle"**}**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,

33 Siehe § 100a Abs. 2 StPO
34 § 24 Abs. 2 BlnDSG
35 Siehe § 162 Abs. 2 StPO

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 Amtsanwaltschaft 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.

2.2 Zehn Vorschläge zur Verbesserung der {XE "EU-Datenschutz-Grundverordnung"}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

[36] Protokoll der Ausschuss-Sitzung vom 22. Oktober 2012

[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

Gesetzgebungsverfahren[38] 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:

38 Hierzu und generell zum neuen europäischen Rechtsrahmen siehe 14.1

39 Siehe Einleitung

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

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 {XE "Datenschutzverstoß"}Datenschutzverstoßes) Vor-Ort-Kontrollen durchführen.[41] Verantwort-liche Stellen würden die Möglichkeit erhalten, durch das Bestreiten eines Anlasses eine Überprü-fung vor Ort zu verhindern. Eine Prüfung wäre dann in der Regel nur im Anschluss an eine richterliche Entscheidung möglich. Etwaige Be-weise für Datenschutzverstöße könnten rechtzeitig vernichtet werden.

Die {XE "Bestellpflicht"}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 {XE "Datenschutzbeauftragte"}betrieblichen und {XE "Datenschutzbeauftragte"}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

[41] Art. 53 Abs. 2b

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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 {XE "Einwilligung"}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 {XE "Auskunfteien"}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 berechtigte Interesse eines Dritten, die gerade im

[42] Art. 7 Abs. 4

Auskunfteibereich Prüfungsmaßstab sind. Der Verordnungsgeber geht offenbar davon aus, dass bei der verantwortlichen Stelle berechtigte 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 {XE "Scoring"}Scoring eingeführt werden.

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

- 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.

{XE "Werbung"}Werbung sollte nur mit {XE "Einwilligung"}Einwilligung der Be-troffenen 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 {XE "Hinweispflicht"}Hinweispflicht vorgesehen sein.

Anders als im Auskunfteibereich 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 {XE "Anonymisierung"}Anonymisierung und {XE "Pseudonymisierung"}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 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 {XE "Auftragsdatenverarbeitung"}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

[43] Art. 6 Abs. 1 f)

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 {XE "BYOD"}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 Geräte – 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 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 Ver-einbarung, 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.

---

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.

46 § 87 Abs. 1 Nr. 1 BetrVG

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 **{**XE "Einwilligung"**}**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 **{**XE "Personaldaten"**}**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 zuordnen 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 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

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

48 § 35 Abs. 2 BDSG

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 **{**XE "Smartphone"**}**Smartphones durch Dritte ist zu untersagen und es ist sicherzustellen, dass wirklich nur Berechtigte auf unternehmens-interne Daten Zugriff nehmen können. Anderen-falls könnte eine unzulässige Übermittlung per-sonenbezogener Daten vorliegen. Bei notwendigen Reparaturen und Wartungsarbeiten muss das Gerät an die IT-Abteilung des Unternehmens übergeben werden. Eine Weitergabe an Dritte sollte ausge-schlossen 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.

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

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 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 **{**XE "Schadsoftware"**}**Schadsoft-ware. Dabei kann z. B. ein Trojaner Tastatur-eingaben 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

---

50 §§ 675, 670 BGB

51 Dies basiert auf § 667 BGB.

52 „**D**enial **o**f **S**ervice“ als Folge einer Überlastung z. B. eines Mailservers durch Überflutung mit Nachrichten

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

{XE "IT-Sicherheit"}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-Authentifizierung[53] 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 VPN[54] realisiert werden. Aktuelle Virenscanner auf den mobilen Geräten sind obligatorisch.

Als weitere Sicherheitsmaßnahme kann eine sinnvolle Protokollierung dienen, die eine Feststellung von Angriffen ermöglicht. Die Installation eines Patchmanagements 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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
Zur Wahrung der Vertraulichkeit und Integrität sollten Daten nur **verschlüsselt** gespeichert werden. Dabei kann entweder der komplette Speicher des Gerätes **{**XE "Verschlüsselung"**}**verschlüsselt werden oder es können verschlüsselte Bereiche (Container) erzeugt wer-den, 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 BSI[55] hat ein Papier zu diesem Thema angekündigt. Es ist anzunehmen, dass auch Maßnahmenempfehlungen im Grundschutzkatalog 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 {XE "Apothekenrechenzentren"}Apothekenrechenzentren {XE "Verordnungsdaten"}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.

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 ausge-

[55] Bundesamt für Sicherheit in der Informationstechnik

stellten 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 **{**XE "Anonymisierung"**}Anonymi-sierung** 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 Rezeptabrech-

nungsstelle 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 **{**XE "Pseudonymisierung"**}**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 Verordnungsdaten verknüpfen alle Rezepte, die den gleichen Versichertencode enthalten. Es ist für sie interessant nachzuvollziehen, wie sich das Verordnungsverhalten 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 Verordnungsdaten wietestgehend 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 **{**XE "Datenschutzverstoß"**}**Datenschutz-verstöße 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 Verar-beitung 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. **{**XE "Verfahrensverzeichnis"**}**Ver-fahrensverzeichnis zu führen.[58] Dieses Verzeichnis enthält Angaben zur Organisation der ver-antwortlichen Stelle (Namen, Adresse, Leitungs-personen), 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 Drittstatten) 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]

---

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.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Formulare/Formulare.php.

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats

Fehlende oder mangelhafte Verträge über die {XE "Auftragsdatenverarbeitung"}Auftragsdatenverarbeitung

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

---

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

Fehlende Unabhängigkeit oder Fachkunde der oder des {XE "Datenschutzbeauftragte"}Datenschutzbeauftragten

Die oder der {XE "Datenschutzbeauftragte"}Datenschutzbeauftragte eines Unter-nehmens ist eine wichtige Kontrollinstanz innerhalb der verantwortlichen Stelle. Sie oder er wirkt auf die Einhaltung der Datenschutz-regelungen 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 be-stehen dürfen. Die Bestellung 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]

65 § 4f Abs. 2 Satz 1 BDSG

66 § 38 Abs. 5 Satz 3 BDSG

67 Siehe Dokumentenband 2010, S. 25 ff.

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats

Fehlendes {XE "Löschkonzept"}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 empfindlichen 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. Berichtung, Löschung, Werbewiderspruch, 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.

68 § 35 Abs. 2 Satz 2 Nr. 3 BDSG
69 § 35 Abs. 3 Nr. 1 BDSG
70 § 43 Abs. 2 Nr. 1 BDSG
71 § 34 Abs. 1 Satz 1 BDSG
72 § 43 Abs. 1 Nr. 8a BDSG

Fehlende oder mangelhafte Verpflichtung auf das {XE "Datengeheimnis"}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 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.

3 Öffentliche Sicherheit

3.1 {XE "Antiterrordatei"}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.

[73] § 5 Satz 2 BDSG

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

[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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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 Daten[77] wie die Telefonnummer, die mithilfe eines IMSI-Catchers ermittelt worden war,[78] waren bei der Polizei in der ATD zudem nicht gekennzeichnet.	Das Bundesverfassungsgericht hat in seinem Urteil vom 24. April 2013 (1 BvR 1215/07) die Antiterrordatei (ATD) in ihren Grundstrukturen für verfassungsgemäß gehalten und ihre Bedeutung für die Abwehr des internationalen Terrorismus ausdrücklich hervorgehoben. Einzelfragen der Ausgestaltung muss der Bundesgesetzgeber bis zum 31. Dezember 2014 nachbessern. Der Gesetzgeber ist unter anderem aufgefordert, innerhalb der vom Bundesverfassungsgericht gesetzten Übergangsfrist regelmäßige Kontrollen mindestens alle zwei Jahre durch die Datenschutzbeauftragten des Bundes und der Länder als den gesetzlich vorgesehenen Aufsichtsinstanzen sicherzustellen. Darüber hinaus werden künftig, neben der laufenden fachlichen Kontrolle durch die Vorgesetzten, auch verstärkt anlasslose Stichprobenkontrollen durch die behördlichen Datenschutzbeauftragten der Polizei und der Verfassungsschutzbehörde erfolgen. Die Aussage zur Datensperrung war zum Zeitpunkt der Prüfung zutreffend. Die technische Möglichkeit zur gesetzlichen Vorgabe einer Datensperrung wurde allerdings erst im Mai 2012 durch das BKA umgesetzt und auch erst im Nachgang zur Prüfung des Berliner Beauftragten für Datenschutz und Informationsfreiheit auf entsprechende Nachfrage beim BKA bei der Polizei bekannt. Dem Kritikpunkt wurde zwischenzeitlich abgeholfen: Die beteiligten Behörden sind nunmehr berechtigt, Datensätze in der ATD zu sperren. Die Notwendigkeit, einen Datensatz nicht zu löschen, sondern nur zu sperren, ist allerdings in den sieben Jahren seit Inbetriebnahme der ATD noch nicht aufgetreten. Was die Möglichkeit der Auswertung der Protokolldaten betrifft, so ist der Kritik des Berliner Beauftragten für Datenschutz und Informationsfreiheit entgegenzuhalten, dass das BKA zur

76 JB 2007, 3.2.2
77 § 3 Abs. 2 ATDG
78 § 100 i StPO

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
	Erfüllung seiner Aufgaben aus § 9 ATDG seit Einführung der ATD Räumlichkeiten und ggf. unterstützendes Personal für die Kontrollen durch die Datenschutzbeauftragten des Bundes und der Länder vorhält. Darüber wurden die Datenschutzbeauftragen nach Auskunft des BKA auch informiert. Bisher wurde diese Möglichkeit jedoch nicht genutzt. Im Nachgang zur Prüfung bei der Verfassungsschutzbehörde wurde der Berliner Beauftragte für Datenschutz und Informationsfreiheit hinsichtlich zweier unterschiedlicher Wege zur Bereitstellung von Protokolldaten informiert, die auch für die Polizei Berlin gelten. Verwaltungsvorschriften zur einheitlichen Auslegung unbestimmter Rechtsbegriffe im ATDG würden im Hinblick darauf, dass insgesamt 38 Behörden des Bundes und der Länder an der ATD beteiligt sind, nur Sinn machen, wenn sie bundesweit einheitlich gelten würden. Nach dem oben bereits zitierten Urteil des Bundesverfassungsgerichts müssen die Sicherheitsbehörden künftig jedenfalls die von ihnen vorgenommenen Konkretisierungen für bestimmte, sehr offen formulierte Daten (z.B. zur Erfassung terrorismusrelevanter Fähigkeiten, § 3 Abs. 1 Nr. b ii ATDG) dokumentieren und veröffentlichen. Im LKA Berlin wird eine einheitliche Gesetzesanwendung durch die fachliche Kontrolle der Vorgesetzten im Dezernat LKA 54 gewährleistet. Ein Verstoß gegen die Kennzeichnungspflicht von Daten liegt nicht vor: Durch die Berliner Polizei wurden weder Rufnummern, die durch einen IMSI-Catcher-Einsatz noch durch Telekommunikations-Überwachungsmaßnahmen gewonnen wurden, in der ATD gespeichert. Hier muss insoweit ein Missverständnis vorliegen: Anlässlich der Prüfung durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit bei der Polizei wurde lediglich hypothetisch eine Informationsgewinnung mittels IMSI-Catcher und die spätere Speicherung so gewonnener Daten in der ATD erörtert.
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	

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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 {XE "Rechtsextremismus-Datei"}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, 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.

Zunächst legt der Senat Wert auf die Feststellung, dass die Einrichtung der RED aufgrund eines Bundesgesetzes erfolgte, welches auch von den Ländern umgesetzt werden muss. Unabhängig davon, welche Fehlerquellen im Einzelnen möglicherweise zu Pannen bei den Ermittlungen im NSU-Komplex geführt haben – die Ergebnisse der diesbezüglich laufenden Untersuchungen sind insoweit abzuwarten –, zeigen die Erfahrungen mit der analog aufgebauten Antiterrordatei, dass eine gemeinsame elektronische Plattform durchaus positive Effekte auf die Zusammenarbeit zwischen verschiedenen und mit unterschiedlichen Aufgaben und Befugnissen ausgestatteten Sicherheitsbehörden hat (s. Evaluierungsbericht der Bundesregierung vom 7. März 2013 zum Antiterrordateigesetz, BT-Drs. 17/12665, 4.1, S. 48). Durch die RED wird eine vergleichbare Intensivierung des Informationsaustauschs zwischen den Sicherheitsbehörden erwartet.

Die beim BKA geführten Verbunddateien zu politisch rechts motivierten Straftaten, auf die im

[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

[80] Siehe 3.1

	Bericht verwiesen wird, sind kein Äquivalent zur RED, da es sich hierbei um Dateien des Polizeilichen Informationssystems handelt, in denen allein polizeiliche Daten gespeichert sind, auf die die Nachrichtendienste keinen Zugriff haben. Die RED führt hingegen als Kontaktanbahnungsinstrument die relevanten Informationen von Polizei und Nachrichtendiensten zusammen und kann dazu beitragen, den Informationsaustausch zwischen Polizei und Nachrichtendiensten auch über Landesgrenzen hinweg zu beschleunigen. Darin liegt der entscheidende Mehrwert der RED gegenüber den genannten polizeilichen Verbunddateien. Im Hinblick auf die Vorgaben des BVerfG zur Antiterrordatei wird der Gesetzgeber allerdings auch das Gesetz zur RED auf den Prüfstand stellen müssen.
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, Fahndungspannen 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.

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 {XE "Stille SMS"}Stille SMS

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

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

81 § 45a ASOG, siehe JB 2011, 3.1
82 JB 2006, 2.2
83 Siehe JB 2003, 3.1 (S. 28 f.)

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 {XE "Abfragegrund"}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.

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.

Die angeregte Prüfung, ob eine unterbliebene Eingabe/Ergänzung des Abfragegrundes bei POLIKS-Abfragen dienstrechtlich zu verfolgen ist, wurde mit folgendem Ergebnis durchgeführt:
Gemäß § 35 Satz 2 BeamtStG sind Beamte verpflichtet, dienstliche Anordnungen ihrer Vorgesetzten auszuführen und deren allgemeine Richtlinien zu befolgen.

Die vorsätzliche oder fahrlässige Nichtbefolgung dienstlicher Anweisungen stellt, je nach den Umständen des Einzelfalls, ein Dienstvergehen gemäß § 47 Abs. 1 BeamtStG dar, wenn sie schuld-

[84] § 100a StPO

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
	haft erfolgte. Die Geschäftsanweisung LKA Nr. 6/2007 über die Erfassung polizeilicher Tätigkeiten und deren Eingabe in das polizeiliche Landessystem zur Information, Kommunikation und Sachbearbeitung (POLIKS) vom 17. September 2007 trifft zur Protokollierung des Abfragegrundes in Informationssystemen eine eindeutige Regelung (Nr. 4 der Tabelle zu Punkt 11), die wie folgt lautet: *Der Abfragegrund muss eingegeben werden, um die Abfragen im System so zu dokumentieren, dass sie für den Anfragenden später bei Bedarf nachvollzogen werden können. Hierbei ist der Katalogbegriff „Vorgangsbearbeitung" nicht ausreichend. Er ist durch weitere Eingaben im Feld „Ergänzungen" zu spezifizieren (z. B. die Vorgangsnummer, die Nennung des anfragenden Funkstreifenwagens oder den Hintergrund der Abfrage).* Die Regelung ist eindeutig und verbindlich. Unterbleibt die erforderliche Spezifizierung pflichtwidrig und schuldhaft, so stellt dies einen Verstoß gegen eine bestehende Weisungslage dar, der je nach den Umständen des Einzelfalls als Dienstvergehen zu bewerten und disziplinarrechtlich zu verfolgen ist. Der Polizeipräsident in Berlin wird die Beschäftigten seiner Behörde darüber informieren.
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 {XE "unbefugter Abruf"}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 erkennungsdienstliche 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 Löschungsantrag des Petenten stellte der Polizeipräsident fest, dass diese Daten für die ordnungsgemäße Aufgabenerfüllung nicht mehr erforderlich sind, und sicherte die **{**XE "Löschpflicht"**}**Löschung zu. Tatsächlich gelöscht wurde 2005 nur der Anlass-vorgang. Aufgrund eines Büroversehens ist die Löschung des personengebundenen Hinweises „BTM-Konsument“ unterblieben. Dieser Hinweis blieb

Der in diesem Beitrag geschilderte Sachverhalt war Gegenstand einer förmlichen Beanstandung nach § 26 Abs. 1 BlnDSG. Hintergrund ist eine im Jahr 2005 durchgeführte unvollständige Datenlöschung zu einem gegen den Betroffenen geführten BtM-Verfahren. Aufgrund eines Büroversehens kam es damals nicht zur Löschung der personenbezogenen Hinweise „BtM-Konsument“ und „Konsument harter Drogen“, sondern nur zur Löschung des Anlassvorgangs.
Die betreffenden Daten (personenbezogene Hinweise) wurden mittlerweile gelöscht.

Zur Vermeidung eines solchen Sachverhalts wurde 2010 im Bereich der zuständigen Dienststelle ein zusätzliches Kontrollinstrument eingeführt: Die im Bereich Informationstechnik durchgeführ-

also im polizeilichen Informationssystem weiter abrufbar.
Die unvollständige Löschung der Daten wurde beanstandet. Nach dem ASOG[85] sind personenbezogene Daten u. a. dann zu löschen und die dazugehörigen Unterlagen zu vernichten, wenn aus Anlass einer Einzelfallbearbeitung festgestellt 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 Auskunftsersuchens und das sich anschließende Löschungsbegehren war eine Einzelfallbearbeitung im Sinne dieser Vorschrift.
Wenn die gesetzlichen Voraussetzungen für Löschungen vorliegen, sind diese nicht nur zuzusagen, sondern auch zu vollziehen.

ten Datenlöschungen werden daraufhin überprüft, ob sie vollständig erfolgt sind.

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 Stadtstreicher“ 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 Länder[87] 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 Innenministerkonferenz[88] in Berlin umgesetzt. Die personengebundenen Hinweise „GEKR“ und „ANST“ werden nun wieder verwendet.

Personengebundene Hinweise (PHW) dienen dem Schutz der Betroffenen sowie der Eigensicherung von Polizeibeamten.

In Berlin werden PHW im Polizeilichen Landessystem zur Information, Kommunikation und Sachbearbeitung (POLIKS) vergeben. Sofern von dort ein Datenbestand im Informationssystem Polizei (INPOL) erzeugt wird (z.B. bei Fahndungen und erkennungsdienstlichen Behandlungen), werden bundesweit zu vergebende PHW dorthin übermittelt.

Durch den Beschluss des Abgeordnetenhauses von Berlin vom 1. Dezember 1988 (Drs. 10/2304 und 10/2688) hatte die Berliner Polizei die Speicherung der PHW „Geisteskrank“ und „Ansteckungsgefahr bzw. Vorsicht Blutkontakt“ in der Vergangenheit zu unterlassen. Damit war in Berlin der beabsichtigte Schutz weder für die

85 § 48 Abs. 2
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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
	Betroffenen noch für die eingesetzten Polizeibeamten möglich. Nachdem der AK II der Innenministerkonferenz in seiner Sitzung vom 20./21. Oktober 2011 unter TOP 22 unter anderem beschloss, die Personengebundenen Hinweise „Ansteckungsgefahr“ (ANST) und „Geisteskrank“ (GEKR) unter Berücksichtigung der im PHW-Leitfaden beschriebenen Vergaberichtlinien weiterhin zu nutzen, wurde die Senatsverwaltung für Inneres und Sport um Zustimmung zur Verwendung dieser PHW auch durch die Berliner Polizei gebeten. Mit Schreiben vom 1. Oktober 2012 wurde dem entsprochen. Die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit befürchtete Gefahr der Stigmatisierung Betroffener ist aufgrund der engen Voraussetzungen für die Vergabe der jeweiligen PHW nicht nachvollziehbar.
Bei der Vergabe von personengebundenen Hinweisen, die jedem Zugriffsberechtigten beim Aufrufen des Namens im polizeilichen Informationssystem **{**XE "POLIKS"**}**POLIKS angezeigt werden, ist Zurückhaltung geboten. Die Praxis hat gezeigt, dass die Hinweise „GEKR“ und „ANST“ für die geltend gemachte Eigensicherung der Polizei nicht erforderlich sind; insbesondere gab es keine Fälle von Ansteckung durch eine infizierte Person. Die Hinweise wirken stigmatisierend. 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{XE "Bundesmeldegesetz"}** Am Entwurf des Bundesmeldegesetzes[89] haben die Datenschutzbeauftragten insbesondere zu folgenden Punkten Kritik geübt:	Der Deutsche Bundestag hat nach Einschaltung des Vermittlungsausschusses das Bundesmeldegesetz am 28. Februar 2013 beschlossen. Der Bundesrat hat dem Gesetz am 1. März 2013 zugestimmt.
➢ Wiedereinführung der erst kürzlich abgeschafften Vermietermeldepflicht	Wesentlicher Streitpunkt war, ob für die Weitergabe persönlicher Daten an Firmen für Werbung und Adresshandel durch die Meldebehörden die

89 BT-Drs. 17/7746

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
➢ Beibehaltung der Hotelmeldepflicht ➢ Keine Widerspruchsmöglichkeit gegen einfache Melderegisterauskünfte ➢ Weiterhin keine Einwilligungslösung bei Melderegisterauskünften in besonderen Fällen ➢ Erweiterte Melderegisterauskünfte schon bei berechtigtem Interesse	ausdrückliche Einwilligung der Betroffenen erforderlich sein sollte oder ob die im bisherigen Entwurf vorgesehene Widerspruchslösung den Betroffeneninteressen genüge. Das nunmehr verabschiedete Gesetz sieht vor, dass künftig die Bürgerinnen und Bürger ihre ausdrückliche Einwilligung gegenüber der Meldebehörde oder dem an den Daten interessierten Unternehmen erteilen müssen, damit die Weitergabe und Nutzung der Daten rechtmäßig ist. Verstöße sollen mit Bußgeldern geahndet werden können. Zudem wird die Einwilligung stets nur streng zweckgebunden erteilt.
Das alles wurde vom Gesetzgeber nicht aufgegriffen. Vielmehr wurde der Entwurf im Vorfeld der legendären 57 Sekunden dauernden zweiten und dritten Lesung[90] (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]	
Wenn das Widerspruchsrecht Wirkung entfalten soll, dürfen keine Melderegisterauskünfte 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.	Da das Meldewesen nach Artikel 73 Abs. 1 Nr. 3 GG in die ausschließliche Gesetzgebungszuständigkeit des Bundes fällt, sieht der Senat von einer Stellungnahme zu Einzelfragen des verabschiedeten Gesetzes ab. Allerdings wird darauf hingewiesen, dass die Wiedereinführung der Vermieternebenmeldepflicht vom Senat als Instrument zur Bekämpfung von Scheinanmeldungen ausdrücklich begrüßt wird.

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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats

4.2 Zugriff auf das Melderegister{XE "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 Zwecke[92] künftig eine Abmahnung erfolgt.

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

Bei den geschilderten Einzelfällen handelt es sich um ein bedauerliches und beanstandungswürdiges Fehlverhalten von Beschäftigten der Bezirksämter, dem nach Auffassung des Senats durch geeignete Maßnahmen der Bezirke entgegengewirkt werden muss.

4.3 Löschung oder Archivierung von Meldedaten

Ein Erbenermittler klagte darüber, dass über Monate hinweg weder das Landesamt für Bürger- und Ordnungsangelegenheiten

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

(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**{**XE "LABO"**}** darf als Meldebehörde Privaten Auskunft aus dem Melderegister erteilen[93] 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.

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

[93] §§ 28, 29 Meldegesetz (MeldeG)
[94] §§ 25 – 27 MeldeG
[95] § 10 MeldeG
[96] § 4 Archivgesetz (ArchG)
[97] § 3 ArchG

zugreifen, da die Speicherfrist noch nicht für alle Daten abgelaufen ist.

Das LABO darf die Alt-Unterlagen ausschließlich zur eigenen Aufgabenerfüllung unter Berücksichtigung der Aufbewahrungsfristen[98] 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 sollten 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.

Datenbestände sind nach Ablauf der Speicherfrist dem Landesarchiv**{**XE "Landesarchiv"**}** anzubieten. Wenn dieses inner-halb von zwölf Monaten keine Archivwürdigkeit feststellt, sind die Daten zu löschen. Über die Ar-chivwürdigkeit entscheidet das Landesarchiv.

4.4 Dauerhafte Aufbewahrung von Einbürgerungsanträgen?

Ein Petent, der seinen Einbürgerungsantrag**{**XE "Einbürgerungsantrag"**}** 2006 zurückgezogen hatte, beschwerte sich An-fang August 2011 darüber, dass seine Daten weiterhin beim Bezirksamt Treptow-Köpenick gespeichert werden und darüber hinaus dem Be-zirksamt 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

[98] § 10 MeldeG

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.

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

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

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**{**XE "Verkehrsdatenerhebung"**}** mit Videotechnik, die von verantwortlichen Stellen des nicht-öffentlichen Be-reichs im Auftrag öffentlicher Stellen durchgeführt werden, sind nach dem Bundesdatenschutzgesetz zu bewerten.[100] Wenn es bei der Verkehrserhebung nicht darauf ankommt, die einzelnen Verkehrs-teilnehmenden 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**{**XE "Kennzeichenerfassung"**}** notwendig. Um die

[100] § 6b Abs. 1 Nr. 3 BDSG

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 Verkehrserhebung 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{XE "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.

Der Senat stellt hierzu richtig, dass die Tangentiale Verbindung Ost (TVO) eine neue Straßenverbindung ist, die einen Lückenschluss zwischen der nördlich der B 1/ B 5 gelegenen Märkischen Allee und der südlich der Straße An der Wuhlheide verlaufenden Spindlersfelder Straße bildet. Sie soll als übergeordnete Stadtstraße sowohl den Durchgangsverkehr aufnehmen als auch eine Er-

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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
	schließungsfunktion mit Entlastung parallel verlaufender und durch Wohngebiete führender Straßen erfüllen. Insofern wurde die Kennzeichenerfassung nicht auf der TVO, sondern im Rahmen der Untersuchungen zur Planung der TVO vorgenommen.
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.	Um die mit dem Bezirksamt Marzahn-Hellersdorf strittige Frage der Erforderlichkeit von Anbindungen aus dem Biesdorfer Gebiet und der Größe des Eigenverkehrs aus dem Gebiet und des Durchgangsverkehrs zu klären, hat ein Ingenieurbüro im Auftrag der Senatsverwaltung für Stadtentwicklung und Umwelt eine Verkehrserhe-bung (Verkehrszählung) und 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.	Diese beiden zur Erfassung vorhandener Verkehrssituationen üblichen, dem Stand der Technik entsprechenden Methoden wurden – wie vom Berliner Beauftragten für Datenschutz und Informationsfreiheit zutreffend dargelegt – von der Senatsverwaltung für Stadtentwicklung und Umwelt unter Beachtung aller rechtlichen Anforderungen datenschutzgerecht eingesetzt.
Wir haben bereits im Vorfeld die Erforderlichkeit der Erhebung der vollständigen Kennzeichen bezweifelt. Zur Erreichung des Projektziels war eine teilweise Kennzeichenerfassung**{**XE "Kennzeichenerfassung"**}** ausreichend. Eine andere Möglichkeit der anonymen Daten-verarbeitung 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 wur-den sofort bei der Erfassung verschlüsselt.	

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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{XE "Smartphone"} bieten den Nutzenden vielfältige Möglichkeiten, die über die ursprüng-lichen Grundfunktionen des Telefonierens sowie den Versand und Empfang von Kurzmitteilun-gen weit hinausgehen. Durch Internetzugang und die Nutzung von Software-Applikationen („{XE "App"}Apps“) haben sich insbesondere Fahrplanaus-künfte als hilfreiche Unterstützung für die ein-fache und schnelle Planung von Reisen im öf-fentlichen Nah- und Fernverkehr bei den An-wendern etabliert. Aufbauend auf dieser Ent-wicklung bieten die Anbieter des öffentlichen Personennahverkehrs (ÖPNV) sowie die Deut-sche Bahn im Fernverkehr zunehmend Lösun-gen für den Erwerb, die Nutzung und die Bezah-lung des Fahrtickets über das Mobiltelefon an.

Seit 2002 befassen sich national und international zahlreiche Projekte damit, das **elektronische Ticketing{**XE "elektronisches Ticketing"**}** zu etablieren. Darunter wird der bar-geldlose Erwerb sowie die elektronische Speiche-rung und Verwaltung von Fahrtberechtigungen für den öffentlichen Personenverkehr auf elektro-nischen 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{XE "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{XE "Smartphone"} sowie

per Handy über das mobile Internet oder als fest installiertes Java-Programm genutzt werden. In einigen Regionen besteht auch die Möglichkeit, nach der Regis-trierung 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.

Von der BVG und der S-Bahn werden laut eigener Auskunft im Rahmen des „Touch & Travel“-Systems keine Kunden**{**XE "Kundendaten"**}**- oder Bewegungsdaten**{**XE "Bewegungsdaten"**}** erhoben. Die Erhebung und Verarbeitung der Daten erfolgt durch die DB Mobility Logistics AG, die auch bei der Nutzung durch die Nahverkehrs-betriebe

Sowohl die BVG als auch die S-Bahn sind Kooperationspartner von Touch&Travel und beschränken sich darauf, das Verfahren Touch& Travel den eigenen Kunden bekannt zu machen und informieren ihre Kunden darüber, dass diese zur Nutzung der eigenen Verkehrsmittel auch durch Touch&Travel berechtigt sind.

Im Internetauftritt der BVG (www.bvg.de) wird hierüber im Abschnitt "Tickets und Tarife/Handyticket (Touch&Travel)" entsprechend informiert und der Nutzer wird sowohl im Unterpunkt "Datenerhebung" wie auch in den Links zum "BVG-Flyer Handyticket", "touchandtravel.de", "Downloads, Bedienungsanleitung, Infoblatt Datenschutz" und "Registrierung Handyticket Touch&Travel" eindeutig informiert, dass für das Verfahren Touch&Travel die DB Mobility Logistics AG (DB ML) die verantwortliche Stelle für die Datenerhebung im Sinne des BDSG ist. Ebenso wird (richtiger Weise) informiert, dass von Seiten der BVG im Rahmen von Touch& Travel keine Kunden- und Standortdaten erhoben bzw. verarbeitet werden. Außerdem steht in den App Stores immer die DB Mobility Logistics AG als Herausgeber.

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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
datenschutzrechtlich verantwortliche Stel-le 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.	Die DB ML hat hier keine wesentlichen "Verbesserungen" erreichen können, weil es derzeit keine technischen Lösungen zur weiteren Reduzierung der Datenerfassung gibt, die umsetzbar wären, ohne dass das Grundmodell dieses Vertriebskonzepts aufgegeben werden müsste. Das Grundkonzept besteht darin, ein niedrigschwelliges Angebot für Fahrgäste zu schaffen, die als Gelegenheitskunden ohne Tarifkenntnisse öffentliche Verkehrsangebote nutzen wollen in der Gewissheit, dass ihnen nach dem jeweiligen Fahrtende der passende Tarif berechnet wird. Nach wie vor existieren keine Alternativen in Form anonymer Verfahren zur sicheren nachträglichen Bezahlung eines vorab nicht bestimmbaren Reisepreises. Dies macht aber gerade die Attraktivität von Touch&Travel für den Fahrgast aus: das zugrunde liegende Vertragsverhältnis basiert darauf, dass die Fahrgäste mittels ihres eigenen Smartphones (oder NFC-Handy) ihre Reiseroute aufzeichnen lassen können, um im Nachhinein den Fahrpreis für die Route ermitteln und abrechnen zu lassen. Es wird also nachträglich ein Fahrschein für eine Reise ausgestellt, deren Verlauf die Nutzer von Touch&Travel erst unterwegs bestimmen wollen. Da auf diese Weise auch bei einer Fahrt schon Beträge im 3-stelligen Euro-Bereich anfallen können, scheinen derzeit anonyme Prepaid-Lösungen mit hinterlegten Sicherheitsleistungen in entsprechender Höhe den Nutzern weiterhin nicht zumutbar.
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.	Innerhalb des erforderlichen Rahmens der Datenverarbeitung wurden bereits Maßnahmen zur Minimierung der Funkortungsdaten erprobt und eingeführt, um mit möglichst wenig Daten auszukommen. Diese Maßnahmen wurden dem Berliner Beauftragten für Datenschutz und Informationssicherheit von der DB ML vorgestellt und dort begrüßt. Es bestand Einvernehmen, dass die Zuverlässigkeit und Genauigkeit der Fahrpreisermittlung gleichermaßen dem Interesse der Kunden und T&T dient. Daraus ergibt sich, dass ein un-

[103] JB 2011, 4.1

verzichtbares Mindestmaß an Daten benötigt wird. Kunden, die diese Datenerfassung nicht wünschen haben demnächst die Möglichkeit, im VBB auch das Handy-Ticket-Deutschland zu nutzen, bei dem der Fahrgast ein bestimmtes, von ihm vorher ausgewähltes Tarifprodukt vor Fahrtantritt mit dem Handy erwirbt.

Parktickets übers Handy

Aktuell bieten in Berlin sechs verschiedene Betreiber den Erwerb von Parkscheinen mithilfe des Mobiltelefons{XE "Handyparken"} an. Um das Angebot zu nutzen, ist es zunächst erforderlich, sich bei dem Betreiber zu registrieren. Eine Vig-nette, die im Auto hinter der Windschutz-scheibe angebracht wird, signalisiert den Be-schäftigten des Ordnungsamtes bei Kon-trollen, dass der Parkschein per Handy erwor-ben wurde. Der Erwerb kann über den 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

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

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.

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 Justizvollzugsdatenschutzgesetz[105] sieht u. a. die Einrichtung einer zentralen Auskunftsstelle**{**XE "zentrale 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

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

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 Gefangenendaten haben sollen und wie eine erfolgte Auskunftserteilung zu dokumentieren ist. Daneben haben wir bei den künftigen Beschäftigten der zentralen Auskunftsstelle eine datenschutzrechtliche Schulung durchgeführt.

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{XE "Einsichtsrecht"} 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{XE

[109] § 48 Abs. 1 Satz 2 JVollzDSG
[110] § 23 Abs. 2 JAG

"Prüfungsakten"**}** gewährt. Ein Dritter darf nur mit schriftlichem Einverständnis des Prüflings dessen Prüfungsakte einsehen. Wie-tergehende Informationsrechte des Prüflings oder Dritter aufgrund anderer Rechtsgrundlagen sind ausdrücklich ausgeschlossen. Der Ausschluss wietergehender 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]

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 Auftrags-datenverarbeitung 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

111 Siehe auch den Beschluss des OVG Berlin-Brandenburg vom 3. Dezember 2007 (OVG 12 N 40.07)
112 § 3 BlnDSG

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.

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{XE "Steuerakten"} – Neubewertung von Gebäudeteilen

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**{**XE "Einsichtsrecht"**}** 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 Diskussions-entwürfe des Bundesministeriums für Finanzen sahen zunächst vor, dass Betroffene ein berech-tigtes Interesse für

[113] JB 2006, 4.4.1

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
ihr Einsichtsbegehren darzule-gen 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 Sinnes-wandel 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 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.	Die Senatsverwaltung für Finanzen wurde vom Berliner Beauftragten für Datenschutz und Informationsfreiheit gebeten, dem Petenten eine Einsichtnahme in seinen Steuervorgang zu gewähren. Die Senatsverwaltung teilte daraufhin mit, dass die notwendigen Unterlagen zur Neubewertung der Gebäudeanteile bereits übersandt wurden. Dem Auskunftsanspruch des Petenten wurde damit entsprochen.
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{XE "Finanzamt"} für Fahndung und Strafsachen zur steuer-lichen Überprüfung{XE "Steuerprüfung"} der Einnahmen von Fahr-schulen 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 Außenprü-fungen der Steuerverwaltungen von Berlin und anderen Bundesländern festgestellt wor-den sei, dass Fahrschulen ihre steuerlichen Verpflichtungen nicht immer ordnungsgemäß erfüllen. In einer Vielzahl von Fällen seien Einnahmen ganz oder teilweise nicht erklärt	Das Finanzamt für Fahndung und Strafsachen forderte beim TÜV und bei der DEKRA sog. Prüflisten an, um die Vollständigkeit der Einnahmen bei Fahrschulen zu überprüfen. Es wurden die folgenden Daten erbeten: - Anzahl der abgelegten Prüfungen - Datum der theoretischen und praktischen Prüfungen inkl. Führerscheinklasse - Anzahl der Wiederholungsprüfungen Nach § 18 Fahrlehrergesetz (FahrlG) müssen die Fahrschulen Ausbildungsnachweise mit den persönlichen Daten des Fahrschülers, der Chronologie der Fahrausbildung und die erhobenen Ausbildungsentgelte mit Gegenzeichnung des Fahrschülers 4 Jahre aufbewahren. Bei Außenprüfungen werden diese Nachweise nicht in allen Fällen vorgelegt. Dadurch kann die Steuerverwaltung ohne weitere Ermittlungen nicht überprüfen, ob die Einnahmen vollständig erklärt worden sind.

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

Die Senatsverwaltung für Finanzen stellte nach Aufforderung des Berliner Beauftragten für Datenschutz und Informationsfreiheit die Hintergründe und rechtlichen Grundlagen dar, die die Anforderung der Daten rechtfertigen. Es wurde u.a. mitgeteilt, dass in den Jahren 2004 bis Januar 2012 von der Betriebsprüfung in Berlin insgesamt 132 Fahrschulen geprüft und in 80 Fällen Mehrergebnisse erzielt wurden, und dem Finanzamt für Fahndung und Strafsachen Berlin aussagekräftige Prüfergebnisse der Finanzverwaltung eines anderen Bundeslandes vorliegen. Dort wurden im Rahmen eines speziellen “Ermittlungs-/Prüfverfahrens“ 816 Fahrschule hinsichtlich der Erfassung ihrer Einnahmen steuerlich überprüft. In 486 Fällen (Stand 23. Juni 2011) wurde ein Mehrergebnis erzielt. Aus diesen Fällen ergaben sich Steuernachforderungen i.H.v. 5,8 Mio. Euro.

Nach der Rechtsprechung setzt die Abgabenordnung[114] 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 Führerschein-prüflinge von 178 Fahrschulen für die Jahre 2008 bis 2010[115] für die Aufklärung zunächst noch unbekannter Steuerfälle und Sachverhalte erforderlich sein soll, ist nicht nachvollziehbar.

Wie bereits im Bericht zutreffend festgestellt wurde, liegen die nach der Rechtsprechung notwendigen Voraussetzungen für das Tätigwerden der Steuerverwaltung vor. Die vorstehend genannten Erfahrungen der Steuerverwaltung über die Besteuerung von Fahrschulunternehmen belegen, dass ein hinreichender Anlass für das Tätigwerden der Steuerverwaltung vorlag.

Name und Anschrift der einzelnen Prüflinge wurden jedoch -wie bereits oben aufgeführt- nicht angefordert.

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

[114] § 208 Abs. 1 Nr. 3 AO
[115] Dabei handelt es sich um mehr als tausend unbeteiligte Betroffene.

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.
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{XE "Jugendamt"} eingesetzt wird. Das webba-sierte Verfahren WIMES{XE "WIMES"} („**Wi**rkungen **mes**sen“) soll in erster Linie dem Zweck die-nen, die Wirksamkeit von Hilfen zur Erzie-hung 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

[116] § 5a BlnDSG

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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{XE "Sozialdaten"} per-sonenbezogen über ein Webportal in die Daten-bank 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{XE "Pseudonymisierung"} der Sozialdaten erfolgte dann erst für die statistische Auswertung. Die Speicherung der Daten in personenbezogener Weise bei dem privaten Dienstleister, der statistische Auswer-tungen 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 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-Sicherheitsgrundsätzen[118] vorgeschriebenes verfahrensspezifisches Sicherheitskonzept vor der Verfahrenseinführung erstellt worden wäre.	
Da der Gesetzgeber enge Grenzen für die Zulässigkeit einer Auftragsdatenverarbeitung{XE "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	Die datenschutzrechtlichen Vorgaben des Gesetzgebers zur Auftragsdatenverarbeitung wurden durch die Senatsverwaltung für Bildung, Jugend und Wissenschaft eingehalten.

[117] § 24 Abs. 3 Satz 3 BlnDSG

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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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.	Die geplante fachliche Erweiterung des Verfahrens wurde aufgrund datenschutzrechtlicher Bedenken verworfen.
8.2 Kinderschutz{XE "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 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.	Die Erkenntnisse aus dem Projekt „Netzwerk Kinderschutz“ werden als Anforderungen in das neue IT-Verfahren Jugendhilfe einfließen.
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.

Der Verband Berlin Brandenburgischer Wohnungsunternehmen**{**XE "Wohnungsunternehmen"**}** e. V. kam auf die Idee, einen ähnlichen Handlungsleitfaden zu entwickeln. Er bat uns um datenschutzrechtliche Bewertung des Entwurfs der Verhaltensempfehlung „Wohnungs-unternehmen und Kinderschutz**{**XE "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**{**XE "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 Einord-

[119] JB 2011, 7.1.4

nung 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 berlineinheitlichen 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 Kooperationsver-

einbarung. Wir haben dem Bezirksamt unsere datenschutzrechtlichen Bedenken mitgeteilt und die HOWOGE in unserer Funktion als Aufsichtsbehörde nach dem Bundesdatenschutzgesetz[120] 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.

8.4 Überschießende Datenerhebung{XE "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

[120] § 33 BlnDSG i. V. m. § 38 BDSG

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**{**XE "Sozialdaten"**}**. Das sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einem Sozialleistungsträger im Hinblick auf die ihm nach dem Sozialgesetz-buch 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.
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.

[121] Siehe § 67 Abs. 1 Satz 1 SGB X
[122] § 26 Abs. 1 BlnDSG

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.

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**{**XE "Gesundheitsdaten"**}**. Speichert oder über-mittelt 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 Ein-

[123] § 67 c Abs. 1 Satz 1 SGB X

willigung 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 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 festgestellt[125] und auf die in solchen Fällen bestehende Informationspflicht hingewiesen.[126] Diese obliegt der übermittelnden Stelle u. a. gegenüber der Datenschutzaufsichts-behörde und der betroffenen Person, wenn beson-dere Arten personenbezogener Daten unrechtmäßig übermittelt wurden. Das LAGeSo hat uns gegen-über versichert, dass die komplette Akte des Peten-ten 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.

Die Angabe, wer in welchem Umfang zu welchen finanziellen Konditionen welche Leistungen erbringt, ist für den Sozialhilfeträger notwendig für die Überprüfung der zweckentsprechenden Verwendung der dem Leistungsberechtigten zur Verfügung gestellten Mittel. Darüber hinausgehende Einzelangaben über persönliche oder sachliche Verhältnisse sind grundsätzlich zur Überprüfung der zweckentsprechenden Mittel nicht erforderlich und können, so sie aus eingereichten Unterlagen ersichtlich sind, geschwärzt werden.

9 Gesundheitswesen

9.1 Neue Hygieneverordnung

Im Rahmen der Novellierung des Bundesinfektionsschutzgesetzes im August

[124] § 67 d Abs. 1 i. V. m. § 67 b Abs. 1 Satz 1 SGB X
[125] § 26 Abs. 2 BlnDSG
[126] § 83a Satz 1 SGB X

2011 wurden die Bundesländer verpflichtet,[127] bis 31. März 2012 für Krankenhäuser, Einrichtungen für ambulantes Operieren u. a. die erforderlichen Maßnahmen zur Verhü-tung, 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 **{**XE "Transparenz"**}**Transparenz im Umgang mit resistenten Keimen verpflichtet werden sollen. Wir haben eine entsprechende Forderung der Patientenbeauftrag-ten des Senats gegenüber dem Senator für Gesund-heit und Soziales unterstützt und darauf hingewie-sen, 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 Informationsfreiheitsbeauftragten 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

Sicherlich ist der Wunsch nach mehr Transparenz im Hinblick auf die Einhaltung allgemeingültiger hygienischer Standards verständlich, allerdings lässt sich dies nur sehr schwer messen und einfach und verständlich für die Patienten darstellen. Bestenfalls könnte hier der jährliche Verbrauch

[127] § 23 Abs. 8 IfSG
[128] GVBl. 2012, S. 215
[129] Entschließung vom 27. November 2012: Mehr Transparenz bei Krankenhaushygienedaten, siehe Dokumentenband 2012, S. 187; siehe auch 18.1

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
darüber hinaus zu mehr Transparenz im Gesundheitswesen und zu einem erhöhten Schutz der Patienten führen.	von Händedesinfektionsmitteln als Surrogat-Parameterin Betracht kommen. Mit einem hohen Verbrauch an Händedesinfektionsmitteln kann davon ausgegangen werden, dass die wichtigste Basishygienemaßnahme im Krankenhaus durchgeführt wird und das medizinische Personal die Hände desinfiziert. Außerdem gibt es bundesweite Vergleichszahlen dazu, die nach verschiedenen Fachrichtungen unterschieden werden und für Patienten zum Vergleich herangezogen werden können. Im Hinblick auf die Heterogenität der Patienten in den Berliner Krankenhäusern ist es nicht sinnvoll, Krankenhäuser zu Veröffentlichung Ihrer Infektionsdaten zu zwingen, zudem ist epidemiologisches- und krankenhaushygienisches Fachwissen zur korrekten Interpretation notwendig.

9.2 Ungesicherte Datenbaustellen in der Zentralen Stelle nach Kinderschutzgesetz

Zwei Jahre nach Inkrafttreten des Berliner Kinderschutzgesetzes[130] 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 feststellen, 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

[130] Siehe JB 2009, 7.1.2

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 herangetreten 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 **{**XE "Transparenz"**}**Transparenzgebot, nach dem die Betroffenen möglichst zu jeder Zeit wissen sollen, was mit den über sie gespeicherten Informationen geschieht. Lediglich in eng

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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**{**XE "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**{**XE "Patientendaten"**}** vornehmen. Ohne Ein-willigung der Sorgeberechtigten kann eine solche Offenbarung nur erfolgen, wenn in dem jeweiligen Einzelfall tatsächliche Anhaltspunkte für eine kon-krete Kindeswohlgefährdung vorliegen und diese nicht anders als durch die Datenübermittlung abzuwenden ist.	

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats

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 Landeskrankenhausgesetzes{XE "Landeskrankenhausgesetz"} (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{XE "Pseudonymisierung"}) 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 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{XE "Endoprothesenregister"} Deutschland

Das bundesweite Endoprothesenregister sam-

[131] JB 2011, 2.2.2

melt 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{XE "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{XE "Orientierungshilfe"} Krankenhausinformationssysteme{XE "Krankenhausinformationssysteme"}[132].

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.

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,

[132] JB 2011, 7.2.1

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{XE "Tablet-Computer"} in der medizinischen Behandlung durch die Charité

Presseberichten entnahmen wir, dass die Charité Tablet-Computer einsetzt, um einigen ihrer Ärztinnen und Ärzte den mobilen Zugriff auf Patientendaten{XE "Patientendaten"} zu gewähren. Wir prüften, ob hierbei die Vertraulichkeit der Daten gewähr-leistet bleibt.

Ärztinnen und Ärzte sind in ihren Kliniken{XE "Krankenhaus"} 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 elektro-nischen 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**{**XE "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**{**XE "IT-Sicherheit"**}** verant-wortlich zeichnet und ein Informationssicherheits-management nicht eingeführt ist, nicht bekannt. Genauso wenig bekannt schienen die Konsequen-zen, 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 wer-

den, 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 sensitiven Schreiben im Gesundheitsamt{XE "Gesundheitsamt"} Steglitz-Zehlendorf

Aufgrund einer Eingabe kontrollierten wir die Datenspeicherung in der Beratungsstelle für behinderte Menschen, Krebs- und AIDS-Kranke des Gesundheitsamts 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 sensitiven Daten{XE "sensitive Daten"} bemängelt und die Beratungsstelle aufgefor-dert, 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**{**XE "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**{**XE "Dienstvereinbarung"**}** dürfen nicht den Schutz des Bundesdaten-schutzgesetzes 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

[133] § 32 BDSG

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**{**XE "Protokollierung"**}** die Anzahl der Anrufe bzw. Übertragungsvolumina der pseudony-misierten Nutzenden dargestellt wird. Bevor die Kontrolldaten für die letzte Stufe der personenbezogenen Prüfung herangezogen werden, ist eine Verhältnismäßigkeitsprüfung durchzuführen. So kann z. B. schwerwiegendes vertragswidriges Verhalten oder der Verdacht einer Straftat oder eines Gesetzesverstoßes weitere Überprüfungsmaßnahmen rechtfertigen. Erst danach ist eine Entpseudonymisierung (Herstel-lung 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**{**XE "Personaldaten"**}**, deren Erhebung und Nutzung dem Erforderlichkeitsgebot unter-liegen. Der Arbeitgeber darf deshalb bei der Kon-trolle privater Internet-Nutzung durch Beschäftigte einen Personenbezug erst nach einer stufenweisen Ausschöpfung anderer Kontrollmöglichkeiten herstellen.

10.2 Dienstvereinbarung zur Telearbeit{XE "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 sensitiver Daten{XE "sensitive Daten"}. Dies sollte ex-plizit 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

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 {XE "Urheberrecht"}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**{**XE "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{XE "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{XE "Smart Meter"} detaillierte Verbrauchsdaten{XE "Verbrauchsdaten"} auf und ermög-lichen eine Übermittlung dieser Daten an exter-ne Marktteilnehmer. Durch eine langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff können sich massive Verletzungen der Privat-sphäre 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

[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

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 möglichst anonymisiert, pseudonymisiert oder aggregiert und an möglichst wenige Stellen übermittelt werden. Die Ableseintervalle 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

Nach dem Hinweis des Berliner Beauftragten für Datenschutz und Informationsfreiheit, dass Angaben in den Wohnlageeinwendungen, soweit sie Rückschlüsse auf die Antragsteller zulassen, nicht ohne deren Einwilligung veröffentlicht werden dürfen, wird die beanstandete Liste ab dem nächsten Berliner Mietspiegel 2013 weder Teil

[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.

[137] § 31 a BlnDSG

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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 angenommen 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.	des Endberichts sein noch veröffentlicht werden. Damit wird die Kritik des Berliner Beauftragten für Datenschutz und Informationsfreiheit aufgegriffen und das künftige Vorgehen den datenschutzrechtlichen Anforderungen angepasst.
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{XE "Bodenbelastungskataster"} betreibt. Darin sind Informationen zu einzelnen Grundstücken wie die Größe und die chronologische Nutzung eines Grundstücks sowie Angaben zu Boden-belastungen gespeichert. Daneben steht eine Karte zum Bodenbelastungskataster zur Ver-fügung. Zahlreiche andere Behörden wie die Senatsverwaltungen, Bezirksämter und die Polizei können auf diese Angaben zugreifen.

Im Bodenbelastungskataster werden Altlasten und Flächen, auf denen das Entstehen einer schädlichen Bodenveränderung zu besorgen ist, geführt. Diese Daten werden den Behörden oder sonstigen öffentlichen Stellen zur Verfügung gestellt, die sie zur Erfüllung der ihnen durch Gesetz zugewiesenen Aufgaben benötigen.

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

Dabei gestattet das Berliner Bodenschutzgesetz, das die Führung des Bodenbelastungskatasters als Teil eines Bodeninformationssystems vorsieht, die Einrichtung eines automatisierten Abrufverfahrens. Da es jedoch in der Vergangenheit Unklarheiten über die datenschutzrechtliche Bewertung der im Bodenbelastungskataster enthaltenen

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
Verfahren durch eine Rechtsverordnung geregelt wird.[138] Die Senatsverwaltung hätte darin vor Inbetriebnahme des Abrufverfahrens festlegen 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.	grundstücksbezogenen Daten gab, wurde bislang auf die Schaffung einer Rechtsverordnung über das Abrufverfahren zum Bodenbelastungskataster verzichtet. Nach Klärung dieser Frage mit Hilfe des Berliner Beauftragten für Datenschutz und Informationsfreiheit wurde seitens der Senatsverwaltung für Stadtentwicklung und Umwelt in enger Abstimmung mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit sowie den betroffenen Behörden (abrufende Stellen) ein Verordnungsentwurf erarbeitet. Dieser befindet sich noch in der Abstimmung, der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat im Februar 2013 eine überarbeitete Entwurfsfassung erhalten. Eine Gegenäußerung erfolgte dazu nicht. Das Abstimmungs- und Mitzeichnungsverfahren wird zur Zeit eingeleitet.
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**{**XE "Grundstücksdaten"**}**. Wenn das Verfahren weiter betrieben werden soll, ist dringend eine Rechtsver-ordnung zu erlassen.	
11.4 Wer darf in die Bauakte{XE "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	Das Recht auf Akteneinsicht ist in Berlin in § 4a VwVfGBln geregelt und wird danach unter-

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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
Informationszugang{XE "Einsichtsrecht"} 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 Einsichtsrechte 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]	schieden, ob die Einsicht wünschende Person am die Akten betreffenden Verwaltungsverfahren beteiligt ist (dann ist grundsätzlich Akteneinsicht zu gewähren, wobei die Einschränkungen der §§ 5 - 12 des IFG gelten) oder nicht (dann gilt das IFG unmittelbar). Ein rechtliches Interesse ist nicht darzulegen. Die Regelung in § 59 BauO Bln beschränkt sich auf die Erlaubnis zur Übermittlung von Daten, also das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten, vgl. § 4 Abs. 2 S. 2 Nr. 4 BlnDSG. Die Akteneinsicht wurde im Rahmen des Gesetzgebungsverfahrens zur Änderung der BauO Bln im Jahr 2005 nicht speziell geregelt, obwohl damals in Vorberatungen der Berliner Beauftragte für Datenschutz und Informationsfreiheit ausdrücklich neben der Datenschutzregelung, wie sie in § 59 BauO Bln eingeführt wurde, eine an § 4a VwVfGBln angelehnte Akteneinsichtsvorschrift gewünscht hatte. Nach seiner Auffassung waren die allgemeinen Regelungen für Verfahrensbeteiligte zu eng gefasst (da nicht alle am Bau Verantwortlichen umfasst seien), und die Regelungen des IFG zu weit gefasst (da sie auch Daten außerhalb von nach außen wirkenden Verfahren beträfen). Die Bedenken wurden verworfen, da die vermeintlichen Besonderheiten der Bauakten auch in anderen Rechtsbereichen vorkommen. Ein gesondertes Akteneinsichtsrecht neben den genannten allgemein geltenden Regelungen wurde nicht für notwendig erachtet. Damit gilt für die Akteneinsicht in Bauakten die allgemeine Regelung von § 4a VwVfGBln, s. o. Ob eine Anhörung von Betroffenen vor Gewährung der Akteneinsicht in jedem Fall erforderlich ist, zieht der Berliner Beauftragte für Datenschutz und Informationsfreiheit selbst in Zweifel, soweit nur die „Kerndaten“ (z. B. Namen, Anschrift, Verfahrensbeteiligung) betroffen sind. Andere Daten werden in Bauakten in der Regel nicht personenbezogen sein, da die Akten vor allem Lagepläne, Bauzeichnungen, z. B. Grundrisse, Ansichten und Schnitte, sowie Bau- und Betriebsbeschreibungen enthalten, vgl. §§ 1 - 8 Bauverfahrensverordnung.
Baubehörden müssen bei Anträgen auf Einsicht-	Im Ergebnis müssen Bauaufsichtsbehörden bei

[139] Siehe dazu schon JB 1995, 5.2
[140] § 59 Abs. 3 BauO Bln
[141] Z. B. Namen, Anschrift, Verfahrensbeteiligung; siehe § 6 Abs. 2 IFG

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
nahme in Bauakten prüfen, welches Interesse an der Einsichtnahme besteht und ob Interessen des Grundstückseigentümers entgegenstehen. Danach richtet sich, welche Informationen herausgegeben werden dürfen.	Anfragen von Nichtverfahrensbeteiligten nicht prüfen, welches Interesse an der Akteneinsicht besteht, sondern lediglich die Vorschriften des IFG berücksichtigen. In der Regel kann davon ausgegangen werden, dass über die „Kerndaten“ nach § 6 Abs. 2 IFG hinaus eher selten personenbezogene Daten betroffen sind, so dass eine Anhörung von Betroffenen entbehrlich sein wird.

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 {XE "Forschung"}Forschungskooperation, das an die Fachleh-rerkonferenz einer Schule gerichtet war. Da-rin wurden Lehrkräfte, die Aufgaben der Konferenzleitung übernommen hatten, zur Teilnahme an einer Online-Befragung{XE "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

Richtig ist, dass die im Jahresbericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit dargestellte Studie genehmigt wurde. Die Genehmigung enthielt jedoch weder schulspezifische Rückmeldungen, noch eine Verlosung auf der Grundlage erhobener Daten unter den an der Studie teilnehmenden Schulen, die zu Beanstandungen führten.

Ausdrücklich wurde im Genehmigungsschreiben darauf hingewiesen, dass die erhobenen Daten nur im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten Projekts verwendet werden dürfen. Der Studienleitung wurde bei Antragstellung eingehend und umfassend die Problematik schulspezifischer Rückmeldungen und Verlosungen im Zusammenhang mit Studien zusätzlich erläutert.

Mit dem Genehmigungsschreiben ist zudem die Auflage erteilt worden, dass durch Art oder Inhalt der Erhebung in Rechte von Lehrkräften nicht eingegriffen werden darf. Hierzu zählt auch, dass die Sicht der Lehrkräfte zum Zeitpunkt der Datenerhebung über die freiwillige Teilnahme an der Studie hinreichend durch die zugeleiteten Informationen berücksichtigt wird.

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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.	Als Erklärung für die fehlende Einhaltung der Auflagen im Genehmigungsschreiben bei der Durchführung der Studie wurden nach Kenntnisnahme von Beschwerden aus Schulen und auf Nachfrage der Senatsverwaltung für Bildung, Jugend und Wissenschaft von der Studienleitung Befürchtungen angegeben, dass die Akzeptanz der Befragung unter Schulleitungen sich hätte verringern bzw. die – vor der Einreichung des Antrags zur Genehmigung der Studie in der Verwaltung – gemachten Zusagen gegenüber Schulleitungen einer schulspezifischen Rückmeldung bzw. Verlosung von Büchergutscheinen nicht hätten eingelöst werden können.
Für die Freiwilligkeit einer Einwilligung**{**XE "Einwilligung"**}** ist die Sicht der Betroffenen zum Zeitpunkt der Datener-hebung aufgrund der vorhandenen und durch die verantwortliche Stelle zugeleiteten Informationen entscheidend.	

12.1.2 Können Partner sich gegenseitig für Elterninterviews**{**XE "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**{**XE "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.

§ 65 Abs. 3 Satz 4 SchulG lässt die Verarbeitung personenbezogener Daten ohne Einwilligung der Betroffenen ausnahmsweise dann zu, wenn sonst der Zweck einer von der Schulaufsichtsbehörde genehmigten wissenschaftlichen Untersuchung nicht erreicht werden kann und das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen überwiegt. Da eine Auskunft durch die Betroffenen in Kenntnis der vorgesehenen Nutzung der erfragten Daten ohne die Einwilligung nicht erlangt werden kann, ist dies eine gesetzlich geregelte Ausnahme vom Grundsatz der Datenerhebung direkt bei der betroffenen Person.

Eine Teilnahme- und Auskunftspflicht besteht gemäß § 9 Abs. 4 SchulG (nur) bezüglich solcher Evaluationsmaßnahmen, die von der Schulaufsichtsbehörde oder in deren Auftrag durchgeführt werden; hier werden erhobene personenbezogene Daten vor der Auswertung anonymisiert oder pseudonymisiert (§ 65 Abs. 1 Satz 2 u. 3 SchulG), so dass schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.

Die Mitwirkung an von der Schulaufsichtsbehörde genehmigten Forschungen Dritter ist freiwillig. Erhobene personenbezogene Daten müssen anonymisiert werden, sobald der Forschungszweck dies zulässt (§ 65 Abs. 3 Satz 5 SchulG). Unter den vorstehend genannten engen Voraussetzungen lässt § 65 Abs. 3 Satz 4 SchulG es ausnahmsweise zu, dass personenbezogene Daten auch dann verarbeitet werden, wenn die Einwilligung widerrufen oder verweigert wurde.

Die Erhebung sensitiver Daten**{**XE "sensitive Daten"**}** (z. B. zur Ein-kommenssituation oder Herkunft) setzt darüber hinaus das gesteigerte Bewusstsein über die Abfrage dieser Daten voraus,

Der Senat stimmt zu, was die Anforderungen an die Einwilligung in die Verarbeitung von besonders schutzwürdigen personenbezogenen Daten angeht; hinsichtlich der im Fall einer

[142] § 10 Abs. 4 BlnDSG

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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.	ausnahmsweise im öffentlichen Interesse zu erwägenden Verarbeitung ohne Einwilligung gemäß § 65 Abs. 3 Satz 4 SchulG ist das Gewicht der schutzwürdigen Belange umso höher zu veranschlagen je tiefer der Einblick in die persönlichen Verhältnisse der Betroffenen eröffnet wird und je später die Anonymisierung erfolgen kann.
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 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.	Der Senat stimmt dem zu, soweit die Datenverarbeitung nur mit Einwilligung der Betroffenen rechtlich zulässig ist. Voraussetzung für das Einwilligungserfordernis von Bezugspersonen des oder der Befragten ist aber, dass Angaben über persönliche oder sachliche Verhältnisse der dritten Person auch tatsächlich zugeordnet werden können. Das ist dann in der Regel nicht der Fall, wenn weder der Familienname noch die Anschrift der Bezugsperson erhoben werden und auch nicht mit Namen und Anschrift der befragten Person übereinstimmen oder sonst erkennbar sind.
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.	Bei der Genehmigung wissenschaftlicher Untersuchungen in Schulen werden die im Datenschutzbericht angeführten Kriterien bei der Prüfung von Anträgen berücksichtigt, dies gilt insbesondere auch für den Grundsatz der Direkterhebung personenbezogener Daten bzw. der Datenerhebung bei Dritten mit schriftlicher Einwilligung wie bei dem angeführten Beispiel beider Elternteile.

12.1.3 Zusammenarbeit mit der Ethik-Kommission{XE "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

[143] JB 2011, 8.1.2

„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 Konse-

quenzen 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**{**XE "Probandendaten"**}** bedeutsam.

Wir berieten die Kommission bei der Neufassung der Mustererklärung zur Einhaltung des Datenschutzes.[144] In dieser Erklärung bringen nunmehr die 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**{**XE "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**{**XE "Bibliothek"**}** Berlins einge-setzt werden.

[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

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

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 Bibliotheksausweise 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 taz[147] in dem Artikel „Schnüffelsoftware auf Schulcomputern“, dass die Schulbuchverlage und die Verwertungsgesellschaften mit den Kultusministerien den Einsatz einer Scan-Software auf Schulcomputern{XE

[146] JB 2011, 8.1.6
[147] taz vom 1. November 2011, S. 6

"Schulcomputer"**}** vereinbart hätten, um illegale Kopien von Unterrichts-materialien aufzuspüren. Bereits am 21. Dezember 2010 war dazu ein Gesamtvertrag zur Einräumung und Vergütung von Ansprüchen nach § 53 **{**XE "Urheberrecht"**}**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**{**XE "Plagiatssoftware"**}** an der Überprü-fung von Schulrechnern mitzuwirken und die privaten und kommunalen Schulträger aufzu-fordern, die Vorgaben des Vertrages anzu-wenden.

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**{**XE "Fernmeldegeheimnis"**}**. Der Zugriff auf sie tangiert auch das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Die Umsetzung der Regelungen des Gesamtver-trages 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 Landesbeamtengesetz noch in anderen Gesetzen eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten zu diesem Zweck vorhanden ist.

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 Verwertungsgesellschaften 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{XE "Smartphone"} 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{XE "App"}“ jedoch auch Funktionen, mit denen wesentlich sensitivere Leistungsdaten (z. B. Noten) verwaltet werden können. Die Verarbeitung von derartigen personenbezogenen Schülerdaten{XE "Schülerdaten"} auf einem privaten Datenverarbeitungsgerät ist den Lehrkräften – wie anderen Bediensteten der Berli-

Der Einsatz privater Datenverarbeitungsgeräte durch Lehrkräfte für die Verwaltung von Schülerdaten ist gemäß § 64 Abs. 2 Satz 3 SchulG in Verbindung mit § 12 Abs. 6 der SchuldatenVO nur mit Genehmigung der Schulleitung zulässig, nachdem der oder die Schuldatenschutzbeauftragte gehört worden ist und die Lehrkraft sich schriftlich verpflichtet hat, die datenschutzrechtlichen Vorschriften einzuhalten und dem Berliner Beauftragten für Datenschutz und Informations-

[148] Siehe Inhaltsprotokoll zur 3. Sitzung am 6. Februar 2012, Punkt 2, Seite 2 ff.
[149] Tagesspiegel vom 10. Dezember 2012, S. 25
[150] Z. B. die Smartphone-Software „Teachertool“, siehe www.teachertool.de

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
ner 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{XE "Tablet-Computer"} auch unsichere „Apps“ installiert 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.	freiheit die Kontrolle zu ermöglichen; Daten, die das Persönlichkeitsrecht in besonderem Maße berühren, dürfen gar nicht auf privaten Geräten verarbeitet werden; Leistungsdaten dürfen dort nur zeitlich eng begrenzt gespeichert werden, Verhaltensdaten nur zum Ausdrucken von Zeugnissen. Die Verarbeitung auf Rechnern mit Festplatte ist grundsätzlich als datensicher anzusehen, wenn personenbezogene Daten verschlüsselt, die Sicherheitsupdates des Betriebssystems regelmäßig durchgeführt, eine Firewall und ein Virenschutzprogramm verwendet und keine öffentlichen Internetzugänge (z.B. in Internet-Cafes oder Hot-Spots) genutzt werden. Auch die Verwendung verschlüsselter USB-Sticks ist hinreichend sicher. Dagegen ist die Frage der technischen Datensicherheit bei der Verwendung von Smartphones bzw. Tablets noch zu klären. Dem Senat sind bisher keine Apps bekannt, die die Sicherheitsanforderungen erfüllen oder entsprechend zertifiziert sind.
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, Vorna-	Mit Rundbrief der Senatsverwaltung für Bildung,

[151] Siehe 2.3
[152] § 64 Abs. 2 Satz 2 und 3 SchulG

men und Angaben zu den jeweils besuchten Schulen um personenbezogene Daten der Abiturientinnen und Abiturienten. Die Übermittlung dieser Schülerdaten{XE "Schülerdaten"} durch die Schule an die Presse ist nur mit schriftlicher Einwilligung{XE "Einwilligung"} der Betroffenen zu-lässig.[153] Wird die Datenverarbeitung auf die Einwilligung der Betroffenen gestützt, sind sie 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.

Jugend und Wissenschaft vom 22. März 2013 sind die betroffenen Schulen darauf hingewiesen worden, dass die Weitergabe von Abiturientennamen an die Presse die vorherige schriftliche Einwilligung jeder einzelnen betroffenen Person voraussetzt. In dem Rundbrief wurde vorsorglich auch darauf hingewiesen, dass die vorherige schriftliche Einwilligung der Betroffenen auch bei der Veröffentlichung personenbezogener Daten aus anderem Anlass erforderlich ist.

[153] § 64 Abs. 5 Satz 2 Nr. 1 SchulG
[154] § 6 Abs. 3 BlnDSG
[155] § 6 Abs. 5 BlnDSG

Das Schulgesetz{XE "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 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{XE "Abiturzeugnis"} des Regierenden Bürgermeisters

Der Süddeutschen Zeitung[158] 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

[156] § 64 Abs. 7 Satz 1 SchulG
[157] § 64 Abs. 7 Satz 1, 2. Halbsatz SchulG
[158] Süddeutsche Zeitung vom 10. Oktober 2011, S. 3

Jahren bei der Leitung der Schule unterstützt hat, habe einen Generalschlüssel für die Schule besessen. Während seiner Abwesenheit habe sein Vorgänger ihn vertreten, 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{XE "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 Zeugnis-

[159] § 13 Satz 1 SchuldatenVO
[160] § 13 Satz 2 SchuldatenVO
[161] § 5 Abs. 4 i. V. m. § 5 Abs. 2 Nr. 1 BlnDSG

daten 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 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{XE "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{XE "Bilddaten"} 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

[162] § 26 Abs. 1 BlnDSG

Verantwortung des (privatrechtlichen) Betreibers des Inter-nats gedreht worden. Diesem sei von der Schulleitung eine Dreherlaubnis in den Räu-men der Schule erteilt worden. Alle Schü-lerinnen und Schüler, die während der Filmaufnahmen Basketball spielen und teil-weise kurz im Bild zu sehen sind, seien vor-her über den Verwendungszweck der Film-aufnahmen 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 Schulgesetz**{**XE "Schulgesetz"**}**[163] darf eine Schule perso-nenbezogene 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**{**XE "Einwilligung"**}** gestützt werden, so ist er in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklä-ren.[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 Einsichts-

[163] § 64 Abs. 1 SchulG
[164] § 6 Abs. 3 BlnDSG; § 4 a Abs. 1 BDSG

fähigkeit 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 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{XE "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 Schul-

[165] Siehe 12.2.3

leitungen 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 Schulgesetz{XE "Schulgesetz"}[167] darf eine Schule jedoch die perso-nenbezogenen Daten einer Schülerin oder eines Schülers an eine andere Schule nur übermitteln, wenn dies zur rechtmäßigen Erfüllung der gesetz-lichen 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 Bru-

[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

der 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 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**{**XE "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**{**XE "Berliner Schulen"**}** bereits 2009 ausführlich behandelt[168] und darauf hingewiesen, dass weder das Schulgesetz noch die dazu ergangenen Verordnungen bereichsspezifi-sche Regelungen zur Videoüberwachung an Schu-len 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

[168] JB 2009, 2.2

Zweck und unter welchen technisch-organisatorischen Rahmenbedingungen die Videotechnik an Schulen eingesetzt wird. Deshalb 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{XE "Bilddaten"} statt-findet.[169] Wir haben datenschutzrechtliche Kontrol-len 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 Bild-

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

materials nicht zur Täteridentifizierung führte. Wir haben die Geeignetheit der Videoüberwachung in diesem Einzelfall bezweifelt. Durch die dargelegten Vorfälle 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{XE "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 überschießenden Daten zu löschen sind. Diese Verpflichtung ergibt sich aber aus dem Erforderlichkeitsprinzip und dem Grundsatz der Datensparsamkeit[172] 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

[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

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 verwendeten 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 Daten[175] 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 Geldwäscheaufgaben 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, Auskunftsersuchen 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

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

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.

13.1.2 Ist das ec-cash-Verfahren{XE "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.

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

13.1.3 Kuvertierungsprobleme in einer Bank

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.

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**{**XE "Kuvertierung"**}**. Es gab zwar eine Doppeleinzugskontrolle, die bei einem Mehrfacheinzug von Briefen die Maschine anhielt, sodass die Fehlkuvertierungen manuell aussortiert werden konnten. Die Beschäf-tigten haben es aber versäumt, die Fehlkuver-tierungen auch tatsächlich auszusortieren. Sie wur-den geschult, damit sich ähnliche Vorfälle nicht wiederholen.

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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
Fehler bei der Kuvertierung bei Banken gefährden nicht nur die Datensicherheit, sondern können auch das Bankgeheimnis verletzen.	

13.1.4 Vorsicht bei Online-Bonitätsprüfungen**{**XE "Bonitätsprüfung"**}**!

Nach einer Bestellung in einem Online-Shop erhielt ein Bürger von einer Auskunftei 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 Auskunftei 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 Auskunftei 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**{**XE "Einwilligung"**}** eingeholt werden, und zwar bevor mit der Datenübermittlung an eine Auskunftei 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 Einwilligung durchgeführt werden, soweit über das Verfahren transparent aufgeklärt wird.

[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.

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 kreditorischen Risiko vorzunehmen.

13.2 Industrie- und Handelskammer

13.2.1 IHK{XE "IHK"} als Adresshändler

Der Gesetzgeber hat den Industrie- und Handelskammern das Recht eingeräumt, mit den personenbezogenen Daten der Kammerzugehörigen zur Förderung des Wirtschaftsverkehrs Adresshandel{XE "Adresshandel"} zu betreiben.[181] Kammerzugehö-rige 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.

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

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

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**{**XE "Widerspruchsrecht"**}** war der Adresshandel der IHK Berlin über viele Jahre rechtswidrig. Der Missstand ist jetzt behoben.

13.2.2 Überprüfung der Wahlvorschläge**{**XE "Wahlvorschlag"**}** 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 Bestellungszeitpunkt und der Darstellung 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 unstreitig. 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 „dünnerer“ Fragebogen verwendet werden. Erst bei Unklarheiten über die Person der Kandidatin oder des Kandidaten und der Qualifikation als besonders bevollmächtigte Person könnten in einer zweiten Phase durch spezielles 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{XE "fragdenstaat.de"}“ – jetzt datenschutzgerecht

Der Verein Open Knowledge Foundation

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

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 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{XE "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

[183] § 4 Abs. 1 BDSG

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 vor-

[184] § 203 StGB

kommen, 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.

§ 6 b BDSG nennt die Voraussetzungen, nach denen die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung**{**XE "Videoüberwachung"**}**) zulässig ist. Allerdings ist es zweifelhaft, ob es sich z. B. bei einem Konzert-mitschnitt 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 eigene Zwecke im Allgemeinen benennt, unabhängig von der Art und Weise der Erhebung.

In der Regel dienen Bild- und Tonaufnahmen**{**XE "Bilddaten"**}** 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 Nut-zungsrechte 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 Tonauf-nahmen 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 Aufführ-ung 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

[185] § 23 Abs. 1 Nr. 2 Kunsturhebergesetz

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.

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 sorgsamen Umgang mit personenbezogenen Daten verpflichtet. Auch ungewollte **{**XE "Datenschutzverstoß"**}**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 Auskunftei. 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 Auskunftei den Abfragegrund unrichtig mit „Wohnraumvermietung“ an und erschlich sich so personenbezogene Daten der Betroffenen.[187] Da

[186] § 43 Abs. 2 Nr. 1 BDSG, § 17 Abs. 2 OWiG
[187] § 43 Abs. 2 Nr. 4 BDSG

der Rechtsanwalt diese Abfrage veranlasst hatte, war er selbst an der Ordnungs-widrigkeit 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 beseitigt, 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.

14. Europäischer und internationaler Datenschutz

14.1 Neuer europäischer Rechtsrahmen

Im Januar hat die Europäische Kommission den Entwurf eines neuen Rechtsrahmens[190] 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

[188] § 14 OWiG
[189] § 38 Abs. 5 BDSG
[190] Siehe schon JB 2011, 10.1
[191] Art. 16 Vertrag über die Arbeitsweise der Europäischen Union

Verarbeitung personenbezogener Daten und zum freien Datenverkehr (**Datenschutz-Grundverordnung{XE "EU-Datenschutz-Grundverordnung"}**).[192] Der zweite Teil beinhaltet den Vorschlag für eine **Richtlinie über die justi-zielle und polizeiliche Zusammenarbeit**.[193] Mit dieser Reform soll die bislang geltende Europäische Datenschutzrichtlinie 95/46/EG von 1995 ebenso ersetzt werden wie der Rahmen-beschluss des Rates[194] 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 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 Entschliessungen verdeutlicht[196] und in umfassenden Stellungnahmen[197] 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 Kohärenzverfahren[199] sowie auf die

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.

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

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 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.

[200] Ebenda

14.2 Weitere Ergebnisse aus Brüssel

Im Juli ist das neue Abkommen zur **Übermittlung von Fluggastdaten{XE "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, sondern auch zu Flügen innerhalb der EU.[203] Dazu müssen die Mitgliedstaaten eine PNR-Zentralstelle einrich-ten, 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 Vorratsdaten-peicherung 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{XE "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

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

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

[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)

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-Richtlinie[209] wurde analysiert, bei welcher Art von verwendeten -Cookies 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{XE "Cloud Computing"}** verfasst,[212] in das auch die Erkennt-nisse aus der Orientierungshilfe Eingang gefunden haben, die im letzten Jahr von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und dem Düsseldorfer 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 Datenüber-

[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 13), siehe Dokumentenband 2012, S. 76

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

[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

mittlung 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. Standardvertragsklauseln[215] anerkannt, die, wenn sie ohne Änderungen vom Auftraggeber und Auftragnehmer genutzt werden, eine Datenübermittlung in den Drittstaat ermöglichen, 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**{**XE "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.

---

215 Beschluss 2010/87/EU vom 5. Februar 2010, siehe Dokumentenband 2010, S. 70
216 § 4c Abs. 2 BDSG
217 JB 2010, 11.1

15 Datenschutzmanagement

15.1 Bundesweite Premiere: Anerkennung von Verhaltensregelungen nach dem BDSG

Der Gesamtverband der Deutschen Versicherungswirtschaft**{**XE "Versicherungswirtschaft"**}** (GDV) hat uns „Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft“ vorge-legt.[218] Diese waren zuvor in mehrjährigen Ver-handlungen mit den Datenschutzaufsichtsbehörden abgestimmt worden. Im November haben wir dem GDV beschieden, dass dieser Verhaltenskodex**{**XE "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 Selbst-regulierung 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 Schweigepflichtentbindungserklärungen abgeben wollten, denn der Abschluss der gewünschten Versicherung war an

[218] Siehe Dokumentenband 2012, S. 37
[219] Siehe § 38a BDSG

die Abgabe der Einwilligung geknüpft.[220] Nunmehr soll die Datenverarbeitung in der Versicherungs-wirtschaft 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.

15.2 Informationspflicht{XE

[220] JB 2011, 9.1.4

"Informationspflicht"} bei Datenlecks{XE "Datenlecks"} in Wirtschaft und Verwaltung

Die Anzahl der Mitteilungen bei einer unrechtmäßigen Kenntnisnahme von personenbezogenen Daten durch Dritte ist insbesondere im nichtöffentlichen 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 BDSG[222] oder BlnDSG[223] 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 Betracht, wenn Telekommunikationsanbieter den durch das TKG gewährten Schutz personenbezogener Daten verletzen.

Häufig werden Vorfälle im Zusammenhang mit der Bedienung von **Bürokommunikationsmittel**n gemeldet, so z. B. **Fehlsendungen per Fax**, die durch einen Faxnummernabgleich vor dem Ver-

---

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).

senden hätten vermieden werden können. Zudem wird uns öfter angezeigt, dass **E-Mails** versehentlich an einen offenen Verteiler versendet wurden, was aufgrund der komfor-tablen 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{XE "Datenpannen"} in der Wirtschaft

Patientenunterlagen{XE "Patientendaten"} im Keller

Aufgrund eines Hinweises aus der Bevölkeung 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 Ortmöglich 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 aus-

[225] JB 2007, 7.3.6; JB 2008, 8.2.4

reichend belegt. Zudem war es problematisch, dass das Krankenhaus sämtliche Patientenunter-lagen 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**{**XE "Aufbewahrungsfristen"**}** erst zu vernichten, wenn feststeht, dass keine Benachrich-tigungspflicht besteht. Akten anderer verant-wortlicher 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

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**{**XE "Tourenpläne"**}** drohten schwerwiegende Beeinträchtigungen für die Rech-te oder schutzwürdigen Interessen der Betroffenen: Bei den Angaben zu den Pflegemaßnahmen handelt es sich um **{**XE "sensitive Daten"**}**sensitive Daten**{**XE

"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.

Fehlsendung 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**{**XE "Personalvermittlung"**}** hatte die Betrof-fenen 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 sensitiven Daten**{**XE "sensitive Daten"**}** im geparkten PKW hinterlassen werden. Außerdem kann auch der Verlust oder Diebstahl von Papier-akten eine Informationspflicht**{**XE "Informationspflicht"**}** auslösen. Eine Fest-platten-verschlüsselung ist nur dann wirksam, wenn das Gerät zum Zeitpunkt des Verlusts auch tatsächlich ausgeschaltet ist. Trotz Verschlüsselung ist zu berücksichtigen, dass ein möglicher Angrei-fer das Gerät in seiner Gewalt hat und folglich unbeschränkt verschiedene

Passworte durchpro-bieren kann. Dementsprechend muss das Passwort für die Verschlüsselung**{**XE "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 Laborin-formationssystems 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**{**XE "Musterformular"**}** muss darauf geachtet werden, dass sie entweder keine personenbezogenen Daten enthalten oder anonymisiert wurden.

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

[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

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**{**XE "Personaldaten"**}** zugreifen, obwohl dies nach dem Berechtigungskonzept der BVG nur Personalverantwortlichen erlaubt war. Auch bestand kein Zweifel daran, dass schwerwie-gende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohten: Informationen zu krankheitsbedingten Fehl-

zeiten 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**{**XE "Personalvertretung"**}** 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 unzu-lässigerweise – 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{XE "sensitive Daten"} betroffen. Andererseits war die Gefahr, die von den Datenempfängern ausging, als gering zu bewerten, da die Mitglieder der Personalver-tretungen generell zur Verschwiegenheit verpflich-tet sind. Das Bezirksamt hat gleichwohl die Betroffenen über die fehlerhaften Datenübermitt-lungen informiert und wird künftig keine Informa-tionen über ärztliche Fachrichtungen an die Perso-nalvertretungen weiterleiten.

Eine Informationspflicht{XE "Informationspflicht"} kann auch dann in Be-tracht kommen, wenn die Daten verarbeitende Stelle eine bewusste Datenübermittlung vorgenom-men hat, die unzulässig war.

Schülerakten verschwunden!

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{XE "Informationspflicht"} zu prüfen. In der Regel ist eine zweiwöchige Prüffrist der datenverarbeitenden Stelle nur bei komplexen Sachverhalten angemes-sen. Da die Grundschule zunächst eine intensive Suche durchgeführt hatte, war die Benachrich-tigung 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 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.

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

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 Fraugen 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**{**XE "Forschung"**}** ausgewertet und in Form von Behand-lungsempfehlungen an die teilnehmenden Einrich-tungen 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**{**XE "Patientendaten"**}** mehr vor. Die Daten sollen nunmehr in den lokalen Systemen der teilnehmenden Einrichtungen ano-nymisiert und in dieser Form an die Forschungs-datenbank 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 Koalitionsfraktionen[228] 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 Datenschutzbeauftragten[229] in dem aktuellen Stiftungskonzept nicht berücksichtigt wurden. So entsprechen die vorgesehenen Mitwirkungsmöglichkeiten über den Beirat 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 getroffe-

[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

ne 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**{**XE "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 verein-facht 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 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

[230] Siehe 16.4.1

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

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 2011[232] 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 Überragung 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 die Privat-sphäre 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 ih-

[232] JB 2011, 2.3

rer 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 Wollen 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 Nutzung[233] – 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

[233] § 13 Abs. 6 TMG

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.

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

Bereits 2011[234] haben wir auf Probleme bei der Nutzung von sozialen Medien – insbesondere in Bezug auf Social Plugins**{**XE "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 gegenwärtig verzichtet werden.

[234] JB 2011, 2.3

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{XE "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 Klarname durch ein Pseudonym ersetzt werden. Das Klarnamenprinzip 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

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

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 werden 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 überwachtes 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 gebil-

[239] Siehe nur § 11 Abs. 4 und 5 Satzung der Piratenpartei
[240] Art. 38 Abs. 4 VvB

det 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.

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**{**XE "IT-Sicherheit"**}** finden sich z. B. unter http://www.verbraucher-sicher-online.de.

16.4.1 Selbstschutz gegen Tracking

Unter (Web-) Tracking**{**XE "Tracking"**}** versteht man im Allgemei-nen die Bildung von Profilen über Internetnut-zende, 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 Erfolgschancen 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{XE "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

[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.

bewusst eingesetzt werden. Mittlerweile bieten alle Browser ausgefeilte Cookie-Konfigurationsmöglichkeiten, meist unter „(Internet-) Einstellungen/Datenschutz“.
Cookies sollten grundsätzlich 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 Listen[242] mit den bereits bekannten Trackingdiensten herunterladen.

Derzeit wird im World Wide Web Consortium (W3C) über die Standardisierung eines Verfahren 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-Richtlinie[243] 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.

[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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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.	

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**{**XE "Suchmaschine"**}** ein unerwünschter Treffer angezeigt wird. Die erste Forderung der Betroffenen ist meist, dass dieser Inhalt aus der jeweiligen Such-maschine – meist Google – gelöscht werden soll. Übersehen wird dabei jedoch, dass der beanstan-dete Inhalt in der Regel nicht von der Suchma-schine 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 Bundes-datenschutzgesetz verweisen, nach dem das Erhe-ben, Speichern, Verändern oder Übermitteln per-sonenbezogener Daten zulässig ist, wenn die Daten allgemein zugänglich sind, es sei denn, dass schutzwürdige Interessen der Betroffenen am Aus-schluss der Veröffentlichung offensichtlich über-wiegen.[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 Löschauf-

[244] § 28 Abs. 1 Satz 1 Nr. 3 BDSG

forderung könnten z. B. sein, dass die Veröffentlichung das Recht am eigenen Bild[245] 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.

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**{**XE "Pseudonymisierung"**}** bit-ten.

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 Verantwor-

[245] § 22 Kunsturhebergesetz

[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.

tung 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 Gesetzgeber 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

2010[248] haben wir ausführlich über die Datenschutzfragen bei Smartphones und sog. Smartphone-Apps berichtet. Problematisch ist dabei, dass die Apps aus unbekannten 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**{**XE "IT-Sicherheit"**}** unzurei-chend dokumentiert. Wir waren an der grund-sätzlichen Bewertung der Ergebnisse mehrerer Vergleichstests der Stiftung Warentest beteiligt.

Das häufigste Problem ist die Übermittlung von Geräte-Identifikationsnummern**{**XE "Geräte-Identifikationsnummer"**}** (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 Werbung zu ermöglichen oder Statistiken über die App-Nutzung zu erstellen. In der Regel werden die Nutzenden darüber nicht aufgeklärt,

[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.

und insbesondere steht keine Möglichkeit zur Verfügung, dieser Art der Datennutzung zu widersprechen.
Andere Apps übermitteln z. B. ohne Einwilligung{XE "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]

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

[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.

Funktionen geändert. Die Prüfungen werden wir fortsetzen.

2010[251] 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 iOS[252] 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 Android[253] 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 8[254] 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-Identifikationsnummer 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

[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.

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**{**XE "digitale Werbeflächen"**}** auch mit Videotechnik. Ein Hersteller hat uns sein Produkt vorgestellt und um unsere Ein-schätzung hinsichtlich des Einsatzes von Video-kameras 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 Bekleidungsherstellers „angezogen“ werden.

[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.

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{XE "Berlin Group"}“) hat auf ihrer 51. Sitzung in Sopot (Polen) ein viel beachtetes Arbeitspapier zu Fragen des Daten-schutzes und der Privatsphäre beim Cloud Compu-ting („Sopot Memorandum“)[256] verabschiedet. Da-rin 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]

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]

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

256 Dokumentenband 2012, S. 171
257 Zur Situation in Deutschland siehe JB 2011, 2.1.1
258 Dokumentenband 2012, S. 168

Eile erarbeitet worden und entsprachen nicht den Vorgaben der IT-Standards**{**XE "IT-Standards"**}** des Landes. Für die Vorbereitung der Kontrolle waren sie deshalb nur bedingt verwendbar.

Die Unterlagen sollen im Wesentlichen die nach dem Berliner Datenschutzgesetz[259] gebotene Trans-parenz der Datenverarbeitung gegenüber interes-sierten Nutzenden der Bäder gewährleisten. Ein wichtiger Bestandteil sind die Dateibeschreibungen, deren Gestaltung in § 19 BlnDSG geregelt ist. Danach hat jede Person das Recht, ohne Angabe von Gründen in den ersten Teil der Dateibeschreibung Einsicht zu nehmen. Wir haben einen repräsentativen Ausschnitt untersucht und festgestellt, dass keine einzige Dateibeschreibung ohne Mängel war. Deshalb haben wir Hinweise für die Korrektur aller Dateibeschreibungen 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 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, empfahlen 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 Infor-

[259] § 5 Abs. 2 Nr. 6 BlnDSG

mationstechnik[260] gefertigt waren. Insbesondere die fehlende Aktualität der Konzepte und Pläne war auffallend.

Obwohl die festgestellten Mängel stellenweise so gravierend waren, dass eine förmliche Beanstandung[261] 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 {XE "Datenschutzbeauftragte"}Datenschutzbeauftragte eines Bezirksamtes hat sich an uns gewandt, weil er bei der Prüfung der Meldungen zur Dateien-übersicht[262] auf Vollständigkeit die notwendi- ge Unterstützung der Fachabteilungen vermisste.

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.

---

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
263 § 19 a Abs. 3 BlnDSG

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 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 Auf-gaben zu unterstützen. In einigen Bezirken sind strukturelle Verbesserungen überfällig.

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

Einer gesetzlich festgeschriebenen Offenlegung von zwischen Forschungseinrichtungen und Unternehmen abgeschlossenen Kooperationsverträgen steht aus Sicht des Senats entgegen, dass die Vertragsinhalte vielfach geheimhaltungsbedürftig sind und entsprechend in den bisher geschlossenen Verträgen oft Vertraulichkeitsklauseln und Geheimhaltungspflichten enthalten sind. Das liegt

[264] JB 2010,12.4
[265] § 7 Satz 1 Nr. 4 BlnDSG

und den freien Zugang zu Dokumenten der EU[266] 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 Hygienebestimmungen[269] 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 nächs-ten Jahr wird die IFK unter dem Vorsitz des Thü-ringischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit stattfinden, dem mit der Änderung des Thüringer Informationsfreiheits-gesetzes zum Jahresende die Funktion des Infor-mationsfreiheitsbeauftragten übertragen wurde. Damit nehmen in allen elf Bundesländern mit Informationsfreiheitsgesetzen ebenso wie im Bund die Datenschutzbeauftragten zugleich die Auf-gaben eines Beauftragten für Informationsfreiheit wahr.

Als ein Meilenstein der Informationsfreiheit kann das im Juni beschlossene **Hamburgische Transparenzgesetz{XE "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

daran, dass die Wirtschaft i. d. R. mit Kooperationen mit Forschungseinrichtungen ein Verwertungsinteresse verbindet. Um geistiges Eigentum optimal zu schützen und später entsprechende Verwertungsrechte beanspruchen zu können oder auch nur aus puren Gründen eines zeitlichen Wettbewerbsvorsprungs kommt die intendierte Offenlegung der Verträge nicht in Frage. Eine Umsetzung der zitierten Entschließung dürfte das Interesse der Wirtschaft, beispielsweise mit hier betreuten Forschungseinrichtungen zusammenzuarbeiten, weitgehend lahmlegen.

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).

272 Hmb GVBl. S. 271

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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 IFG[274] zusammenführen mit den fortschrittlichen Rege-lungen des hamburgischen Modells, damit auch in Berlin der grundlegende Paradigmenwechsel zu einem Informationszugang vollzogen werden kann, der grundsätzlich von Amts wegen und nicht erst auf Antrag zu gewähren 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.	Der Gesetzesentwurf entspricht in seinem Ansatz der vom Senat schon heute betriebenen Informationsfreiheitspolitik. Das Berliner Informationsfreiheitsgesetz gewährleistet ein umfassendes Informationsrecht und ist im bundesweiten Vergleich eine der informationsfreundlichsten Regelungen. Darüber hinaus hat der Berliner Senat sich in den Richtlinien der Regierungspolitik für die aktive Bereitstellung von Daten und Informationen aus den Landesbehörden ausgesprochen. Mit dem Open-Data-Portal, das im September 2011 als Pilotanwendung eingerichtet und seit dem kontinuierlich ausgebaut wurde, stellt Berlin öffentliche Daten zentral strukturiert, maschinenlesbar und offen lizensiert bereit. Auch ohne gesetzliche Verpflichtung bzw. auf untergesetzlicher Ebene verfolgt der Senat das Ziel, den Bürgerinnen und Bürgern in zunehmendem Maße aktiv Verwaltungsdaten über das Internet bereitzustellen.
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 öffent-lichen Stellen Informationen zu erhalten, hat bis-lang 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	

[273] Drs. 17/0456

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

[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

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{XE "Hygienesiegel"} im Gaststättenbereich** berich-tet.[277] Die meisten Bezirke bezweifeln zu Unrecht nach wie vor, dass sie die Ergebnisse von Res- taurantüberprüfungen ins Internet stellen dür-fen. Daran hat auch das neugefasste Verbraucher-informationsgesetz nichts geändert.[278] Während das für den Verbraucherschutz zuständige Bundes-ministerium 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 ge-stoppt. 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 wurden.[279] Ggf. müssen rechtlich verpflichtende Bestimmungen einheitlich für alle Bezirke geschaffen werden.[280]

Auch für die **Forschung{XE "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 Forschungsprojekt[281] 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 Lebensmittel-aufsicht mehr Angaben über die Betriebe und die bei ihnen durchgeführten

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

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“

Lebensmittelkontrollen beinhaltet. Für den Fall, dass die Einsichtnahme der Unterlagen des Bezirksamtes in personenbe- ziehbarer Form geplant war, musste den Betroffe-nen 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 Bezirksamts konnte zugunsten des Informationszugangs die Verwendung der Daten zu reinen Forschungszwecken und die im weiteren Verarbeitungsprozess angestrebte Anonymisierung der Daten berücksichtigt werden.

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 Darstellung des Sachverhaltes durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit ist in mehrfacher Hinsicht unzutreffend:

- faktisch, wenn in der Überschrift eine Mehrzahl von Problemfällen suggeriert wird, es sich aber um einen Einzelfall handelt;
- faktisch, wenn behauptet wird, dem Beauftragten sei erst nach „Androhung einer Beanstandung wegen Verletzung der Unterstützungspflicht“ eine abschließende Antwort erteilt worden. Richtig ist vielmehr, dass nach einem längeren Schriftwechsel zwischen der Senatskanzlei und dem Beauftragten deren abschließendes Schreiben vor der Beanstandungsandrohung abgesandt wurde. Diese Tatsache war für den Berliner Beauftragten für Datenschutz und Informationsfreiheit aufgrund der Zeichnungsdaten der jeweiligen Schreiben ohne weiteres erkennbar;
- rechtlich, weil zwingend zu berücksichtigen ist, dass die Protokollierung der Senatsbeschlüsse einschließlich der in der Sitzung erfolgten und vorhergehenden Beratungen keine trennscharfe Abgren-

[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.)
[284] § 10 Abs. 3 Nr. 1 IFG
[285] § 14 Abs. 2 Satz 2 GO Sen

	zung zwischen den beiden Komponenten „Beschluss“ und „Protokoll“ zulässt. Dies ist dem Berliner Beauftragten für Datenschutz und Informationsfreiheit bereits im Rahmen des oben angeführten längeren Schriftwechsels erläutert worden.
Die Auffassung der Senatskanzlei war in mehrfacher Hinsicht rechtsirrig. Der Schutz des behördlichen Entscheidungsprozesses[286] 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.	Insofern bleibt der Senat bei seiner Rechtsauffassung, dass § 14 Absatz 2 der Geschäftsordnung des Senats, der die Vertraulichkeit seiner Beratungen und Beschlüsse festlegt, im Einklang mit der in Berlin geltenden Rechtslage zur Informationsfreiheit steht. Der Senat sieht daher keine Veranlassung, seine auf der Grundlage von Artikel 58 Absatz 4 der Verfassung von Berlin erlassene Geschäftsordnung zu ändern. In diesem Fall vertreten das Verfassungsorgan Senat und der Berliner Beauftragte für Datenschutz und Informationsfreiheit unterschiedliche Rechtsauffassungen.
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	Dem Berliner Beauftragten für Datenschutz und Informationsfreiheit ist in rechtlicher Hinsicht lediglich dahingehend zuzustimmen, dass ein Senatsbeschluss als solches den Beratungsvorgang abschließt und daher nicht automatisch, sondern lediglich wegen der o.g. zusätzlichen Argumentation unter den Ausschlusstatbestand des § 10 Absatz 3 Nr. 1 Informationsfreiheitsgesetz (IFG) fällt.

[286] § 10 Abs. 3 Nr. 1 IFG

wurden.

Die Senatskanzlei teilte uns erst nach mehreren Monaten und nach mehrmaliger Aufforderung sowie Androhung einer Beanstandung[287] wegen Verletzung der Unterstützungspflicht[288] 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 proaktive Veröffentlichungspflicht für alle Senatsbeschlüsse einführen.

Privatisierungsverträge{XE "Privatisierungsverträge"} der Wohnungsbaugesellschaft GSW

Mehrere Petenten begehrten 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 veröffentlichende 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

Die Abwägung zu dem Versagungsgrund der Betriebs- und Geschäftsgeheimnisse erfolgt auf der Grundlage von Informationen der betroffenen Gesellschaften, hier insbesondere der GSW als Beteiligte des Verfahrens. Die GSW hat zu den einzelnen Abschnitten des Vertrages jeweils nach-

287 § 26 Abs. 1 BlnDSG
288 § 28 Abs. 1 BlnDSG
289 § 7 IFG
290 § 12 IFG
291 § 1 IFG

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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.	vollziehbar dargelegt, inwieweit ihre schützenswerten Interessen betroffen sind und wie sie durch eine Veröffentlichung verletzt werden. Aus Sicht der Verwaltung gab es keine Erkenntnisse, dass diese dargelegten Erwägungen unzutreffend sind und eine Einschränkung von Betriebs- und Geschäftsgeheimnissen zu Lasten der Gesellschaft notwendig ist. Auf der anderen Seite galt es zu berücksichtigen, dass eine Veröffentlichung unter einem Verstoß gegen die Abwägung zu Schadensersatzansprüchen und ggf. auch zu strafrechtlichen Konsequenzen führen kann.
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 entgegenstehen, 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]	Eine Ablehnung oder Verzögerung der Einsichtnahme gegenüber dem Berliner Beauftragten für Datenschutz und Informationsfreiheit hat es durch die Senatsverwaltung für Finanzen nicht gegeben. Diesem wurden die Unterlagen vollumfänglich zur Verfügung gestellt, wobei sich der betreffende Mitarbeiter ausdrücklich für die ausführlichen mündlichen Hintergrundinformationen der Vertragsgeschichte und die angefertigten und ausgehändigten Kopien bedankt hat. Gleichzeitig hat er in diesem Gespräch die kollegiale Zusammenarbeit gelobt.
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.	Dem Berliner Beauftragten für Datenschutz und Informationsfreiheit wurde außerdem mitgeteilt, dass seine Auffassung bei der weiteren Entscheidungsfindung berücksichtigt wird, jedoch für die Widerspruchsbehörde keine verbindliche Vorgabe darstellen kann.
Behörden gehen mit dem Ausschlussgrund des Schutzes von Betriebs- und Geschäftsgeheimnissen noch immer zu großzügig um.	Was die Frage der „Offenkundigkeit“ durch rechtswidriges Veröffentlichen der Verträge im Internet betrifft, so ist davon auszugehen, dass eine unautorisierte Offenlegung aus unbekannter Quelle nicht der Maßstab für die Beurteilung nach dem IFG sein kann.

<u>Mühsame Akteneinsicht bei der Senatsverwaltung für Stadtentwicklung und Umwelt</u>

[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

[293] § 134 BGB

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
Ein Petent begehrte bei der Senatsverwaltung für Stadtentwicklung und Umwelt die Übersendung von Kopien des Antrags sowie des Genehmigungsbescheids nebst Anlagen in einem wasserrechtlichen Genehmigungsver fahren Dritter. Nachdem wir vermittelnd tätig geworden waren, erhielt der Petent einige der begehrten Unterlagen. Die Herausgabe der übrigen Umweltinformationen{XE "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 {XE "Urheberrecht"}Urheberrechte{XE "Urheberrecht"} verletzt wer-den würden, und wiesen darauf hin, dass eine ab-strakt geäußerte Vermutung eine Ablehnung nicht rechtfertigen kann. Auf mehrmalige Nachfragen wurde uns zwar 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 Senatsver-waltung nunmehr zum Ergebnis gekommen war, dass dem Informationszugang doch keine Urheber-rechte entgegenstehen. Interessant war die Begrün-dung der Senatsverwaltung vor allem deswegen, weil diese nun ausführte, dass eine urheber-rechtliche 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 Be-richten nicht um schöpferische Leistungen, da die Ingenieure keinen Freiraum bei der Darstellung hätten.	Dem Petenten wurden auf seinen Antrag auf Aktenauskunft vom 31. Januar 2012 im März 2012 Kopien der wasserbehördlichen Genehmigungen übersandt. Kopien der Pläne, Zeichnungen und statischen Prüfberichte wurden aus Gründen des Urheberrechtes nicht übersandt. Tatsächlich hat es bis zur Auskunftserteilung in dem von dem Petenten gewünschten Umfang bis Oktober 2012 gedauert, da der Vorgang aufgrund eines gegen den Bescheid gerichteten Schreiben des Petenten, der als Widerspruch ausgelegt wurde, in das Widerspruchsverfahren und somit an die für die Widersprüche nach dem IFG zuständige Stelle weitergegeben wurde, wo er einer umfassenden rechtlichen Prüfung, die auch Ermittlung zu tatbestandlich schwierigen Sachverhalten erforderlich machte, unterzogen wurde.
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	Umgehend nach Erlass des Widerspruchsbescheides im Oktober 2012, der den ursprüngliche Bescheid teilweise aufgehoben hat, wurde dem Petenten Kopien der Pläne, Zeichnungen usw. übersandt. Der Senat teilt die Auffassung des Berliner Beauftragten für Datenschutz und Informationsfreiheit, dass grundsätzlich Einsichtbegehren nach dem In-

[294] § 18a Abs. 1 IFG i. V. m. § 9 Abs. 1 Satz 1 Nr. 2 UIG

Umständen hinnehmbar.[295]

formationsfreiheitsgesetz in kürzerer Zeit abschließend zu bescheiden sind.

Eine Behörde darf der Herausgabe von Kopien nicht pauschal Urheberrechte entgegenhalten. Vielmehr hat sie im Einzelfall zu prüfen, ob tatsächlich Urheberrechte entgegenstehen.

Einsicht{XE "Einsichtsrecht"} in eine Vereinbarung zum baurechtlichen Sozialplanverfahren

Zwei Petenten begehrten bei der Senatsverwaltung für Stadtentwicklung und Umwelt Einsicht in eine Vereinbarung zum Sozialplanverfahren[296] 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.

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{XE "Auskunftsanspruch"} in Bezug auf den Regelungsgehalt der geschwärzten Passagen gehabt. Eine Durchsicht der Verein-barung, die uns die Senatsverwaltung zur Prüfung übersandt hatte, ergab, dass der Akteneinsicht keine Ausschlussgründe entgegenstanden und insbesondere keine Betriebs- oder Geschäftsgeheimnisse[298] 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 sei[299] 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

295 Eine sog. Untätigkeitsklage kann gegen eine Behörde bereits nach drei Monaten erhoben werden, siehe § 75 VwGO.
296 §§ 180, 181 BauGB
297 § 12 IFG
298 § 7 IFG
299 § 14 Abs. 2 IFG
300 § 14 Abs. 2 Satz 1 IFG

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 Infor-mationsinteresse das Interesse der Betroffenen an der Geheimhaltung überwiegt[301].

Trinkwasseruntersuchungen{XE "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

[301] § 14 Abs. 2 Satz 1 IFG

Petentin sprechen sowie auf welcher Rechtsgrundlage das Gesundheitsamt**{**XE "Gesundheitsamt"**}** sie nach ihrer behan-delnden Ärztin gefragt und sodann Kontakt mit dieser aufgenommen hat.

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**{**XE "Gesundheitsamt"**}** sie nach ihrer behandeln-den Ärztin gefragt 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

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
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.	Grundsätzlich führt die Trinkwasserverordnung dazu in § 21 Information der Verbraucher aus, dass der Unternehmer einer Wasserversorgungsanlage den betroffenen Verbrauchern mindestens jährlich geeignetes und aktuelles Informationsmaterial über die Qualität des bereitgestellten Trinkwassers zu übermitteln hat. Darüber hinaus sind Informationen über die Trinkwasseruntersuchungen in gewerblich genutzten Gebäuden (Wohnhäusern) unverzüglich allen betroffenen Verbrauchern schriftlich oder durch Aushang bekannt zu machen.

<u>Fehlerhafte Rechtsfortbildung im Rechtsamt Reinickendorf</u>

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 Prüfvorgänge 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 Stellung-nahme, aus welchen rechtlichen Gründen die Akteneinsicht verweigert wird, teilte uns das bezirkliche Rechtsamt{XE "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 Korruptionsbe-kämpfung in der Hauptverwaltung“ festge-schrieben. Auch müsse es immer Bereiche geben, die einer Einsichtnahme wegen der besonderen Materie der Akten von vornherein entzogen seien.

Diese rechtsirrige 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**{**XE "Einsichtsrecht"**}** 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.

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 Unterstützungspflicht[304] 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

302 § 4 Abs. 1 IFG
303 § 5 Satz 1 IFG i. V. m. § 37 Abs. 3 BeamtStG
304 § 28 Abs. 1 BlnDSG

wurde uns die begehrte Einsichtnahme ermöglicht.

Die Durchsicht des gesamten Prüfvorgangs 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 Prüfvorgänge 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.

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 Daten[306] sowie der Schutz besonderer öffentlicher Belange, der Rechtsdurchsetzung und der Strafverfolgung[307] 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 vor-

[305] § 17 Abs. 5 Satz 2 IFG
[306] § 6 IFG
[307] § 9 IFG
[308] § 17 Abs. 5 Satz 1 IFG

genannten Verzeichnisse entgegen der gesetzlichen Vorgabe nicht allgemein zugänglich gemacht werden[309] 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 Beratungsersuchen 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]
Das Bezirksamt teilte uns später mit, dass der bisherige auf Personendaten basierende Aktenplan nun auf ein den Anforderungen des IFG genügendes nummerisches 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.

Die Senatsverwaltung für Inneres und Sport wird in Kürze zum wiederholten Male in einem Rundschreiben alle öffentlichen Stellen des Landes Berlin auf ihre Pflicht aus § 17 Abs. 5 Informationsfreiheitsgesetz (IFG) hinweisen, Aktenpläne und ggf. weitere Verzeichnisse zu führen und allgemein zugänglich zu machen.

Allgemein zugängliche Aktenpläne sind die Grundvoraussetzung für eine spätere detaillierte Informationsanfrage, wie der Fall im weiteren für den Petenten unglücklichen Verlauf zeigte.

Der Petent begehrte 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 Ä – der Höchstgebühr[311] –, wobei sich dem Bescheid nicht entnehmen ließ, wie sich die Gebühr

[309] § 17 Abs. 5 Satz 2 IFG
[310] Abrufbar unter www.datenschutz-berlin.de/content/berlin/berliner-beauftragter/aktenordnung
[311] Siehe Tarifstelle 1004 b) Nr. 3 des Gebührenverzeichnisses zur Verwaltungsgebührenordnung

zusammensetzte.

Eine Prüfung des umfangreichen Bescheids ergab, dass die Akteneinsicht**{**XE "Einsichtsrecht"**}** bei 18 der vorgenommenen 19 Einschränkungen nicht bzw. nicht vollständig hätte abgelehnt werden dürfen. So rügte das Be-zirksamt mehrfach, dass der Petent sein Informa-tionsinteresse 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 Entscheidungsprozesses[313] mehrfach komplette Unterlagen ab, ohne zu begründen, weshalb hier keine beschränkte Akteneinsicht gewährt werden konnte.[314]

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**{**XE "Gebührenbescheid"**}** schlüsselte es zwar den Verwaltungs-aufwand nunmehr nachvollziehbar pro Aktenord-ner auf, ging jedoch nicht auf unsere Argumente ein und rückte auch nicht von der Höchstgebühr ab. Dem Petenten blieb daher nur die Klage-erhebung. Hierzu stellten

312 § 6 Abs. 1 IFG
313 § 10 IFG
314 § 15 Abs. 3 IFG i. V. m. § 12 IFG
315 § 11 IFG

wir ihm unsere Stellung-nahme 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.

19 Was die Menschen sonst noch von unserer Tätigkeit haben…

Ein Bürger informierte uns darüber, dass er von einem Krankenhaus irrtümlich einen **Entlassungsbericht{XE "Entlassungsbericht"}** mit Gesundheitsdaten eines anderen Patie-nten **per Fax erhalten** habe. Die Klinik teilte uns mit, dass ärztliche Mitteilungen nur bei Dring-lichkeit oder auf Patientenwunsch veranlasst wür-den. 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{XE "Hotelmeldeschein"}**. 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{XE "Zeitschriften-Abonnement"}**. Auf dem Bestellformular kreuzte er „Zahlung per Rechnung“ an und füllte die Felder nicht aus, die

[316] Siehe § 60 Abs. 1 Satz 1 Nr. 3 SGB I

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2012	Stellungnahme des Senats
für die **Bankverbindungsdaten** vorgesehen waren. Trotzdem buchte das Unterneh-men den Rechnungsbetrag vom Konto des Betrof-fenen ab. Das Unternehmen griff dabei auf Bank-verbindungsdaten 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 werden konnten. Aufgrund unserer Intervention hat das Unternehmen nunmehr ein **Sperrkonzept** entwickelt und umgesetzt.	
Ein Bürger begehrte bei der **Ärztekammer 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**{**XE "Auskunftsanspruch"**}** bestehe, sondern sich dieser nur bezogen auf bestimmte Verfahrensakten ergeben könne. Ei-ne 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 begehrte und die Gebühr nicht etwa pro Akte, sondern grundsätzlich pro Antrag erhoben wird. Nach unserer Intervention erhielt der Bürger gebührenfreie Auskünfte.	An die Ärztekammer Berlin wurden im Jahr 2012 insgesamt sechs Anträge nach dem Berliner Informationsfreiheitsgesetz (IFG) gerichtet. In drei Fällen wurden die Anträge abgelehnt, in einem Fall nur teilweise Auskunft erteilt, im Übrigen wurde den Anträgen stattgegeben. Alle Ablehnungen erfolgten unter dem Gesichtspunkt des berechtigten Schutzes personenbezogener Daten (§ 6 Absatz 1 IFG). Auch in dem hier geschilderten Fall, in welchem Auskünfte im Zusammenhang mit berufsrechtlichen und berufsgerichtlichen Verfahren begehrt wurde, hat die Kammer sich zunächst in der Pflicht gesehen, das informationelle Selbstbestimmungsrecht ihrer Mitglieder zu schützen.
Eine Bürgerin bat nach dem IFG beim **Bezirksamt Charlottenburg-Wilmersdorf** um Übersendung dreier **Rechtsgutachten zu einem Bebauungsplan{XE "Bebauungsplan"}**. Ein Gutachten wurde ihr zwar zur Verfügung gestellt, die Herausgabe der beiden übrigen Gutachten jedoch unter Verweis auf den Schutz des behördlichen Entscheidungspro-zesses[318]	

[317] Siehe Tarifstelle 1004 des Gebührenverzeichnisses zur Verwaltungsgebührenordnung

[318] § 10 IFG

abgelehnt: Diese dienten 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{XE "Aktenplan"} des Büros des Bezirksbürgermeisters** einsehen. Das Bezirks-amt 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 Einsicht-nahme mitteilen werde. Wir wiesen das Bezirks-amt darauf hin, dass Aktenpläne, Aktenordnungen und ähnliche Verzeichnisse allgemein zugänglich zu machen sind[320] 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.

20 Aus der Dienststelle

20.1 Entwicklungen

Der langjährige Stellvertreter des Berliner Beauftragten für Datenschutz und Informationsfreiheit, Diplominformatiker Hanns-Wilhelm Heibey, trat

[319] § 10 Abs. 2 Satz 1 IFG
[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.

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 Computing[322] 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 Senats[323] 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]

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 Kommission[325] Stellung zu nehmen.

20.3 Zusammenarbeit mit anderen Stellen

322 JB 2011, 2.1.1
323 Abgh.-Drs. 16/4334
324 Siehe 1
325 Siehe Einleitung und 14.1

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 Entschließungen 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 fasste mehrere Entschließungen zu aktuellen Fraugen 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]

[326] Dokumentenband 2012, S. 9 ff.
[327] Dokumentenband 2012, S. 25, 61
[328] Dokumentenband 2012, S. 185 ff.
[329] Siehe 14.2 und Dokumentenband 2012, S. 63 ff.

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 Entschließung 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.

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:

330 Dokumentenband 2012, S. 167 f.
331 Dokumentenband 2012, S. 171 ff.

- 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